TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Rahvusvahelise ja Euroopa õiguse õppetool

Sille Rästas

KÜBERRÜNNAKUTE OMISTAMINE RIIGILE RAHVUSVAHELISES ÕIGUSES

Magistritöö

Juhendaja
Mag.jur Erki Kodar

Tartu
2015

Sisukord

Sissejuhatus

"It is going to take a true partnership between the private sector, the government and academia to address the challenges [of cyberspace]."[1]

2007. aasta aprillis ja mais, vahetult pärast Punaarmee sõjamonumendi ehk nn. Pronkssõduri teisaldamist Tallinna kesklinnast Kaitseväe kalmistule, pandi Eesti valitsusasutuste, suurimate pankade ning päevalehtede kodulehekülgede vastu toime suuremahulised teenusetõkestusrünnakud. 2008. aastal pärast Venemaa sissetungi Lõuna-Osseetiasse toimusid ulatuslikud teenusetõkestusrünnakud, mis olid suunatud Gruusia pankade, ajalehtede ja valitsusasutuste vastu.[2] 2008. aastal plahvatas Türgis torujuhe ning hilisema uurimise käigus selgus, et torujuhtme plahvatuse taga võis olla küberrünnak. Väidetavalt said häkkerid ligipääsu gaasitoru arvutisüsteemidele läbi gaasitoru valvanud turvakaamerate tarkvaras esinenud turvaaukude tõttu. Häkkeritel õnnestus välja lülitada kõik alarmid, lõpetada igasugune andmeedastus ja mõjutada torus olnud toornafta survet selliselt, et see ülesurve tõttu plahvatas.[3] 2010 aastal avastati Iraani, Indoneesia ning teiste riikide arvutitest keeruka ülesehitusega pahavara, mida kutsutakse Stuxnet'iks. Ussviirus Stuxnet mõjutas Iraani uraaniumi rikastamiseks kasutatud tsentrifuugide töösagedust ning selle tagajärjel said tsentrifuugid kahjustada ja Iraani tuumaprogrammi areng takerdus.[4] Ameerika Ühendriikide hinnangul suunati Ühendriikide valitsusasutuste vastu 2014. aastal kokku umbes 61 000 küberrünnakut.[5]

---

[1] Rogers, Michael. Hearing of the House (Select) Intelligence Committee on the subject of "Cybersecurity Threats: The Way Forward". Federal News Service: Washington D.C, 2014. Arvutivõrgus: https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf (04.05.2015).

[2] Economist. War in the Fifth Domain. The Economist, 1. juuli 2010. Arvutivõrgus: http://www.economist.com/node/16478792 (04.05.2015).

[3] Robertson, Jordan; Riley, Michael A. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. Bloomberg, 10. detsember 2014. Arvutivõrgus: http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar (04.05.2015).

[4] David E. Sanger, Obama Order Sped Up Wave of Cyberatacks Against Iran, New York Times, 1. juuni 2012. Arvutivõrgus: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. (04.05.2015)

[5] Berman Russell. The U.S. Government Is Under (Cyber) Attack. The Atlantic. 17. november 2014. Arvutivõrgus: http://www.theatlantic.com/politics/archive/2014/11/the-government-is-under-cyber-attack/382859/ (04.05.2015).

Valitsusasutuste küberintsidentide hulk kasvas aastatel 2010-2013 kolmkümmend viis protsenti.[6]

Eelnev näitab teravalt, et erinevat tüüpi küberründed riikide vastu on praktikas levinud, neid kasutatakse üha rohkem erinevate majanduslike- ja poliitiliste eesmärkide saavutamiseks ning on vähetõenäoline, et see tendents lähitulevikus muutuks. Termini "küberrünnak" all mõeldakse igasugust kübermaailmas toimepandud rünnakut, millega püütakse õõnestada vastase arvutivõrgu toimimist poliitilistel või rahvusliku julgeoleku eesmärkidel. See definitsioon hõlmab endas nii rünnakuid, mida võib pidada relvastatud rünnakuks kui ka madala intensiivsusega rünnakuid. Samas jääb definitsiooni alt välja rünnakud mida panevad toime mitteriiklikud kuritegelikud rühmitused oma erahuvides või riikide küberspionaaž.

Rahvusliku julgeoleku ning rahvusvahelise turvalisuse tagamiseks peab olema võimalik vastutusele võtta küberrünnakute organiseerijad, koordineerijad ning läbiviijad. Eriti oluline on vastutuse küsimus kui küberrünnakute taga on riigid, sest sellised rünnakud mõjutavad oluliselt rahvusvahelist ekviliibriumi. Riigid on oma olemuselt abstraktsioonid, mistõttu ei ole võimelised iseseisvalt käituma. Riik saab käituda üksnes läbi enda esindajate ja agentide. Otsese omistamise doktriin tähendabki juriidilist protseduuri, mille käigus tuvastatakse, kas näiteks konkreetse küberrünnaku elluviija ja riigi vahel on seesugune seos, et oleks võimalik väita, et kõnealune küberrünnak pandi toime riigi poolt.

Omistamist reguleerivad riigivastutuse artiklite eelnõu artiklid 4-11. Riigivastutuse artiklid on kodifitseeritud tavaõiguse normid ning nende kehtivust on tunnustatud rahvusvaheliste kohtute ja tribunalide poolt. ÜRO Peaassamblee kiitis 2001. aastal resolutsioonis nr 56/83 riigivastutuse artiklid heaks. Riigivastutuse artiklites sätestatud omistamisreeglite vaikivaks lähtepunktiks on, et rahvusvahelise õiguse rikkumised, mille omistamisega tegeletakse toimusid füüsilises maailmas. Küberrünnakud ei leia aga aset reaalses maailmas, vaid kübermaailmas ning seetõttu puuduvad küberrünnakutel ka traditsiooniliste rünnakute tüüpilised omadused.[7]

Kui reaalses maailmas toimunud rünnakute puhul tuvastab riik A, et tema vastu toimepandud rünnaku lähtekohaks on riigi B sõjaväeüksus, siis on riigi A vastu toimepandud rünnakute omistamine riigile B tõenäoline. Küberrünnakute kontekstis on reaalse koha, kust rünnak

[6] Frates, Chris; Devine, Curt. Government Hacks and Security Breaches Skyrocket. Cable News Network, 19. detsember. 2014. Arvutivõrgus: http://edition.cnn.com/2014/12/19/politics/government-hacks-and-security-breaches-skyrocket/ (04.05.2015).

[7] Brenner, Susan. "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare. The Journal of Criminal Law & Criminology, Volume 97, Issue 2, 2007, lk 409.

pärines, tuvastamine ründaja kindlaksmääramisel on märksa ebaolulisem, sest isegi kui küberrünnaku ohverriik tuvastab, et rünnak tuleb (suure tõenäosusega) riigi B sõjaväele kuuluvast serverist, siis see ei tähenda automaatselt, et rünnaku taga on tingimata riigi B sõjavägi. Küberrünnakute toimepanijatel on väga mitmeid erinevaid võimalusi, kuidas varjata oma asukohta või võltsida andmeid nii, et jätta mulje, et küberrünnak tuleneb ükskõik millisest kolmandast riigist.

Võttes arvesse, et küberrünnakud erinevad oma olemuselt traditsioonilistest rahvusvahelise õiguse vastastest tegudest, on käesoleva magistritöö keskseks küsimuseks, kas praegu kehtivaid riigivastutuse artiklites sisalduvaid omistamise norme on võimalik rahuldavalt kohaldada küberrünnaku kontekstis või mitte? Kui esimesele küsimusele on vastus eitav, siis tuleb küsida, millises viisil on võimalik riikide vastutust küberrünnakute kontekstis kehtestada?

Erialakirjanduses on suurt tähelepanu pööratud küsimusele, kas ja millistel tingimustel on küberrünnakud jõu kasutamine ÜRO harta artikkel 2 lõige 4 mõttes ning millal on küberrünnakud relvastatud rünnakud, mille korral on riikidel õigus enesekaitsele ÜRO harta artikli 51 alusel.[8] Omistamise problemaatikaga on tegeletud palju vähem ning täielikku üksmeelt selle osas, kas ja kuidas küberrünnakute omistamise doktriin suhestub teiseste omistamise reeglitega. Küberrünnakute omistamine on keeruline ülesanne, mis hõlmab endas nii tehnilisi kui ka õiguslikke külgi. Käesolevas töös keskendutaksegi üksnes omistamisele ja magistritöö piiratud mahtu ning fookust arvesse võttes ei tegeleta küsimusega, milliseid küberrünnakuid saab pidada jõu kasutamiseks ja milliseid mitte. Autor ei proovi ka anda ammendavat vastust küsimusele, milline küberrünnak on rahvusvahelise õiguse vastane tegu riigivastutuse artiklite eelnõu artikli 2 mõttes.

Töös kasutatakse peamiselt analüüsivat ja kirjeldavat meetodit. Võrdlevat meetodit kasutatakse erinevate õiguskirjanduses valitsevate seisukohtade kõrvutamiseks. Töös on allikatena

[8] Vt nt: Schmitt, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, Volume 37, Issue 3, 1999; Barkham, Jason. Information Warfare and International Law on the Use of Force. New York University Journal of International Law and Politics, Volume 34, Issue 1, 2001; Schmitt, Michael N. Cyber Operations and the Jus Ad Bellum Revisited. Villanova Law Review, Volume 56, Issue 3, 2011; Georgiades, Eugenia; Caelli, William J.; Christensen, Sharon; Duncan, W.D. Crisis On Impact: Responding to Cyber Attacks on Critical Information Infrastructures, Journal of Information, Technology & Privacy Law, Volume 30, 2013; Jensen, Eric Talbot. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, Stanford Journal of International Law, Volume 38, Issue 2, 2002; Waxman, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). Yale Journal of International Law, Volume 36, Issue 2, 2011; Hoisington, Matthew. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. Boston College International and Comparative Law Review, Volume 32, Issue 2, 2009.

kasutatud põhiliselt Ameerika Ühendriikide ning Euroopa õigusteadlaste artikleid, rahvusvahelist kohtupraktikat ning õigusaktide kommentaare ja nende *travaux préparatoires*.

Magistritöö ülesehitus lähtub töö hüpoteesist. Esimeses peatükis uuritakse rahvusvahelises õiguses kehtivate omistamisreeglite sisu üldiselt. Esmalt käsitletakse riigivastutuse õiguse ja omistamisreeglite ajaloolist kujunemist ja sisu. Seejärel analüüsitakse omistamisreegleid üldiselt ning viimaks käsitletakse omistamise tõendamisega seonduvaid küsimusi.

Teises peatükis suundutakse konkreetsemalt küberrünnakute poole. Selles peatükis käsitletakse esmalt natukene põhjalikumalt küberrünnaku definitsiooni, seejärel uuritakse küberrünnakute liike ning viimaks analüüsitakse omistamise tehnilisi väljakutseid.

Kolmandas peatükis käsitletakse küberrünnakute omistamist. Kolmanda peatüki esimeses alapeatükis hinnatakse küberrünnakute omistamise võimalust riigile, teises alapeatükis analüüsitakse mitteriiklike üksuste poolt elluviidud küberrünnakute omistamist ning viimasena uuritakse kaudse vastutuse kohaldamist küberrünnakute kontekstis.

1. Omistamine

1.1. Riigivastutuse doktriini areng

1.1.1. Ajalooline areng

Riikide vastutus on tänapäevase rahvusvahelise õiguse aluspõhimõte, mis tuleneb rahvusvahelise õigussüsteemi olemusest ning riikide suveräänsuse ja võrdsuse doktriinidest.[9] Hoolimata sellest, et tänaseks on riikide vastutus muutunud rahvusvahelise õiguse lahutamatuks osaks, siis pikka aega ei pööratud sellele märkimisväärset tähelepanu. Varased autorid keskendusid pigem konkreetsete õigusharude nagu mereõiguse, sõjaõiguse ning diplomaatiliste suhete õiguse küsimustele ja iga valdkonna konkreetsete reeglite tuvastamisele. Isegi kui riikide vastutust käsitleti, siis üksnes juhuslikult ning süsteemitult, läbi iga konkreetse rahvusvahelise õigusharu prisma.[10]

Riikide vastutuse küsimust hakati süsteemselt käsitlema alles 19. sajandi lõpus ning 20. sajandi alguses. Märkimisväärseimad autorid sellest perioodist on Heinrich Triepel ja Dionisio Anzilotti. Saksa õigusteadlase Heinrich Triepeli teos "*Völkerrecht und Landesrecht*" ilmus 1899. aastal ja see käsitles mõningaid tänapäevase riigivastutuse doktriini küsimusi nagu näiteks erinevate organite, sealhulgas indiviidide, riigiorganite ning avalik-õiguslike juriidiliste isikute tegude omistamist riigile ja föderatsiooni subjektide tegude omistamist föderatsioonile.[11] Anzilotti tegeles peamiselt riigi vastutusega välismaalastele põhjustatud kahju eest,[12] kuid kõige olulisemaks võib pidada tema panust omistamise kriteeriumide sõnastamisel.[13] Anzilotti leidis, et tuleb eristada indiviidi tegusid ja selle riigi rahvusvahelisi kohustusi, kelle nimel indiviid käitub. Riigi vastutus ei järgne mitte üksikisiku teole vaid üksnes siis kui see rikub riigile kuuluvat rahvusvahelisest õigusest tulenevat kohustust.[14] Anzilotti tõi välja ka riigi vastutust välistavad asjaolud, mille esinemisel riik õigusvastase teo

[9] Shaw, Malcolm N. International Law, 6th edition. Cambridge [etc.]: Cambridge University Press, c2008, 2011, lk 778.

[10] Crawford, James. State Responsibility. The General Part. New York; Cambridge: Cambridge University Press, 2013, 2014, lk 3.

[11] Crawford, James. State Responsibility, lk 22.

[12] Crawford, James. State Responsibility, lk 23.

[13] Dupuy, Pierre-Marie. Dionisio Anzilotti and the Law of International Responsibility of States. European Journal of International Law, Vol. 3, Issue 1, 1992, lk 143.

[14] Dupuy, Pierre-Marie. Dionisio Anzilotti and the Law of International Responsibility of States, lk 143.

toimepanemise eest ei vastuta ning vastutuse kohaldamise tagajärjed.[15] Triepeli ja Anzilotti nägemus riigivastutusest kui eraldiseisvast teemast muutus laialdaseks ning riigivastutuse doktriini hakati neist seisukohtadest mõjutatuna rohkem uurima.

1.1.2. Riigivastutuse kodifitseerimine

1924. aastal tegi Rahvasteliidu Täiskogu ettepaneku, et Rahvasteliidu Nõukogu kutsuks kokku ekspertide komisjoni, kes muuhulgas tuvastaks, millistes rahvusvahelise õiguse küsimustes oleks rahvusvahelise kokkuleppe saavutamine kõige ihaldatum ning võimalikum.[16] Rahvusvahelise Õiguse Progressiivse Kodifitseerimise Ekspertide Komisjon kohtus esmakordselt 1925. aastal, kus valiti algselt välja üksteist rahvusvahelise õiguse küsimust. Riigi vastutus välismaalastele ja nende varale põhjustatud kahju eest osutus üheks valitud teemaks. Iga Ekspertide Komisjoni poolt väljavalitud teemaga tegelemiseks loodi eraldi alamkomisjon, kelle ülesanne oli teha riikide seas eeluuring, kas riikide arvates tuleks konkreetset küsimust reguleerida rahvusvahelise õigusega või mitte. Kakskümmend viis vastanud riiki nõustusid, et riikide vastutust tuleks rahvusvahelisel tasandil kodifitseerida, viis vastanut arvasid, et kodifitseerimine on vajalik aga teatud reservatsioonidega ning vaid neli vastajat arvasid, et riikide vastutuse normide kodifitseerimine ei ole võimalik ega kohane. Analüüsides saadud vastuseid leidis riigivastutuse alamkomisjon, et aeg on küps rahvusvahelise riigivastutuse konventsiooni loomiseks.[17]

1927. aastal toimus Rahvasteliidu täiskogu istung, kus võeti vastu resolutsioon korraldada rahvusvaheline konverents kolme küsimuste kodifitseerimiseks: kodakondsus, territoriaalveed ja riigi vastutus välismaalastele ja nende varale põhjustatud kahju eest. Loodi konverentsi ettevalmistav komisjon, kelle ülesanne oli uurida kõiki kolme eelnimetatud teemat ning koostada oma uurimistulemuste kohta raportid. Riigi vastutuse välismaalastele ja nende varale põhjustatud kahju kohta koostatud raportid sisaldasid tänaseks juba omaseks saanud põhimõtteid nagu näiteks, riik ei saa tugineda siseriiklikule õigusele, et välistada rahvusvahelist vastutust ning riigi vastutus rahvusvahelisel tasandil võib tõusetuda nii seadusandliku,

[15] Crawford, James. State Responsibility, lk 24.

[16] Ago, Roberto. First report on State responsibility by Mr. Roberto Ago, Special Rapporteur - Review of previous work on codification of the topic of the international responsibility of States. Yearbook of the International Law Commission, 1969, Volume 2, United Nations: New York, 1970, lk 131. Arvutivõrgus: http://legal.un.org/ilc/documentation/english/a_cn4_217.pdf (04.05.2015).

[17] Ago, Roberto. First report on State responsibility by Mr. Roberto Ago, Special Rapporteur, lk 131.

täidesaatva kui ka kohtuvõimu teostamisel.[18]

1930. aastal toimus Haagis I rahvusvahelise õiguse kodifitseerimise konverents. Kolme konverentsi teema jaoks loodi kolm komisjoni. Riigivastutuse komisjon leidis üksmeele teatud küsimustes, kuid suured eriarvamused tekkisid seoses välismaalaste kohtlemisega seonduvates põhimõtetes. Välismaalaste kohtlemise küsimus oli aga riigivastutuse küsimusega väga tihedalt seotud, mistõttu ei olnud komisjonil võimalik ka üksnes riigi vastutuse üldpõhimõtetega tegeleda. Suurte sisuliste eriarvamuste ning ajapuuduse tõttu ei saanud riigivastutuse komisjon võtta kodifitseerimise küsimuse osas mingit seisukohta.[19]

Vahemärkusena tuleb mainida, et eksisteerisid ka mõned eraalgatuslikud kodifitseerimiskatsed. Kõige olulisemaks neist on Harvardi ülikooli poolt 1929. aastal koostatud riigivastutuse kodifikatsioon. Selle olulise täiendamisega alustati uuesti 1956. aastal ning kui kodifikatsioon 1961. aastaks valmis sai, siis oli tegemist sisuliselt täiesti uue versiooniga.[20] See 1961. aasta uus Harvardi kodifikatsioon oli oluline allikas Rahvusvahelise Õiguse Komisjoni poolt riigivastutuse sätete koostamisel.

Riigivastutuse küsimus jäi mõneks ajaks tagaplaanile, kuni 1947. aastal loodud Rahvusvahelise Õiguse Komisjon alustas 1956. aastal uuesti riigivastutuse kodifitseerimisega. Riigivastutuse teema eriraportööriks valiti Francisco V. García-Amador, kes esitas aastatel 1956-1961 Rahvusvahelise Õiguse Komisjonile kokku kuus raportit, mis hõlmasid riikide vastutuse artiklite täielikku eelnõud.[21] Eriraportöör García-Amador keskendus üksnes riigi vastutusele välismaalastele ja nende varale põhjustatud kahju eest, sest seda peeti tol ajal üldiselt kõige rohkem väljaarenenumaks riigivastutuse valdkonnaks ning selles küsimuses oli juba olemas ka hulgaliselt rahvusvaheliste vahekohtute praktikat.[22] Eriraportöör García-Amadori käsitluse rõhuasetus oli suunatud põhiliselt riigi kohustusele hüvitada tekitatud kahju. Tema käsitluse järgi ei tulenenud riigi kohustus hüvitada tekitatud kahju mitte riigi poolt rahvusvahelise

[18] Crawford, James. State Responsibility, lk 31.

[19] Ago, Roberto. First report on State responsibility by Mr. Roberto Ago, Special Rapporteur, lk 132.

[20] Ago, Roberto. First report on State responsibility by Mr. Roberto Ago, Special Rapporteur, lk 128.

[21] Crawford, James; Pellet, Alain; Olleson, Simon; Parlett, Kate (toim). The Law of International Responsibility. Oxford [etc.]: Oxford University Press, 2010, lk 69.

[22] Crawford, James jt. The Law of International Responsibility, lk 70.

kohustuse rikkumisest vaid vastutus tõusetus üksnes üksikisikute õiguste rikkumisest.[23] Eriraportöör García-Amadori riigivastutuse artiklite eelnõu artikkel 21 nägi isegi ette üksikisikutele võimaluse oma kahjunõudega pöörduda teise riigi vastu selleks riikidevahelise lepinguga loodud rahvusvahelise tribunali poole.[24]

Omistamisele oli eriraportöör García-Amadori eelnõus pühendatud artiklid 12-16. Nende artiklite ülesehitus oli sarnane täna kehtivatele – riigile on omistatavad on tema organite teod ja tegematajätmised, k.a. teod *ultra vires* (artikkel 12), seadusandluse (artikkel 13) ning riigi allüksuste teod (artikkel 14) ja mässuliste teod, kellel õnnestus korralda riigipööre (artikkel 16). Artikkel 15 sätestas, et riigi territooriumil asuva kolmanda riigi organite või rahvusvaheliste organisatsioonide teod on asukohariigile omistatavad üksnes juhul kui riik oleks saanud kahju tekitamist ära hoida, kuid hooletusest seda ei teinud.[25]

Eriraportöör García-Amadori koostatud raportid said väga laialdast kriitikat ja Rahvusvahelise Õiguse Komisjon esitatud raportitega sisuliselt ei tegelenudki,[26] viidates vajadusele tegeleda muude küsimustega nagu arbitraažimenetlus ning diplomaatilised- ja konsulaarsuhted.[27] Neid raporteid ei kasutatud Rahvusvahelise Õiguse Komisjoni poolt ka edasise kodifitseerimise allikatena.

Pärast eriraportöör García-Amador lahkumist Rahvusvahelise Õiguse Komisjonist 1962. aastal, otsustas Rahvusvahelise Õiguse Komisjon alustada taaskord riikide vastutuse küsimusega, kuid nüüd keskenduda vähem riikide poolt välismaalastele põhjustatud kahjule ja rohkem üldiste riikide rahvusvahelise vastutuse reeglite defineerimisele.[28] 1963. aastal määrati uueks eriraportööriks Roberto Ago, kes esitas aastatel 1969-1980 kokku kaheksa raportit. Ago koostatud riigivastutuse artiklite eelnõu üheks olulisemaks uuenduseks võib pidada vastutuse

[23] García-Amador, Francisco V. International responsibility: Sixth report by F. V. Garcia Amador, Special Rapporteur. Yearbook of International Law Commission 1961, Volume 2, United Nations: New York, 1962, lk 46. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1961_v2_e.pdf.

[24] García-Amador, Francisco V. International responsibility: Sixth report by F. V. Garcia Amador, Special Rapporteur, lk 49.

[25] García-Amador, Francisco V. International responsibility: Sixth report by F. V. Garcia Amador, Special Rapporteur, lk 52.

[26] Crawford, James jt. The Law of International Responsibility, lk 72.

[27] Report of the Commission to the General Assembly. Report of the International Law Commission on the work of its twenty-first session, 2 June-8 August 1969. Yearbook of the International Law Commission 1969, Volume 2, United Nations: New York, 1970, lk 229, para. 67. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes(e)/ILC_1969_v2_e.pdf.

[28] Crawford, James. State Responsibility, lk 36.

eristamist selle tagajärgedest – riikide rahvusvahelist vastutust ei käsitletud enam üksnes riigi kohustusena maksta reparatsioone.[29] Teiseks oluliseks muudatuseks võib pidada vastutuse tekkimise aluse sidumist kohustuse rikkumisega ja mitte kahju tekitamisega.[30] See põhimõte sai rahvusvaheliselt laialdast heakskiitu ning Ago poolt välja pakutud artikkel 1, mis sätestab, et "iga rahvusvahelise õiguse vastane tegu toob endaga kaasa rahvusvahelise vastutuse", on jäänud tänaseni muutmatu sõnastusega riigivastutuse artiklite osaks. Rahvusvahelise Õiguse Komisjon võttis aastatel 1973-1981 esialgselt vastu 35 artiklit ja need sätted moodustasid riigivastutuse eelnõu esimese osa.

Ago eelnõus pühendati omistamisele artiklid 5-13. Riigile on omistatavad tema riigiorganite teod (artikkel 5), hoolimata nende positsioonist riigisiseses hierarhias (artikkel 6), riigi autonoomsete üksuste teod (artikkel 7), avalikke funktsioone täitvate isikute teod, kes siiski ei kuulu ametlikult riigiorganite hulka (artikkel 8), riigi käsutusse antud kolmanda riigi või rahvusvahelise organisatsiooni organite teod (artikkel 9),[31] riigiorganite *ultra vires* teod (artikkel 10), ning teod, mille on toime pannud ülestõusmisliikumise osalised, kes on muutunud riigipöörde tulemusena riigiorganiteks (artikkel 13). Riigile ei ole omistatavad eraisikute teod (artikkel 11) ja teiste rahvusvahelise õiguse subjektide organite teod (artikkel 12).[32]

Aastatel 1988-1996 tegeles Rahvusvahelise Õiguse Komisjon eelnõu teise ja kolmanda osaga ning 1996. aastal toimus riigivastutuse artiklite eelnõu esimene lugemine. Esimesel lugemisel tõusetus mitmeid probleeme, mida püüti aastatel 1997-2001 lahendada – artikleid sõnastati ümber ja lühendati, mõningad problemaatilisemad artiklid jäeti lõplikust tekstist üldse välja.[33] Kuigi omistamise artiklite sõnastust muudeti selle aja jooksul oluliselt, siis nende sisu jäi praktiliselt muutumatuks võrreldes eriraportöör Ago poolt väljapakutuga.

Riikide vastutuse artiklite eelnõu võeti Rahvusvahelise Õiguse Komisjoni poolt lõpuks vastu

[29] Crawford, James jt. The Law of International Responsibility, lk 77.

[30] Crawford, James jt. The Law of International Responsibility, lk 78.

[31] Ago, Roberto. Third report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The internationally wrongful act of the State, source of international responsibility. Yearbook of the International Law Commission, 1971, Volume 2, Part one, lk 233 jj. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1971_v2_p1_e.pdf (04.05.2015).

[32] Ago, Roberto. Fourth report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The internationally wrongful act of the State, source of international responsibility. Yearbook of the International Law Commission, 1972, Volume 2, United Nations: New York, 1974, lk 72 jj. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1972_v2_e.pdf (04.05.2015).

[33] Crawford, James jt. The Law of International Responsibility, lk 84.

31. mail 2001 aastal ning 12. detsembril 2001 aastal lisas ÜRO peaassamblee artiklite teksti ka oma resolutsioonile nr 56/83. ÜRO peaassamblee pidi otsustama, kas riigivastutuse artiklid võetakse vastu peaassamblee otsusega või koostatakse artiklitele tuginedes rahvusvaheline konventsioon, kuid selles küsimuses pole siiani ühist seisukohta leitud ning alates 2004. aastast on igal peaassamblee istungil otsustatud selle küsimuse lõplik otsustamine edasi lükata. Sellest hoolimata on riigivastutuse artiklid muutunud rahvusvaheliselt üldtunnustatuks ning sätted moodustavad lahutamatu osa tänasest rahvusvahelise õiguse süsteemist.

1.2. Omistamise doktriin rahvusvahelises õiguses

Varasem riigivastutuse doktriin koosnes kolmest põhilisest elemendist, milleks olid rahvusvaheliselt õigusvastase teoga kahju põhjustamine, selle teo omistatavus riigile ning riigi kohustus hüvitada tekitatud kahju. Kahju hüvitamise kohustus ei olnud traditsioonilise käsitluse järgi mitte üksnes riigi vastutuse üheks tagajärjeks, vaid riigi vastutus tähendaski kohustust hüvitada kahju.[34]

Tänapäevases käsitluses on riikide vastutuse doktriinil kaks elementi: rahvusvaheliselt õigusvastane tegu ja selle omistatavus riigile. Riigivastutuse artiklite artikli 1 kohaselt toob iga rahvusvahelise õiguse vastane tegu endaga kaasa rahvusvahelise vastutuse. Riigivastutuse artiklite artikkel 2 sätestab riigivastutuse kahe-elemendilise struktuuri, mille kohaselt on tegu rahvusvahelise õiguse vastane, kui käitumine, mis koosneb teost või tegevusetusest, on riigile omistatav ning see rikub riigi rahvusvahelist kohustust.

Juba Alaline Rahvusvaheline Kohus sedastas, et riikide rahvusvaheline vastutus tekib kui tegu on riigile omistatav ning see tegu rikub teise riigi lepingust tulenevaid õigusi.[35] Rahvusvaheline Kohus leidis Tehrāni kaasuses, et esmalt peab Rahvusvaheline Kohus tuvastama, millised Iraanile etteheidetavad teod on Iraanile omistatavad ning alles siis on Rahvusvahelisel Kohtul võimalik tuvastada, kas need teod rikkusid riigile teatud lepingutest tulenevaid rahvusvahelisi kohustusi.[36] Sellest nähtub, et juhul kui etteheidetavad teod ei ole riigile omistatavad, siis ei ole võimalik jätkata küsimusega, kas riik kõnealuste tegude eest vastutab. Oluline on märkida, et Rahvusvaheline Kohus muutis Bosnia Genotsiidi lahendis oma varasemat lähenemist. Bosnia Genotsiidi lahendis tegeles Kohus esmalt rikkumiste tuvastamisega ja alles siis hindas, kas

[34] Crawford, James jt. The Law of International Responsibility, lk 194.

[35] Phosphates in Morocco Case, (1938) P.C.I.J., Ser. A/B, No. 74, lk 22.

[36] United States Diplomatic and Consular Staff in Tehran, Judgment, I.C.J. Reports 1980, p. 3, lk 29-30, para. 56. Arvutivõrgus: http://www.icj-cij.org/docket/files/64/6291.pdf.

toimepandud teod on Jugoslaavia Liitvabariigile omistatavad.[37] Rahvusvahelise Kohtu kohtuniku ja Rahvusvahelise Õiguse Komisjoni endise eriraportööri James Crawfordi arvates võis sellise "ümberpööratud" lähenemise kasutamist Bosnia Genotsiidi kohtuasjas õigustada vajadusega dokumenteerida esmalt kõik sõjakoledused, hoolimata sellest, et nende ametlik omistamine riigile ei pruugi olla võimalik.

Riigivastutuse artiklite artikkel 2 sätestab sätestab, et riigi vastutus koosneb kahest elemendist, kuid riigivastutuse artiklite viies peatükk sätestab olukorrad, millal riigi vastutus toimepandud tegude eest on välistatud. See tähendab, et isegi siis kui riik on rikkunud mõnda rahvusvahelist kohustust ja see rikkumine on riigile omistatav, kuid esineb mõni viiendas peatükis toodud asjaolu, siis riik rahvusvahelise õiguse rikkumise eest ei vastuta. Sellest tulenevalt saab väita, et tänapäevane riikide vastutuse doktriin koosneb siiski kolmest elemendist, milleks on õigusvastane tegu, selle omistatavus riigile ning vastutust välistavate asjaolude puudumine.[38]

Omistamise problemaatika tõusetub esmajoones asjaolust, et mitte ükski rahvusvahelise õiguse subjektidest, riik või rahvusvaheline organisatsioon, ei ole võimeline käituma iseseisvalt. Riigid saavad tegutseda vaid oma agentide ning esindajate poolt ja kaudu[39] ning rahvusvahelise õiguse jaoks on oluline küsimus, kas konkreetse agendi või esindaja tegu on riigi tegu rahvusvahelise õiguse tähenduses. Omistamine on seega termin, mis tähendab õiguslikku operatsiooni, mille funktsioon on teha kindlaks kas ükskõik millist füüsilise isiku tegevust või tegevusetust saab pidada riigi tegevuseks.[40] See, kas omistamise näol on tõepoolest tegemist õigusliku operatsiooniga või pelgalt faktilise olukorra tuvastamisega on olnud õiguskirjanduses teatava vaidluse all. Rahvusvahelise Õiguse Komisjoni riigivastutuse teema eriraportöör Gaetano Arangio-Ruiz nägemuse järgi on omistamisele õigusliku tähenduse andmine ekslik ja üleliigne. Ekslik seetõttu, et sellel puudub lähtepunkt rahvusvahelises õiguses ning üleliigne seetõttu, et see dubleerib rahvusvahelise õiguse vastase teo tuvastamist ning vastutuse määramist.[41]

---

[37] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43. Arvutivõrgus: http://www.icj-cij.org/docket/files/91/13685.pdf.

[38] Crawford, James jt. The Law of International Responsibility, lk 224.

[39] German Settlers in Poland, (1923) P.C.I.J., Series B, Advisory Opinion No. 6. On 3 February 1923, lk 22. Arvutivõrgus: http://www.icj-cij.org/pcij/serie_B/B_06/Colons_allemands_en_Pologne_Avis_consultatif.pdf (04.05.2015).

[40] Crawford, James jt. The Law of International Responsibility, lk 221.

[41] Gaetano Arangio-Ruiz. Second report on State responsibility, by Mr.Gaetano Arangio-Ruiz, Special Rapporteur. Yearbook of the International Law Commission, 1989, Volume II (Part I), United Nations: New York, 1992, lk

Omistamine tähendab sisuliselt kriteeriumite kogumit, mis peavad olema täidetud, et oleks võimalik öelda, kas konkreetse rahvusvahelise õiguse vastase teo on toime pannud riik või mitte. Kui omistamise reeglite alusel hinnatakse, et tegu on riigile omistatav, siis vastutab teo eest riik ning teo tegelik toimepanija muutub ebaoluliseks. Teo tegelik toimepanija on sellisel juhul vaid "tööriist", mille kaudu riik oma tahet ellu viib.[42] Omistamise doktriini kohaldatakse siiski laiemalt kui üksnes riigivastutuse kitsas raamistikus ning omistamise küsimus võib tõusetuda põhimõtteliselt ükskõik millisest riigi tegevusest, millel on mingisugune juriidiline tähendus, kuid mis ei pea olema "rahvusvahelise õiguse vastane tegu".[43] Näiteks on võimalik omistamise doktriini kasutada, et hinnata, kas mingisuguse rahvusvahelise lepingu allkirjastamine riigi esindaja poolt toob kaasa riigile teatud juriidilisi kohustusi kui riigiesindajal, kes lepingu allkirjastas, ei olnud siseriikliku õiguse alusel selleks pädevust.[44]

Rahvusvahelise Õiguse Komisjon piirdus riigivastutuse artiklite eelnõu koostamisel üksnes rahvusvahelise õiguse teiseste reeglite sõnastamisega. Riigivastutuse sätted ei püüa reguleerida riikide rahvusvahelisi kohustusi, vaid üksnes näeb ette üldisemad teisesed reeglid, mis kohalduvad juhul, kui riik on rikkunud oma rahvusvahelisi kohustusi ja mis näevad riigile selle kohustuse rikkumise eest vastutuse ning heastamisvahendid.[45] Sellest lähtuvalt on riigivastutuse artiklites sätestatud omistamisreegleid võimalik kohaldada ühetaoliselt põhimõtteliselt kõikidele rahvusvahelise õiguse esmastele normidele.[46] Üldistatult võib öelda, et primaarnormid kehtestavad riikidele kohustusi rahvusvahelise kogukonna ees ning teisesed normid näevad ette tagajärjed, mis järgnevad esmaste normide rikkumisele.[47] Esmaste ja teiseste normide eristamine on siiski pälvinud teatavat kriitikat. Mitmed autorid on leidnud, et esmaste ja teiseste reeglite eristamine on üksnes abstraktne ja isegi kunstlik. Kriitikud on

---

51, para. 175. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1989_v2_p1_e.pdf (04.05.2015).

[42] Crawford, James jt. The Law of International Responsibility, lk 221.

[43] Crawford, James jt. The Law of International Responsibility, lk 222.

[44] Vt nt: Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea intervening), Judgment, I.C.J. Reports 2002, p. 30, lk 131-132, paras. 265-268. Arvutivõrgus: http://www.icj-cij.org/docket/files/94/7453.pdf (04.05.2015).

[45] Bodansky, Daniel; Crook, John R. Symposium: The ILC's State Responsibility Articles. Introduction and Overview. American Journal of International Law, 96 (2002), lk 773.

[46] Crawford, James jt. The Law of International Responsibility, lk 224-225.

[47] Ago, Roberto. Second report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The origin of international responsibility. Yearbook of International Law Commission, 1970, Volume 2, United Nations: New York, 1972, lk 179. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/ Ybkvolumes%28e%29/ILC_1970_v2_e.pdf.

seisukohal, et teisestel omistamisreeglitel puudub igasugune praktiline tähendus, sest teo omistamine on lahutamatult seotud rikutud materiaalõiguse primaarnormiga ning teo omistamiseks tehtav õiguslik operatsioon võib võtta väga erinevaid vorme sõltuvalt rikutud normist. [48]

Eriti teravalt tõusetub esmaste ja teiseste normide eristamise probleemistik juhul, kui riigile heidetakse ette rahvusvahelise kohustuse rikkumist tegevusetusega.[49] Selleks, et tuvastada, kas riigi agentide tegevusetust saab riigile omistada, tuleb esmajoones tuvastada, kas riigil üldse oli kohustus tegutseda ja mida selline aktiivse tegutsemise kohustus endas täpselt hõlmab rahvusvahelise õiguse alusel.[50] Tegutsemiskohustus ja selle sisu tuleb primaarnormist, mistõttu teisese omistamisnormi kohaldamine muutub asjakohatuks. Lisaks võib mõningatel puhkudel võib esmase normiga kaasneda ka selle normiga lahutamatult seotud omistamise reegel, kuid selliste normide olemasolu on pigem erandlik.[51] Hoolimata teatavast kriitikast esmaste ja teiseste normide eristamise aadressil on riikide praktika näidanud, et normide eristamine esmasteks ja teisesteks on pälvinud rahvusvahelisel areenil laialdase tunnustuse. Näiteks Suurbritannia ning Prantsusmaa vaheline Eurotunneli arbitratsioonivaidlus põhineski suuresti üksnes esmaste ja teiseste normide eristamise küsimusel. [52] Seega hoolimata teatud õigusteadlaste poolt esitatud kriitikast saab siiski suure kindlusega väita, et omistamisreeglite kodifitseerimine üksnes teisesete normidena on õigustatud.

Omistamise doktriin on tänastes riigivastutuse artiklites sätestatud kokku 8 artiklis ning sätted jagunevad sisuliselt kolmeks grupiks. Esimese grupi moodustavad artiklid 4-7, mis käsitlevad riigile tema organite ning agentide tegude omistamist ja neid artikleid võib pidada ka omistamise doktriini tüvireegliteks. Teiseks iseseisvaks kategooriaks võib pidada artiklit 8, mis käsitleb riigile tema organiteks või agentideks mitteolevate isikute tegude omistamist. Kolmandasse kategooriasse kuuluvad artiklid 9-11, mis tegelevad praktikas üsna

[48] Crawford, James jt. The Law of International Responsibility, lk 225.

[49] Crawford, James. First report on State responsibility, by Mr. James Crawford, Special Rapporteur. Arvutivõrgus: http://legal.un.org/ilc/documentation/english/a_cn4_490.pdf (04.05.2015).

[50] Crawford, James jt. The Law of International Responsibility, lk 225.

[51] Näiteks sätestab Ühinenud Rahvaste Organisatsiooni mereõiguse konventsiooni artikkel 139, et riik vastutab isiku poolt tekitatud kahju eest, kui ta on seda isikut toetanud ja ei ole võtnud kahju ärahoidmiseks konventsioonis ettenähtuid meetmeid.

[52] Gourgourinis, Anastasios. General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System. The European Journal of International Law, Volume 22, Issue 4, 2011, lk 1020.

harvaesinevate olukordadega, kus riigiorganiteks mitteolevate kolmandate isikute tegevus omistatakse riigile ilma, et riik otseselt seda tegevust oleks juhtinud või kontrollinud. Alljärgnevalt analüüsitaksegi neid artikleid põhjalikumalt.

1.3. Riigiorganite tegevuse omistamine

1.3.1 Riigi ametlikud organid

Nagu eelmises peatükis juba mainitud, mitte ükski rahvusvahelise õiguse subjektidest ei ole võimeline käituma iseseisvalt. Riigid kui poliitilised abstraktsioonid saavad tegutseda vaid oma agentide ja esindajate poolt ja kaudu.[53] Riigi vastutus tema organite tegevuse eest on rahvusvahelises õiguses üldtunnustatud põhimõte. See põhimõte on kodifitseeritud riigivastutuse artiklite artiklis 4 ning selle sätte kuulumist tavaõiguse normide hulka on Rahvusvaheline Kohus kinnitanud.[54]

Riigivastutuse artiklite artikkel 4 lõige 1 sätestab, et riik vastutab kõigi oma organite tegevuse eest, olenemata sellest, kas tegemist on täidesaatva-, seadusandliku- või kohtuvõimu esindaja teoga. Artikkel 4 lõige 2 sätestab, et termin "riigiorgan" hõlmab iga isikut või üksust, kellel on vastav staatus siseriikliku õiguse alusel. Selle sätte tähenduses on terminil "riigiorgan" laiem tähendus, ning see hõlmab nii organeid, mis kuuluvad riigistruktuuri hulka, kui ka territoriaalsed üksuseid, mis on siseriikliku õiguse alusel iseseisevad, kuid riigile allutatud.[55]

Riigile tema ametlike organite tegude omistamise jaoks ei ole võimude lahususe printsiibil tähtsust. Rahvusvahelise õiguse alusel vastutab riik üheselt näiteks nii oma relvajõudude tegevuse eest, parlamendi poolt vastuvõetud seaduste eest kui ka kohaliku omavalitsuse ametnike käitumise eest juhul kui need rikuvad mingit riigi rahvusvahelist kohustust. Kui näiteks siseriiklik kohus on võtnud vastu otsuse, mis rikub rahvusvahelist õigust, siis on selle omistamine riigile artikli 4 alusel võimalik ja rikkumise eest vastutab riik, ükskõik kui suur ka siseriikliku õiguse alusel kohtuvõimu autonoomia ei oleks.[56] Tähtsust ei ole ka sellel, kas teo toime pannud organil on rahvusvaheline (näiteks välisministeeriumi välissuhete osakond) või siseriiklik funktsioon (näiteks kohaliku omavalitsuse sotsiaalamet) või kas teo reaalselt toime

[53] German Settlers in Poland, P.C.I.J., Ser. B., No. 6, lk 22.

[54] Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion, I.C.J. Reports 1999, p. 62, lk 29, para 62. Arvutivõrgus: http://www.icj-cij.org/docket/files/100/7619.pdf (04.05.2015).

[55] Crawford, James jt. The Law of International Responsibility, lk 239.

[56] Crawford, James. State Responsibility: the General Part, lk 121.

pannud isik on selle struktuuriüksuse sees ülemus või alluv.[57] Samamoodi ei ole riigi rahvusvahelise vastutuse jaoks oluline millisteks allüksusteks on riigivõim jaotatud või kui iseseisvad need territoriaalsed allüksused on siseriikliku õiguse alusel.

1.3.2. Riigivõimu teostamiseks volitatud organid

Lisaks oma ametlike organite tegevuse eest vastutamisele, vastutab riik ka isikute eest, keda ta on volitanud riigivõimu teostama, kuid kes ei ole riigi ametlik organ, juhul kui isik või üksus käitus talle antud volituste raames (artikkel 5). Artiklis 5 sätestatud omistamisreeglit saab kohaldada seega nii avalik-õiguslikele üksustele, osaliselt avalik-õiguslikele üksustele kui ka erinevatele avalik-õiguslikele agentuuridele ja teatud puhkudel ka eraõiguslikele juriidilistele isikutele.[58] Samas ei ole riigile omistatav kõikide ettevõtete tegevus, kus riik omab osalust või mis on mingil moel riigi kontrolli all (näiteks kui ettevõtte nõukogus kuulub häälteenamus riigi poolt määratud isikutele). Osalus ja kontroll on asjaolud, mida võib pidada usaldusväärseteks indikaatoriteks, et ettevõtte poolt toimepandud rahvusvahelise õiguse rikkumisi on võimalik riigile omistada, kuid need ei võimalda siiski ettevõtte tegevuse automaatset riigile omistamist.[59]

Artiklis 5 ei ole defineeritud, mida täpselt kasutatud termin "riigivõim" hõlmab, kuid riigivastutuse artiklite eelnõu kommentaaride kohaselt tuleb selle termini sisustamisel lähtuda konkreetse riigi ajaloost, traditsioonidest ja ühiskondlikust korraldusest. Selleks, et tuvastada, kas riigi poolt isikule või organile antud volituse näol on riigivõimu teostamise üleandmisega, tuleks lisaks ka küsida, kas tavapäraselt on konkreetne tegevus riiklik ülesanne või mitte. Kui mingit tegevust võib teostada igaüks, ilma riigiorganitelt vastava loa või volituse saamiseta, siis ei pruugi olla tegemist riigivõimu teostamisega. Siinkohal saab kasutada ka immuniteediteooriast tuntud eristust, mille kohaselt tegudele *iure imperii* kohaldatakse immuniteedireegleid ning tegudele *iure gestionis* immuniteet ei kohaldu. See aga ei tähenda, et tegemist oleks absoluutse reegliga - näiteks ei ole turvateenuse osutamine kõrgele ametiisikule *acta iure imperii*, kuid teatud puhkudel võib sellise teenuse osutamisel toime pandud tegusid

[57] Crawford, James. The Law of International Responsibility. Lk 239

[58] Rahvusvahelise Õiguse Komisjon. Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, Yearbook of International Law Commission, 2001, Volume 2, Part 2, United Nations: New York and Geneva, 2007, lk 43. Arvutivõrgus: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (04.05.2015).

[59] Crawford, James jt. The Law of International Responsibility, lk 245.

siiski riigile omistada.[60]

Termini "riigivõimu teostamise" sisustamise puhul ei ole oluline mitte üksnes volituse sisu vaid ka see, kuidas ja millistel eesmärkidel (näiteks riigi teatud suveräänsete huvide saavutamiseks) volitus antakse ning millisel määral annab volituse saaja oma tegevusest riigile aru.[61] Riigivõimu teostamine eraõiguslike juriidiliste isikute poolt võib olla näiteks börsi korraldamine, vanglate administreerimine, lennufirma poolt lennujaamas passikontrolli korraldamine jne.[62]

Riigivõimu teostamiseks volituste saamine ei pea toimuma seadusest tuleneva volitusnormist, piisab ka sellest, kui riik on näiteks sõlminud eraõigusliku juriidilise isikuga lepingu teatud riigivõimu ülesannete täitmiseks.[63] Kui riigiorgan, kes andis eraõiguslikule isikule riigivõimu ülesannete täitmiseks volituse või sõlmis temaga lepingu, oli pädev seda siseriikliku õiguse alusel tegema, siis on võimalik selliste eraõiguslikule isikute tegevust riigile omistada.[64]

Rahvusvaheline Kohus analüüsis *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua) kohtulahendis, kas isikud, kes tegutsesid Ameerika Ühendriikide sõjaväe või luureagentuuride otseste juhiste alusel, nn. UCLA-d, ning kellele Ühendriigid maksid ka selle eest raha, olid Ühendriikide poolt volitatud riigivõimu teostama. Kohus võttis lisaks ka arvesse, et Ameerika Ühendriigis osalesid UCLA-te poolt toime pandud rünnakute ettevalmistamises ja juhtimises ning asjaolu, et Ühendriigid pakkusid UCLA-tele igakülgset toetust. Sellest tulenevalt leidis Kohus, et UCLA-te poolt läbiviidud rünnakud olid Ameerika Ühendriikidele omistatavad.[65]

Riigi poolt volitatud organite poolt toimepandud tegude omistamine riigile on artikkel 5 alusel võimalik üksnes ulatuses, milles riik seda organit volitas.[66] See tähendab, et kui näiteks riik on volitanud eraturvafirmat täitma teatuid ülesandeid avaliku korra kaitsmiseks, siis vastutab riik

[60] Crawford, James. State Responsibility, lk 130.

[61] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 43

[62] Crawford, James jt. The Law of International Responsibility, lk 244.

[63] Crawford, James. State Responsibility, lk 131.

[64] Crawford, James. State Responsibility, lk 132.

[65] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports 1986, p. 14, lk 40, para. 86. Arvutivõrgus: http://www.icj-cij.org/docket/files/70/6503.pdf.

[66] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 43.

üksnes rahvusvahelise õiguse vastaste tegude eest, mis on selle eraturvafirma poolt toime pandud avaliku korra kaitsmisel (k.a. *ultra vires* teod). Riigile ei ole võimalik omistada selle eraturvafirma muid toimepandud rikkumisi, mis ei ole avaliku korra kaitsmisega seotud.

1.3.3. Teise riigi käsutusse antud riigiorganid

Riigivastutuse artiklite eelnõu artikkel 6 tegeleb väga kitsa, kuid mitte haruldase olukorraga, kus üks riik on andnud oma võimuorgani teise riigi käsutusse. Artikkel 6 sätestab, et sellises olukorras vastutab riigiorgani tegevuse eest see riik, kelle käsutusse teise riigi võimuorgan anti, kui tegu pandi toime selle riigi riigivõimu teostamisel. Ehk siis organi tegevuse eest vastutab see riik, kelle käsutusse organ anti ja mitte see riik, kes oma võimuorgani teise riigi käsutusse andis.

"Käsutusse andmine" tähendab, et see toimub vastuvõtja riigi nõusolekul, organ allub ainult kasusaaja riigi juhistele ja kontrollile, kooskõlas kasusaaja riigi toimimismehhanismidega.[67] Artikli 6 mõjualast jäävad välja kõik olukorrad, kus üks riik saadab teise riiki oma võimustruktuuride esindajad, kuid saadetud esindajad kohustuvad järgima ka koduriigi juhised või täidavad koduriigi eesmärke. Näiteks ei kohaldu artikkel 6 muuhulgas kultuurimissioonidele, diplomaatilistele- või konsulaarmissioonidele ja välismaistele abiorganisatsioonidele.[68] Kaks lisatingimust, mis peavad olema täidetud, et artiklis 6 sätestatud omistamisreegel kohalduks on järgnevad: esiteks peab saadetud organ olema saatjariigi riigiorgan või täitma riigiorgani ülesandeid ning teiseks peab saadetud organ täitma vastuvõtja riigis riiklike ülesandeid. Seega juhul kui riik saadab mingi ametliku koostööprogrammi raames teise riiki teatud ala eksperte (nt insenere), kes ei ole riigiorganid ega teosta riigivõimu, siis artikkel 6 kohaldamine ei ole võimalik, et omistada saatjariigile nende inseneride poolt toime pandud rahvusvahelise õiguse rikkumisi.

1.3.4. Riigiorganite *ultra vires* teod

Riigivastutuse artiklite eelnõu artikkel 7 sätestab, et riik vastutab oma organite tegevuse eest ka siis, kui organ ületab oma võimupiire või läheb vastuollu talle antud juhistega. Ehk siis riigi vastutus oma organite tegevuse eest on piiramatu niikaua kuni organ tegutseb oma ametlikes ülesannetes.[69] Igale võimukandjale on antud teatud volituste piir, mille raames on tal lubatud käituda. Kui isik ületab neid piire oma ametiülesannete täitmisel, siis see asjaolu ainuüksi ei

[67] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 44.

[68] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 44.

[69] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 41.

vabasta riiki rahvusvahelisest vastutusest. Rahvusvaheline Kohus leidis Relvastatud Tegevuste otsuses, et "tulenevalt sõjaväe staatusest ja Uganda sõdurite funktsioonist Kongos on Uganda sõdurite tegevus Ugandale omistatav. Vastuväide, et need isikud ei täitnud nendel konkreetsetel puhkudel valitsusorganite funktsioone on seega sisutu. Ugandale sõdurite käitumise omistamise jaoks on ebaoluline, kas UPDF käitus vastuolus talle antud juhistega või ületas oma võimupiire."[70] Samas ei vastuta riik igasuguse käitumise eest, mida tema võimustruktuuride esindajad toime panevad, vaid ainult sellise käitumise eest, mis on toime pandud riigi nimel. Praktikas võib aga tihtipeale osutuda keeruliseks konkreetselt üksnes erahuvides käitumise eristamine riigi nimel käitumisest.

1.4. Riigiväliste organite tegevuse omistamine

1.4.1. Riigi poolt juhiste andmine

Kuigi teatud olukordades võrdsustatakse riik tema inimestega (näiteks enesemääramise õiguse puhul) või vähemalt tema kodanikega (näiteks diplomaatilise kaitse andmise otsustamisel),[71] siis riigivastutuse doktriini üldpõhimõtte kohaselt ei omistata riigile füüsiliste ja juriidiliste isikute tegusid, kes ei ole riigi esindajad.[72] Küll aga on teatud puhkudel õigustatud riigiorganiga formaalselt mitteseotud isikute tegevuse omistamine riigile. Riigivastutuse artiklite artikli 8 kohaselt omistatakse riigile eraisikute või eraisikute grupi poolt toimepandud teod, kui teo toime pannud isik või isikute ühendus käitus riigi juhistel või riigi suunamise või kontrolli all. Isik või isikute ühendus muutub sellisel juhul juhiseid andva riigi käepikenduseks, läbi mille riik oma tahet ellu viib.

Riigi poolt juhiste andmine tähendab sisuliselt olukorda, kus riik palkab või õhutab eraisikuid või isikute gruppe osalema riigi poolt läbiviidavas tegevuses, kuid neid isikuid ei ole ametlikult selleks volitatud ning tegemist ei pruugi alati olla ka riigivõimu teostamisega. Näiteks võib riik saata isikud vabatahtlikena teise riiki kindlat ülesannet täitma, andes isikutele konkreetsed juhised tegutsemiseks, kuid saadetud isikud ei kuulu ametlikult politseijõudude või relvastatud vägede hulka.[73] Või näiteks sõlmib riik lepingu mõne eraturvafirmaga, et see teatud kolmandas

[70] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p.168, lk 78, para. 214. Arvutivõrgus: http://www.icj-cij.org/docket/files/116/10455.pdf (04.05.2015).

[71] Crawford, James. State Responsibility, lk 141.

[72] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 47.

[73] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 47.

riigis tagaks saatjariigi vägede turvalisust (ja see ei ole *acta iure imperii*) ning siis sätestada selle eraturvafirma käitumisjuhised kas lepingus või anda juhiseid jooksvalt tegevuse käigus.[74] Erinevus riigi juhendamise all toime pandud tegude ning riigivastutuse artikli 5 alusel omistatavate tegude vahel ongi see, et artikkel 5 nõuab, et rikkumised oleksid toime pandud riigivõimu teostamisel ja ametlikult selleks volitatud üksuste poolt, artikli 8 kohaldamiseks piisab sellest, kui riigi poolt palgatud üksused tegutsevad riigi nimel.

Problemaatiliseks on aga osutunud küsimus, millisel määral peab riik andma mitteriiklike üksustele juhiseid, et nende poolt toimepandud teod oleksid riigile omistatavad ning kas juhiseid saanud üksuste poolt *ultra vires* toimepandud rikkumised on ka riigile omistatavad?

Riigivastutuse artiklite eelnõu kommentaarid sedastavad, et kui riik annab isikutele, kes ei ole riigiorganid, seaduslikke juhiseid, siis ta üldjuhul ei vastuta selle eest, et neid juhiseid rakendati rahvusvahelise õiguse vastasel viisil.[75] Riigi vastutus võib siiski tõusetuda juhul kui riik on küll andnud isikutele seaduslikud juhised, kuid nende täitmisega kaasneb paratamatult rahvusvahelise õiguse rikkumine, s.t. rikkumine ei ole juhuslik.[76] Seega näiteks juhul kui riik on andnud ebaselgeid või lahtiseid juhised, siis riik vastutab tegude eest, mis operatsiooniga kaasnevad või mida võib mõistlikult pidada antud juhistega hõlmatuteks.[77] Sellest nähtuvalt vastutab riik ka mitteriiklike üksuste *ultra vires* rikkumiste eest juhul kui need on mõistlikult seotud selle operatsiooniga, mida need üksused riigi juhiste all toime panevad.

1.4.2. Allumine riigi kontrollile või suunistele

Mitteriiklike üksuste poolt toimepandud rahvusvahelise õiguse vastaste tegude riigile omistamise teine alternatiiv artikli 8 alusel on riigile sellise tegevuse omistamine, mille puhul on teo toime pannud isikud, kes ei ole riigiorganid, kuid kes alluvad riigi kontrollile või suunistele. Riigivastutuse artiklite eelnõu kommentaaride kohaselt on riigi suunised ja kontroll kaks eraldiseisvat alust ning vastutuse tekkimiseks piisab vaid ühe nende esinemisest.[78] Küll aga on rahvusvahelise praktika järgi on riigi poolt antud suuniseid ja rakendatavat kontrolli koheldud kui ühtset omistamise standardit, selle erinevaid osasid eristamata. Kuna

[74] Crawford, James. State Responsibility, lk 145.

[75] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 48.

[76] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 48.

[77] Crawford, James. State responsibility, lk 145.

[78] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 48.

riigivastutuse artiklite eelnõu ei täpsusta, milline peab olema riigi poolt rakendatud kontroll või millised peavad olema riigi poolt antud suunised selleks, et tegevus oleks riigile omistatav, siis on rahvusvahelises õiguses välja arenenud sisuliselt kaks erinevat kontrollistandardi doktriini. Rahvusvahelise Kohtu praktikast tuleneb efektiivse kontrolli doktriin ning Endise Jugoslaavia Rahvusvahelise Kriminaaltribunal on välja töötatud üldise kontrolli doktriini.

1.4.2.1. Efektiivne kontroll

Efektiivse kontrolli doktriini käsitles Rahvusvaheline Kohus esmakordselt Nicaragua kohtuasjas. Selles kaasuses oli üheks keskseks küsimuseks, kas Ameerika Ühendriigid vastutavad Nicaragua paramilitaarse rühmituse ehk kontrate poolt toimepandud rahvusvahelise õiguse rikkumiste eest või mitte. Rahvusvaheline Kohus analüüsis seda probleemi sisuliselt kolmest aspektist: kas Ühendriigid vastutavad Nicaragua paramilitaarse liikumise eest üldiselt, kas Ühendriigid vastutavad konkreetsete paramilitaarsete operatsioonide eest ning kas Ühendriigid vastutavad konkreetsete rahvusvahelise humanitaarõiguse rikkumise eest, mida kontrad nende paramilitaarsete operatsioonide käigus toime panid?

Rahvusvaheline Kohus leidis, et kuigi Ameerika Ühendriigid ei loonud relvastatud vastupanuliikumist Nicaraguas, siis Ühendriikide poolt rahalise ning muu toetuse andmine kasvatas dramaatiliselt kontrate arvukust.[79] Seega ei saanud Ameerika Ühendriigid vastutada Nicaraguas tekkinud paramilitaarse liikumise eest üldiselt.

Teiseks leidis Kohus, et Ameerika Ühendriigid vastutavad kontrate finantseerimise ja neile logistilise toetuse andmise eest. Ühendriigid andsid kontratele relvi, laskemoona, varustust ja toitu,[80] õpetasid kontraid välja ning jagasid neile luureteavet Nicaragua vägede liikumise kohta.[81] Lisaks leidis Rahvusvaheline Kohus, et mõningad kontrate poolt ellu viidud operatsioonid olid planeeritud tihedas koostöös Ühendriikide sõjaväe konsultantidega, tuginedes Ühendriikide luureinfole[82] ning Ameerika Ühendriigid valisid sobilikke sihtmärke kontrate rünnakute jaoks. Kõike eelnevat arvesse võttes pidi Kohus tuvastama, kas

[79] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), lk 44, para. 94.

[80] Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America), lk 49, para. 100.

[81] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), lk 49, para 101.

[82] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), lk 51, para. 106.

Ühendriikide märkimisväärne sekkumine oli selline, mis annaks alust väita, et kontrate näol oli tegemist Ameerika Ühendriikide *de facto* organiga või kas kontrad tegutsesid Ühendriikide nimel. Kohus oli seisukohal, et hoolimata Ühendriikide olulisest panusest kontrate tegevuse organiseerimisesse ei tuvastanud Kohus, et kontrate ja Ameerika Ühendriikide vahel oleks valitsenud selline täielik sõltuvus ühelt poolt ja täielik kontroll teiselt poolt, et oleks võimalik järeldada, et kontrad käitusid Ameerika Ühendriikide nimel.[83] Seetõttu ei olnud võimalik omistada Ühendriikidele kõiki kontrate poolt toimepandud tegusid.

Kuna täielikku sõltuvust ei suutud Rahvusvaheline Kohus tuvastada, jätkas Kohus analüüsimisega, kas mõningaid konkreetseid humanitaarõiguse rikkumisi saab Ühendriikidele omistada kuna too pakkus kontratele märkimisväärset toetust. Siinkohal sõnastaski Rahvusvaheline Kohus efektiivse kontrolli standardi. Rahvusvaheline Kohus, leidis et: „Ameerika Ühendriikide osalus, isegi kui see oli ülekaalukas või otsustav, kontrate finantseerimisel, organiseerimisel, väljaõpetamisel, varustamisel ja relvastuse muretsemisel, militaarsete või paramilitaarsete sihtmärkide valikul ning kõigi nende operatsioonide planeerimisel, ei ole iseenesest piisav [...] omistamaks Ameerika Ühendriikidele kontrate toimepandud tegusid [...]. Selleks et nende käitumine tooks kaasa Ameerika Ühendriikide õigusliku vastutuse, on põhimõtteliselt vaja tõestada, et riik omas efektiivset kontrolli militaarsetes või paramilitaarsetes operatsioonides, mille käigus pandi toime väidetavad rikkumised.“[84] Rahvusvaheline Kohus ei avanud siiski efektiivse kontrolli standardi täpsemat sisu, ega analüüsinud milliste tingimuste täitmisel võib öelda, et riigil on efektiivne kontroll teatud rühmituste üle.

1.4.2.2. Üldine kontroll

Rahvusvahelise Kohtu poolt väljapakutud efektiivse kontrolli standardi sobivus seati kahtluse alla Endise Jugoslaavia Rahvusvahelise Kriminaaltribunali apellatsioonikoja poolt Duško Tadići kohtuasjas. Duško Tadić oli valvur ühes Bosnias asunud interneerimislaagris ning osales ligi 14 000 inimese hukkamises. Tadićile esitati süüdistused sõjakuritegudes ning inimsusevastastes kuritegudes.

Oluline on siinkohal välja tuua, et Endise Jugoslaavia Rahvusvahelisel Kriminaaltribunalil

[83] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), lk 62, para. 109.

[84] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), lk 65, p 115. Tõlge: Värk, René. Riigi vastutus mitteriiklike terroristlike rühmituste eest. Juridica, (2012), 20(2), lk 104.

puudub jurisdiktsioon riikide üle ning üldjuhul riikidele teatud tegude omistamise küsimus ei kuulu Tribunali jurisdiktsiooni alla. Tribunalil on jurisdiktsioon üksnes füüsiliste isikute üle, kes tegutsesid endise Jugoslaavia Föderatiivse Sotsialistliku Vabariigi territooriumil.[85] Tribunalil puudub seega pädevus, et hinnata, kas mõnele riigile saaks omistada mõne eraisiku poolt toimepandud rahvusvahelise õiguse rikkumisi.

Omistamise küsimus tõusetus Duško Tadići kohtuasjas seetõttu, et Tribunal pidi tuvastama, kas Tadić pani talle süükspandavad kuriteod toime rahvusvahelise või mitterahvusvahelise relvastatud konflikti raames, sest Endise Jugoslaavia Rahvusvahelise Kriminaaltribunalil on pädevus otsustada üksnes 1949. aastal vastuvõetud Genfi konventsioonide raskete rikkumiste üle,[86] kuid 1949. aasta Genfi konventsioonid kohalduvad vaid relvastatud konfliktidele, mis on rahvusvahelised. Tribunal pidi oma jurisdiktsiooni üle otsustamisel tuvastama, kas Serbiale või Horvaatiale saab omistada eraisikute poolt konflikti raames toimepandud kuritegusid. Kui omistamine on võimalik, siis on tegemist rahvusvahelise konfliktiga, mille raames toimepandud kuritegude üle on Tribunalil jurisdiktsioon.

Tribunali istungikoda tugines oma otsuses suures osas Rahvusvahelise Kohtu poolt Nicaragua lahendis toodud seisukohtadele ja sedastas, et "kuigi Serbial oli võimekus oluliselt mõjutada ja isegi kontrollida Serblaste Vabariigi vägesid, siis puuduvad piisavad tõendid, et järeldada, et Serbia oleks andnud juhiseid või oleks püüdnud anda juhiseid Serblaste Vabariigi vägedele sõjaliste operatsioonide läbiviimiseks või, et Serbia mõjutas Serblaste Vabariigi vägesid rohkemal määral, kui selliselt, nagu see loomulikult esineb sõjaliste eesmärkide ja tegevuste koordineerimisel."[87] Istungikoda leidis kokkuvõttes, et "kuigi Serbia valitsuse poolt pakutud abi Serblaste Vabariigi relvastatud vägedele oli nende poolt läbiviidavate tegevuste jaoks ülioluline, ja Serblaste Vabariigi relvajõud olid peaaegu täielikult Serbia poolt pakutavast abist sõltuvad, siis pole piisavalt tõendeid, et hinnata, kas Serbia ka tegelikult kasutas sellisest sõltuvussuhtest tulenevat kontrolli või efektiivset kontrolli Serblaste Vabariigi vägede üle.[88]

Tribunali apellatsioonikoda kritiseeris tugevalt esimese astme koja ülemäärast tuginemist

[85] Statute of the International Criminal Tribunal for the Former Yugoslavia (as amended on 7 July 2009), 25 May 1993. Arvutivõrgus: http://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf (04.05.2015).

[86] Statute of the International Criminal Tribunal for the Former Yugoslavia (as amended on 7 July 2009), 25 May 1993.

[87] Prosecutor v. Duško Tadic, Judgment, Case No. IT-94-1-T, ICTY Trial Chamber, 7 May 1997, lk 216, para. 605. Arvutivõrgus: http://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf (04.05.2014).

[88] IT-94-1-T, lk 216, para. 605.

Nicaragua lahendile. Apellatsioonikoda leidis, et Nicaragua lahendis väljapakutud test on vastuolus riigivastutuse õiguse loogikaga.[89] Seda seetõttu, et riigivastutuse artiklite artikkel 8 eesmärgiks on ära hoida olukord, kus riik viib ellu oma tahet läbi eraisikute, kuid teisalt ütleb lahti nende eraisikute poolt toimepandud tegudest, kui teo toimepanija on oma käitumisega rikkunud rahvusvahelist õigust ning välistab sellega riigi vastutuse. Apellatsioonikoja arvates riigile eraisikute poolt toimepandud tegude omistamiseks peab riik küll omama kontrolli nende isikute tegevuse üle, kuid omistamiseks vajaliku kontrolli ulatus võib varieeruda olenevalt iga üksiku juhtumi asjaoludest. Apellatsioonikoda ei näinud põhjust, miks igal üksikul juhul peaks test riigipoolse kontrolli hindamiseks olema väga kõrge künnisega.[90]

Lisaks tõi apellatsioonikoda välja, et riigile üksikisikute või mitte-organiseeritud rühmituste poolt toimepandud tegude omistamise puhul on rahvusvahelises praktikas olnud teistsugune standard kui näiteks organiseerunud militaarsete struktuuride üle teostatava kontrolli puhul. Apellatsioonikoda leidis, et rahvusvahelise praktika järgi saab eraisikute või mitte-organiseerunud rühmituste poolt toimepandud tegusid riigile omistada juhul, kui riik on teo toimepanijale andnud konkreetsed juhised konkreetse teo jaoks või kui riik on kõnealused teod avalikult heaks kiitnud. Organiseerunud relvastatud rühmituste, omakaitseväelaste või paramilitaarsete rühmituste puhul ei ole vajalik, et nad sõltuksid riigist täielikult, et riik valiks nende sihtmärgid või annaks neile konkreetseid juhiseid sõjaväeliste operatsioonide läbiviimiseks ja rahvusvahelise humanitaarõiguse rikkumiseks. Riigil on rühmituste üle kontroll siis, kui kõnealune riik lisaks rühmituse rahastamisele, treenimisele, varustamisele ja muule operatiivse toetuse pakkumisele ka organiseerib, koordineerib või planeerib rühmituse sõjalist tegevust.[91]

Erinevus Nicaragua lahendis väljapakutud efektiivse kontrolli standardist ongi asjaolu, et riigil ei pea olema kontroll iga konkreetse operatsiooni üle, mille käigus rahvusvahelise õiguse vastased teod toime pandi, vaid piisab sellest, et riik kontrollib rühmituse sõjalist tegevust üldiselt. Seda vähemnõudlikumat testi organiseeritud rühmituste tegevuse omistamiseks saab selgitada asjaoluga, et organiseeritud rühmitustes valitseb enamasti selge hierarhia ning kui riigi on võimalust rakendada üldist kontrolli kogu rühmituse üle, siis on tal ka kontroll iga

[89] Prosecutor v. Duško Tadic, Judgement, Case No. IT-94-1-A, ICTY Appeals Chamber, 15 July 1999, lk 47, para. 116. Arvutivõrgus: http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf (04.05.2015).

[90] IT-94-1-A, lk 48, para. 117.

[91] IT-94-1-A, lk 59, para. 137.

rühmaliikme üle.[92] See seisukoht on aga tekitanud õigusteadlaste seas mõningat diskussiooni. Näiteks kui Antonio Cassese toetas üksikisiku ja grupi üle teostatava kontrolli jaoks erinevate standardite kasutamist,[93] siis James Crawford leidis, et omistamise jaoks on seesugune vahetegemine üksikisiku ja grupi vahel on üleliigne, sest on keeruline näha kuidas üldise kontrolli standardi kohaldamine üksikisikule ja grupile saaks kaasa tuua erinevad järeldused.[94]

1.4.2.3. Üldise kontrolli standardi kriitika

Bosnia Genotsiidi lahendis tegeles Rahvusvaheline Kohus uuesti põhjalikumalt omistamise standardite küsimusega. Varasemalt oli Kohus puudutanud mitteriiklike rühmituste omistamise küsimust küll ka Relvastatud Tegevuste kaasuses, kus vaidluse poolteks olid Uganda ja Kongo Demokraatlik Vabariik. Selles kaasuses pidi Kohus otsustama, kas teatud Kongos tegutsenud rühmituste tegevust on võimalik omistada Ugandale või mitte. Kohus leidis, et tulenevalt tõendite puudumisest ei ole võimalik anda hinnangut, kas Ugandal oli piisav kontroll kõnealuste paramilitaarsete rühmituste üle ja viitas Nicaragua lahendile.[95] Sisulisemat analüüsi tõendite puudumise tõttu ei järgnenud.

Bosnia Genotsiidi lahendis otsustas Rahvusvaheline Kohus võtta lõpuks seisukoha Endise Jugoslaavia Rahvusvahelise Kriminaaltribunali poolt Tadići kaasuses väljapakutud üldise kontrolli standardi osas. Bosnia Genotsiidi kaasuse asjaolud olid sarnased Tadići kaasuse asjaoludega. Nimelt pöördus Bosnia ja Herzegovina Rahvusvahelise Kohtu poole, et too otsustaks, kas Serbia vastutab Bosnia sõja ajal Bosnia serblaste omakaitsevägede poolt toimepandud genotsiidiaktide eest või mitte. Rahvusvaheline Kohus leidis esiteks, et Tribunali poolt välja pakutud üldise kontrolli standardit kohaldati eelkõige selleks, et tuvastada, kas tegemist oli rahvusvahelise konfliktiga ning leidis, et puudub loogiline põhjendus, miks peaks olema mingi riigi osalemine teatud konfliktis ja selle konflikti jooksul toimepandud rahvusvahelise õiguse rikkumiste omistamine sellele riigile olema tuvastatud kohaldades ühte ja sama standardit.[96] Teiseks leidis Kohus, et üldise kontrolli standardi negatiivseks tagajärjeks

[92] IT-94-1-A, lk 49 para. 120.

[93] Cassese, Antonio. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. The European Journal of International Law, Volume 18, Issue 4, lk 661.

[94] Crawford, James. State Responsibility, lk 153.

[95] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), lk 62, para. 160.

[96] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), lk 171 para. 405.

on riigivastutuse liigne laiendamine, mis kaugeneb riikide rahvusvahelise vastutuse fundamentaalsest printsiibist, mille kohaselt vastutab riik üksnes iseenda tegevuse eest, ehk siis isikute tegevuse eest, kes käituvad riigi nimel ükskõik millisel alusel. Rahvusvahelise tavaõiguse kohaselt, mis on kodifitseeritud riigivastutuse artiklite eelnõu artiklis 8, on mitteriiklike organite või neisse kuuluvate isikute tegevuste omistamine riigile võimalik üksnes siis, kui riik andis juhiseid või suuniseid, mille alusel käitudes isikud need rikkumised toime panid või kus riik rakendas efektiivset kontrolli tegevuse üle, mille jooksul rikkumised toime pandi. Kohus leidis, et kuna Tribunali poolt välja pakutud üldise kontrolli test laiendab nõutavat sidet riigiorganite ja riigivastutuse vahel ebamõistlikult, siis on üldise kontrolli test ebasobilik.[97]

Rahvusvahelise Kohtu kriitika üldise kontrolli standardi kohta pälvis väga laialdast vastukaja.[98] Antonio Cassese kritiseeris Kohtu seisukohta, et efektiivse kontrolli standard on artikli 8 kohaldamisel on tunnustatud rahvusvaheline tavaõigusena. Kohus ei analüüsinud ühegi teise rahvusvahelise kohtu või –tribunali lahendit, milles oleks hinnatud mõnda kontrollistandardit. Rahvusvaheline Kohus tugines üksnes enda poolt tehtud Nicaragua lahendile, milles samuti Kohus ei olnud analüüsinud teiste rahvusvaheliste kohtute praktikat kontrollistandardite kohaldamisel, ning Rahvusvahelise Õiguse Komisjoni poolt koostatud riigivastutuse artiklite kommentaaridele, mis omakorda tuginesid üksnes Nicaragua lahendile.[99] Kohus ei andnud hinnangut Endise Jugoslaavia Rahvusvahelise Kriminaaltribunali poolt viidatud lahenditele, kuid juba asjaolu, et Tribunal sai oma otsuses toetuda paljudele mitmetele teistele lahenditele, mis toetasid võimalust kohaldada mõnda muud standardit, et tuvastada riigi poolt mitteriiklike

[97] Application of the Convention on the Prevention and Punishment of the Crime of Genocide, lk 171 para. 406.

[98] Vt nt: Abass, Ademola. Proving State Responsibility for Genocide: The ICJ in Bosnia v. Serbia and the International Commission of Inquiry for Darfur. Fordham International Law Journal, Volume 31, Issue 4, 2007 (milles kaheldi, kas efektiivse kontrolli test peegeldab täpselt tavaõigust); Griebel, Jörn; Plücken, Milan. New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia. Leiden Journal of International Law, Volume 21, Issue 03, September 2008 (milles kirjeldati efektiivse kontrolli kasutamist Bosnia Genotsiidi lahendis kui "kehtivate reeglite väärkohadamist, mis tõenäoliselt ei leia üldist heakskiitu" ning "õiguslikku viga, mida võib olla keeruline tulevikus parandada"); Shackelford, Scott. Holding States Accountable for the Ultimate Human Right Abuse: A Review of the International Court of Justice's Bosnian Genocide Case. Human Rights Brief, Volume 14, Issue 3, March 2007 (milles leiti, et genotsiidisüüdistuste puhul on õigustatud üldise kontrolli kohaldamine ning mitte liigselt kitsendava efektiivse kontrolli test). Mitmed autorid aga näitasid oma poolehoidu Rahvusvahelise Kohtu seisukohtadele, vt nt: Rajković, Nikolas. On 'Bad Law' and 'Good Politics': The Politics of the ICJ Genocide Case and Its Interpretation. Leiden Journal of International Law, Volume 21, Issue 04, December 2008 (milles leiti, et laiendav omistamise test oleks mõjutatav õigusväliste eesmärkide saavutamiseks ning võimaldaks areneda politiseeritud jurisprudentsil ning, et Kohtu tuginemine Nicaragua lahendile andis selge signaali, et rahvusvahelisi kohtuid ei peaks kasutama oma õigusväliste eesmärkide saavutamiseks); Milanović, Marko. State Responsibility for Acts of Non-state Actors: A Comment on Griebel and Plücken. Leiden Journal of International Law, Volume 22, Issue 02, June 2009.

[99] Cassese, Antonio. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, lk 650 jj.

üksuste üle teostatud kontrolli, viitab, et rahvusvaheline praktika ei ole nii ühtne, et Kohus saaks sellise ülima enesekindlusega viidata efektiivse kontrolli standardi kuulumist tavaõiguse hulka.

Võttes arvesse üsnagi teravat kriitikat Rahvusvahelise Kohtu suunas väga paljude õigusteadlaste poolt, on keeruline nõustuda James Crawfordiga, kes leidis, et Bosnia Genotsiidi lahendiga Rahvusvaheline Kohus sisuliselt lõpetas debati teemal, et milline on korrektne kohaldatav kontrollistandard riigivastutuse artiklite eelnõu artikli 8 mõttes.[100] Arutelud korrektse kontrollistandardi üle ilmselt jätkuvad, sest nagu kohtunik Robert Jennings sõnastas oma eriarvamuses Nicaragua lahendis - niivõrd range kontrollistandard ei näi ei realistlik ega õiglane[101] ning Bosnia Genotsiidi lahendi valguses ei tuleb sellega nõustuda.

1.5. Muud omistamise alused

1.5.1. Riigivõimu teostamine ametliku riigivõimu puudumisel

Riigivastutuse artiklite eelnõu artikkel 9 sätestab, et riigile omistatakse isiku või isikute grupi teod juhul, kui need isikud teostavad riigivõimu ametlike võimuorganite puudumisel või tegevusetuse korral ning asjaolud nõuavad selliste võimuelementide rakendamist. Artiklit 9 on võimalik kohaldada üksnes väga erandlikel juhtudel näiteks revolutsiooni, relvastatud konflikti või võõrriigi okupatsiooni korral, kus tavapärased ametlikud organid on laiali saadetud, lagunemas, maha surutud, ajutiselt mittetöötavad või ka näiteks juhul kui õiguspäraseid võimuorganeid alles taastatakse pärast okupatsiooni.[102]

Artikli 9 alusprintsiibiks võib pidada *levée en masse* põhimõtet, mille alusel on kodanikel õigus enesekaitseks regulaarvägede puudumisel. *Levée en masse* põhimõtet on tunnustatud 1907. aasta Haagi IV konventsioonis maasõja seaduste ja tavade asjus ning sõjavangide kohtlemise 12. augusti 1949 Genfi (III) konventsioonis.[103]

Artikkel 9 kohaldamiseks peab esinema kolm tingimust: isikud tegutsevad omal initsiatiivil, nad peavad täitma riigivõimu ülesandeid, ametlik riigivõim peab puuduma või olema tegevusetu ning esinevad elulised asjaolud, mis nõuavad riigivõimu teostamist. Artikli 9

[100] Crawford, James. State Responsibility, lk 156.

[101] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Dissenting opinion of Judge Sir Robert Jennings, lk 533. Arvutivõrgus: http://www.icj-cij.org/docket/files/70/6525.pdf (04.05.2015).

[102] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 49, para. 1.

[103] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 49, para. 2.

kohaldamisala hulka ei kuulu riigivõimu teostavate isikute käitumine, keda ei ole küll *de iure* riigiorganina tunnustatud, kuid mis omab faktilist kontrolli teatud riigiterritooriumi üle. Sellisel juhul on tegemist *de facto* valitsusega, mida võib pidada riigiorgani osaks ja mis asendab varasema.[104] Seega *de facto* riigiorganite esindajate tegusid on võimalik omistada riigivastutuse artiklite eelnõu artikkel 4 alusel ja mitte artikkel 9 alusel. Lisaks, sarnaselt riigivastutuse artiklite eelnõu artiklile 6, tuleb artikli 9 kohaldamisel esmajoones eristada, kas toimepandud rahvusvahelise õiguse vastased teod on *acta iure imperii*, mis on riigile omistatavad või *acta iure gestionis*, mida riigivõimu teostamiseks pidada ei saa.[105] Asjaolud, mis nõuavad riigivõimu teostamist peavad olema sellised, et eraisikute poolt mingite riigivõimu ülesannete täitmine on vajalik ja õigustatud.[106] Samas on oluline mainida, et rikkumised, mille omistamine on küsimuse all, ei pea olema otseselt seotud selle konkreetse ülesande täitmisega. See tähendab, et kui näiteks mingi rühmitus täidab ametlike politseijõudude puudumisel politsei ülesandeid, kuid rühmituse poolt toime pandud rahvusvahelise õiguse vastane tegu ei ole seotud politseiülesannete täitmisega, siis on nende tegude omistamine riigile sellest hoolimata võimalik.

1.5.2. Vastuhakuliikumiste tegevus

Riigivastutuse artiklite eelnõu artikkel 10 käsitleb vastuhaku- või ülestõusmisliikumise tegevuse omistamise küsimust. Artikkel 10 lõige 1 sätestab, et kui vastuhakuliikumine moodustab riigi uue valitsuse, siis tema tegevus omistatakse sellele riigile. Lõige 2 sätestab, et juhul kui vastuhakuliikumine moodustab uue riigi endise riigi territooriumil või enda administreeritud territooriumil, siis omistatakse vastuhakuliikumise poolt toimepandud rahvusvahelise õiguse rikkumised sellele uuele riigile. Lõige 2 võib kohalduda nii setsessiooni, riigi lagunemise kui ka riikide ühinemise korral.[107]

Artikkel 10 ei defineeri, milliseid rühmitusi kasutatud termin "vastuhakuliikumine" hõlmab ja millised mitte. Seda eelkõige seetõttu, et vastuhakuliikumised võivad võtta väga erisuguseid vorme olenevalt sellest, kas tegemist on üsna piiratud ulatusega sisemise rüsinaga, kodusõjaga,

[104] Aguilar-Amory and Royal Bank of Canada claims (Great Britain v. Costa Rica). Reports of International Arbitral Awards, Volume I, 18 October 1923, lk 81-82. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_I/369-399.pdf (04.05.2015).

[105] Crawford, James. State Responsibility, lk 169.

[106] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 49, para. 6.

[107] Dumberry, Patrick. New State Responsibility for Internationally Wrongful Acts by an Insurrectional Movement. The European Journal of International Law, Volume 17, Issue 3, lk 617.

kolonialismivastase võitlusega, rahvuslike vabastusjõudude tegevusega, revolutsiooni või kontrrevolutsiooniga jne.[108] Riigivastutuse artiklite kommentaaride kohaselt võib võtta termini "vastuhakuliikumine" defineerimise aluseks 12. augusti 1949 Genfi konventsioonide 8. juuni 1977 (II) lisaprotokolli siseriiklike relvakonfliktide ohvrite kaitse kohta, mille artikkel 1 lõige 1 sätestab, et lisaprotokolli rakendatakse nende relvakonfliktide puhul, mis toimuvad riigi ning tema "teisitimõtlejate relvajõudude või muude organiseeritud relvastatud rühmituste vahel, kes kellegi juhtimisel kontrollivad tema territooriumi nii, et neil on võimalik läbi viia pidevaid ja kooskõlastatud sõjalisi operatsioone ja rakendada käesolevat protokolli." Sama paragrahvi lõige 2 sätestab, et "protokolli ei rakendata siserahutuste ja -pingete korral, nagu massilised korratused, isoleeritud ja juhuslikud vägivallaaktid ja teised samalaadsed aktid, mis ei ole relvakonfliktid." [109] Lisaprotokolli tähenduses artiklis 1 defineeritud "teisitimõtlejate relvajõud" ongi sisuliselt termini "vastuhakuliikumise" põhiidee.[110]

On laialdaselt tunnustatud põhimõte, et riik ei vastuta vastuhakuliikumiste poolt toimepandud rahvusvahelise õiguse rikkumise eest (kui ta ei rikkunud hea usu põhimõtet või ei olnud hooletu vastuhaku mahasurumisel) juhul, kui sellel vastuhakuliikumisel ei õnnestunud enda eesmärkide (näiteks iseseisvuse) saavutamine.[111] Seda eelkõige seetõttu, et vastuhakuliikumised on riigi ametliku struktuuri välised üksused, nad ei teosta riigi seaduslikku võimu ning neid ei saa pidada riigi "juhiste, suuniste või kontrolli all olevateks".[112] Riigivastutus võib tekkida üksnes juhul kui vastuhakuliikumine oli edukas ning sellel õnnestus moodustada valitsus või uus riik. See on kooskõlas üldise riigivastutuse põhimõttega, mille alusel vastutab riik üksnes iseenese tegude eest. Edukate vastuhakuliikumiste tegude omistamine uuele riigile või valitsusele on õigustatud tuginedes nii öelda "orgaanilise" või "strukturaalse" järjepidevuse põhimõttele.

[108] Draft Articles on State Responsibility with Commentaries thereto Adopted by the International Law Commission on First Reading. lk 70, para. 1. Arvutivõrgus: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf (04.05.2015).

[109] 2. augusti 1949 Genfi konventsioonide 8. juuni 1977 (II) lisaprotokoll siseriiklike relvakonfliktide ohvrite kaitse kohta. Arvutivõrgus: https://www.riigiteataja.ee/akt/79271 (04.05.2015).

[110] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 59, para. 9.

[111] Vt nt: Home Frontier and Foreign Missionary Society of the United Brethren in Christ (United States v. Great Britain). Reports of International Arbitral Awards, Volume VI, 18 December 1920, lk 44. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_VI/42-44_Brethren.pdf; Sambiaggio Case (of a general nature). Reports of International Arbitral Awards, Volume X, 1903, lk 499. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_X/499-525.pdf.

[112] Crawford, James. State Responsibility, lk 170.

Strukturaalse järjepidevuse tõttu on side eduka vastuhakuliikumise ja uue valitsuse vahel piisav, et omistada riigile eduka vastuhakuliikumise tegusid. Strukturaalsest järjepidevusest kantuna on uuele valitsusele omistatavad ka endise valitsuse teod vastuhaku allasurumisel.[113] Selle põhimõtte kohaldamine võib osutuda siiski keeruliseks, kui uue riigi loomisesse panustasid mitmed erinevad mässuliste rühmitused. On leitud, et sellistel puhkudel saab uuele riigile omistada kõikide revolutsiooniliste rühmituste poolt toime pandud tegusid ja mitte üksnes selle rühmituse omi, kes moodustab uue valitsuse.[114] Seda seisukohta on kritiseeritud, sest sellise käsitlus on vastutus ülemäära laiendav ning suure tõenäosusega riikidele vastuvõetamatu.[115] Riigile kõikide ülestõusus osalenud rühmituste poolt toimepandud tegude omistamine, üksnes seetõttu, et üks osalenutest osutus edukaks, võib minna vastuollu riikide vastutuse üldpõhimõttega, mille kohaselt vastutab riik üksnes enda tegude eest. On keeruline näha sidet uue riigi ja endiste (valitsust mittemoodustanud) rühmituste vahel, mis õigustaksid riigile nende poolt toimepandud tegude omistamist. Teistsugune oleks olukord loomulikult siis, kui edukaks osutunud vastuhakuliikumine omas efektiivset või üldist kontrolli ka teiste ülestõusus osalenud rühmituste üle. Sellisel juhul tuleks tegude omistamiseks kohaldada siiski riigivastutuse eelnõu artiklit 8.

Problemaatiliseks võib osutuda ka olukord, kus olemasolev riik sõlmib näiteks mässulistega rahulepingu, mille alusel kaasatakse mässulised riigi ametlikesse struktuuridesse. Kui sellisel puhul saaks omistada vastuhakuliikumise kõiki varasemaid tegusid riigile, siis see võib olla riigile negatiivseks stiimuliks rahulepingu sõlmimiseks.[116] Riik ei peaks vastutama vägivaldse opositsioonirühmituse tegude eest üksnes seetõttu, et rühmitus kaasatakse valitsusse üldise rahutagamise eesmärgil. Seetõttu tuleb riigivastutuse artiklite kommentaaride kohaselt artikkel 10 lõige 1 kohaldamisele üksnes juhul, kui vastuhakuliikumise ja uue valitsuse vahel on tõeline ja oluline side.[117]

[113] Crawford, James. State Responsibility, lk 175.

[114] Dumberry, Patrick. New State Responsibility for Internationally Wrongful Acts by an Insurrectional Movement, lk 612.

[115] Crawford, James. State Responsibility, lk 179.

[116] Crawford, James. State Responsibility, lk 176.

[117] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 51 para. 7.

1.5.3. Käitumise tunnustamine ja omaksvõtt riigi poolt

Riigivastutuse artiklite artikkel 11 sätestab viimase omistamise aluse. Artikkel 11 alusel on võimalik omistada riigile käitumist, mida ei ole võimalik omistada eelnevate artiklite alusel, selles ulatuses, mida riik on tunnustanud ning võtnud omaks. Tunnustamine ja omaksvõtmine on kumulatiivsed tingimused ning need indikeerivad sündmuste tavapärast järjestust. Riigivastutuse artiklite eelnõu kommentaaride kohaselt võib teo riigi poolt tunnustamine ja omaksvõtmine olla kas selgesõnaline või riigi käitumisest tuletatav.[118]

Artiklis 11 kajastatud põhimõtet on kohaldatud näiteks Majakate Arbitraaži vaidluses, kus arbitraažitribunal leidis, et Kreeka vastutab Kreeta poolt sõlmitud kontsessioonilepingu rikkumise eest, kuigi selle kontsessioonilepingu sõlmis Kreeta ajal, mil ta oli alles Ottomani Impeeriumi autonoomne osa. Tribunal tugines oma otsuses osaliselt asjaolule, et Kreeka toetas Kreeta poolt kontsessioonilepingu rikkumist justkui nagu see oleks olnud tavapärane tehing ja Kreeka jätkas rikkumist isegi pärast territooriumi üle suveräänsuse saamist. Sellest nähtub, et juhul kui riik toetab ja jätkab mingit rikkumist, siis võib asuda seisukohale, et riik on sellega ka aktsepteerinud võimalikku vastutust, mis sellest rikkumisest võib tuleneda.[119]

Riigi poolt eraisikute tegevuse omaksvõtmise üheks näiteks võib pidada ka Adolf Eichmanni kinni püüdmist ning sellele järgnevat kohtuprotsessi. Adolf Eichmann töötas Natsi-Saksamaal holokausti transpordiadministraatorina ning omas olulist rolli holokausti toimepanemisel. Teise maailmasõja lõpul põgenes Eichmann Argentiinasse, kus ta elas kuni tema kinninabimiseni grupi Iisraeli kodanike poolt 10. mail 1960. aastal. Argentiina süüdistas Iisraeli valitsust, et oli Eichmanni kinnipüüdmises kaassüüdlane. Julgeoleku Nõukogu leidis, et Iisrael oli nõustunud, või vähemalt oli teadlik, Eichmanni Argentiinas kinni püüdmise plaaniga. Kui Eichmanni tabajad käitusid Iisraeli juhiste või suuniste ja kontrolli all, siis võib nende käitumist omistada Iisraelile riigivastutuse artiklite eelnõu artikli 8 alusel, kuid kui esineb kahtlusi, kas Iisraeli käitumine täidab artiklis 8 esitatud ranged nõudmised, siis võiks lähtuda Iisraeli käitumisest pärast Eichmanni tabamist ning omistada eraisikute grupi teod Iisraelile artikkel 11 alusel.[120]

Rahvusvaheline Kohus on riigivastutuse artiklite eelnõu artiklis 11 sõnastatud põhimõtet kohaldanud sisuliselt kahes kaasuses, millest tuntuim on kindlasti Tehrāni Pantvangide kaasus,

[118] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 54, para. 9.

[119] Crawford, James. State Responsibility, lk 182-183.

[120] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 53, para. 5.

milles Rahvusvaheline Kohus leidis, et Iraan vastutab Ameerika Ühendriikide konsulaate hõivanud üliõpilaste käitumise eest, võttes arvesse Iraani käitumist pärast mässuliste poolt konsulaatide hõivamist. Rahvusvahelise Kohtu sõnul muutis ajatolla Khomeini ja teiste Iraani organite heakskiit konsulaadi hõivamisele oluliselt tekkinud olukorra õiguslikku sisu ning konsulaatide jätkuv okupeerimine ning pantvangide hoidmine muutus selle tõttu riigi poolt toimepandud tegudeks ning teo algselt toimepandud tudengid muutusid niiöelda riigi esindajateks.[121] Gabčíkovo-Nagymaros Projekti kaasuses leidis Rahvusvaheline Kohus, et kuna Slovakkia võttis omaks Ungariga 7. aprillil 1993. aastal sõlmitud erikokkuleppega kõik õigused ja kohustused, mis tulenesid Ungari ja Tšehhoslovakkia vahel 1977. aastal sõlmitud lepingust seoses Gabčíkovo-Nagymaros projektiga, siis võib Slovakkia olla vastutav mitte üksnes enda poolt toime pandud õigusvastase käitumise eest, vaid ka Tšehhoslovakkia poolt toimepandud rikkumiste eest.[122]

Riigivastutuse artiklite eelnõu kommentaaride kohaselt ei piisa üldjuhul riigile teatud käitumise omistamiseks artikli 11 alusel pelgalt sellest, et riik üksnes seda käitumist toetab või kiidab käitumise sõnadega heaks. Sellistel puhkudel riigivastutus ei tõusetu ning riik peaks võtma ette teatud samme, et oleks selge, et riik identifitseerib kõnealust käitumist justkui iseenda omana.[123] Sisuliselt peaks riik sedastama oma heakskiitu või toetust kirjalikult läbi ametlike kanalite või siis võtma vastu ametlikud otsused seoses sellega. Sellist seisukohta on aga kritiseeritud justnimelt seetõttu, et kui üksnes sõnalisest heakskiidust omistamise aluse tuvastamiseks ei piisa, siis kuidas on sellisel puhul võimalik omistada riigile teod, mille heakskiitmine riigi poolt on tuletatud üksnes selle riigi käitumisest, mida riigivastutuse artiklite eelnõu kommentaarid peavad võimalikuks.[124] Riigile ei peaks olema võimalik omistada tegusid, mille osas riik on andnud vaikiva nõusoleku, kuid omistamiseks peaks piisama siiski ka sellest, kui riigi kõrgeimad esindajad – president, peaminister vms – on avalikus ning ametlikus kõnes andnud selles riigis toimepandud või selle riigiga seotud rahvusvahelise õiguse vastastele tegudele heakskiidu ning on tunnustanud seda riigi suveräänsete huvidega kooskõlas olevana.

[121] United States Diplomatic and Consular Staff in Tehran, lk 36 para. 74.

[122] Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, I.C.J. Reports 1997, p. 7, lk 78, para. 151. Arvutivõrgus: http://www.icj-cij.org/docket/files/92/7375.pdf (04.05.2015).

[123] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 53.

[124] Crawford, James jt. The Law of International Responsibility, lk 275.

1.6. Tõendamine

1.6.1. Tõendamiskoormus

Tõendamisega seotud probleemistik jääb tihtipeale tagaplaanile, kuid omistamise teemat käsitledes ei saa tõendamisega seonduvast kuidagi kõrvale hiilida. Omistamine on protseduur, kus seotakse konkreetsed teod konkreetsete toimepanijatega ja need omakorda konkreetse riigiga. See tähendab, et tõendada tuleb nii asjaolu, et tegu on tõepoolest toime pandud, kes teo toime pani ning milline seos eksisteerib teo tegeliku toimepanija ning riigi vahel.

Tõendamiskoormuse üldtunnustatud põhimõte on, et vaidluse iga pool peab tõendama asjaolu, millele ta tugineb. Rahvusvaheline Alaline Kohus sõnastas juba oma 1925. aasta otsuses reegli, et tõendamiskoormus lasub poolel, kes väidab, et mingi õigusakt või –toiming on rahvusvahelise õiguse alusel tühine.[125] Kohtunik Lucio Moreno Quintana sedastas oma eriarvamuses Portugali ja India vahelises vaidluses, et "teatud õiguse olemasolu rahvusvahelistes suhetes on fakt, mida, juhul kui teine pool selle vaidlustab, tuleb tõendada selle poole poolt, kes õiguse olemasolule tugineb. See on elementaarne protseduurireegel."[126]

Eelmainitud tõendamiskoormuse põhimõte ei muutu isegi juhul, kui teisel poolel oleks märkimisväärselt lihtsam teatud asjaolu tõendada. Näiteks Avena kaasuses leidis Rahvusvaheline Kohus, et Ameerika Ühendriikidel oli kohustus tõendada, et kõnealused Mehhiko kodanikud olid ka Ameerika Ühendriikide kodanikud, hoolimata sellest, et kogu vajalik informatsioon oli suure tõenäosusega ainult Mehhiko käes. Rahvusvaheline Kohus leidis, et Ameerika Ühendriikidel oli seega kohustus nõuda vajadusel tõendid Mehhikolt välja.[127] Kohtunik Hisashi Owada tõdes oma eriarvamuses Naftaplatvormide kaasuses, et teatud eluliste asjaolude tõttu on mõningatel puhkudel on tõendite asümmeetria paratamatu,

[125] The Mavrommatis Jerusalem Concessions, (1925) P.C.I.J., Ser A. No. 5. On 26 March 1925, lk 30. Arvutivõrgus: http://www.icj-cij.org/pcij/serie_A/A_05/15_Mavrommatis_a_Jerusalem_Arret_19250326.pdf (04.05.2015). Vt ka: Nottebohm Case (second phase), Judgement of April 6th, 1955: I.C.J. Reports 1955, p. 4, Dissenting Opinion by Judge Read, lk 35-36. Arvutivõrgus: http://www.icj-cij.org/docket/files/18/2680.pdf (04.05.2015).

[126] Case concerning Right of Passage over Indian Territory (Merits), Judgrnent of 12 April 1960: I.C.J. Reports 1960, p. 6, Dissenting Opinion of Judge Moreno Quintana, lk 89. Arvutivõrgus: http://www.icj-cij.org/docket/files/32/4541.pdf (04.05.2015).

[127] Avena and Other Mexican Nationals (Mexico v. United States of America), Judgment, I.C.J. Reports 2004, p. 12, lk 34, para. 57. Arvutivõrgus: http://www.icj-cij.org/docket/files/128/8188.pdf (04.05.2015).

kuid sellistel puhkudel peaks Rahvusvaheline Kohus ise olema faktide tuvastamisel ja tõendite nõudmisel proaktiivsem.[128]

1.6.2. Tõendamisstandard

Teine aspekt, millel on määrav tähtsus teo omistamisel, on küsimus, millisel määral peab olema asjaolu tõendatud, et kohtud saaksid sellele asjaolule tugineda kui tõesele. Ühtset rahvusvahelist tõendamisstandardit loodud ei ole ning selle sõnastamine osutuks ilmselt võimatuks võttes arvesse, et tavapäraselt kohaldatakse erinevaid tõendamisstandardeid kriminaalasjadele ning tsiviilasjadele. Seega tuleb iga rahvusvahelisi vaidlusi lahendava organi puhul eraldi kontrollida, milline on selle konkreetse organi tõendamisstandard.

Rahvusvahelise Kriminaalkohtu Rooma statuut artikkel 66 lõige 3 sätestab *expressis verbis*, et süüdistatava süüdimõistmiseks peab kohus veenduma tema süüs mõistliku kahtluseta (*beyond reasonable doubt*). [129] Samasugust standardit kohaldavad ka Endise Jugoslaavia Rahvusvaheline Kriminaaltribunal ja Rwanda Rahvusvaheline Kriminaaltribunal. [130] Ka Euroopa Inimõiguste Kohus on oma jurisprudentsis korduvalt viidanud, et olulised asjaolud peavad olema tõendatud väljaspool mõistlikku kahtlust.[131]Eritrea-Etioopia Nõuete Komisjoni protseduurireeglid ei sätesta tõendamise standardit, kuid Komisjon sõnastas konkreetselt nõutava tõendamisstandardi Sõjavangide lahendis ning selleks standardiks on selged ja veenvad tõendid (*clear and convincing evidence*).[132] Ameerika Inimõiguste Kohus leidis, et kui väited on tõendatud veenval viisil (*in a convincing manner*), siis on nõutav tõendamisstandard täidetud.[133] Maailma Kaubandusorganisatsiooni vaidluste lahendamise organ on sõnastanud

[128] Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, p. 161, Separate Opinion of Judge Owada, lk 164 para. 47. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9733.pdf (04.05.2015).

[129] Rahvusvahelise Kriminaalkohtu Rooma statuut, vastu võetud 17.07.1998. Arvutivõrgus: https://www.riigiteataja.ee/akt/78574 (04.05.2015).

[130] Rules of Procedure and Evidence of the International Criminal Tribunal for the former Yugoslavia (as amended 22 May 2013), 11 February 1994. Arvutivõrgus: http://www.icty.org/x/file/Legal%20Library/Rules_procedure_evidence/IT032Rev49_en.pdf; Rules of Procedure and Evidence of the International Tribunal for Rwanda (as amended 10 April 2013), 29 June 1995. Arvutivõrgus: http://www.unictr.org/sites/unictr.org/files/legal-library/130410_rpe_en_fr.pdf (04.05.2015).

[131] Thienel, Tobias. The Burden and Standard of Proof in the European Court of Human Rights. German Yearbook of International Law. Berlin: Duncker & Humblot, lk 544.

[132] Prisoners of War, Eritrea's Claim 17. Eritrea Ethiopia Claims Commission, Partial Award of 1 July 2003, lk 41 para. 46-47. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_XXVI/23-72.pdf (04.05.2015).

[133] Velasquez Rodriguez Case, Judgment of July 29, 1988, Inter-American Court of Hunman Rights (Ser. C) No. 4 (1988), para. 129. Arvutivõrgus: http://www1.umn.edu/humanrts/iachr/b_11_12d.htm (04.05.2015).

lävendi, mille kohaselt peab pool tõendama enda väiteid selliselt, et tekiks *prima facie* eeldus, et väidetud asjaolud on tõesed, pärast mida tõendamiskoormus langeb teisele poolele, kes peab tõendama asjaolusid selliselt, et need lükkaksid ümber teise poole poolt esitatud faktid.[134] Mõned autorid on väljapakkunud, et Maailma Kaubandusorganisatsiooni vaidluste lahendamise organi tõendamisstandardiks sobiks pigem siiski tõendite ülekaalukus (*preponderance of evidence*).[135]

Rahvusvahelises Kohtus nõutavat tõendamisstandardit ei ole sätestatud ei Rahvusvahelise Kohtu statuudis, reeglites ega ka praktilistes juhistes ning Rahvusvaheline Kohus on oma praktikas formuleerinud mitmeid erinevaid tõendamisstandardeid ja kohaldanud erinevaid standardeid, mõnikord isegi ühe kohtulahendi sees.[136]

Corfu Kanali lahendis sõnastas Rahvusvaheline Kohus kolm erinevat standardit, milleks on: piisav kindlus (*degree of certainity*)[137], tõendid ei jäta ruumi põhjendatud kahtlusele (*no room for reasonable doubt*)[138] ning tõendid on piisavad, et neid pidada vaieldamatuteks tõenditeks (*conclusive evidence*).[139] Naftaplatvormide kaasuses leidis Rahvusvaheline Kohus, et kohus ei pea omistama vastutust lähtudes kogutud tõendite vahekorrast (*balance of evidence*) kui kättesaadavad tõendid ei ole kohtu silmis piisavad.[140] El Salvador ja Hondurase vahelises vaidluses tuvastas Rahvusvaheline Kohus olulise asjaolu, tuginedes tõenäosuste kaalumise meetodile (*balance of probabilities*).[141] Lisaks on mitmeid viiteid tõendamisstandarditele, mis

---

[134] Maailma Kaubandusorganisatsioon. Legal issues arising in WTO dispute settlement proceedings: Burden of proof. Arvutivõrgus: https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c10s6p1_e.htm (04.05.2015).

[135] Headen Pfitzer, James; Sabune, Sheila. Burden of Proof in WTO Dispute Settlement: Contemplating Preponderance of the Evidence. ICTSD Dispute Settlement and Legal Aspects of International Trade, April 2009, Issue Paper No. 9, lk 5. Arvutivõrgus: http://www.ictsd.org/downloads/2012/02/burden-of-proof-in-wto-dispute-settlement.pdf (04.05.2015).

[136] Del Mar, Katherine. The International Court of Justice and Standards of Proof. Artikkel raamatus: Bannelier, Karine (toim.). The ICJ and the Evolution of International Law: the Enduring Impact of the Corfu Channel Case. London; New York: Routledge, 2012, 2013, lk 99.

[137] Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, p. 4, lk 17. Arvutivõrgus: http://www.icj-cij.org/docket/files/1/1645.pdf (04.05.2015).

[138] Corfu Channel case, Judgment of April 9th, lk 18.

[139] Corfu Channel case, Judgment of April 9th, lk 17.

[140] Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, p. 161, lk 189, para. 57. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9715.pdf (04.05.2015).

[141] Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua intervening), Judgement, I.C.J. Reports 1992, p. 506, lk 159, para. 248. Arvutivõrgus: http://www.icj-cij.org/docket/files/75/6671.pdf (04.05.2015).

nõuavad kas piisavat kindlust (*sufficient certainty*), [142] kindlust (*with certainty*), [143] vaieldamatuid tõendeid (*conclusive evidence*)[144] või ka täielikult vaieldamatuid tõendeid (*fully conclusive evidence*). [145] Enamasti on Rahvusvaheline Kohus või kohtunikud oma eriarvamustes siiski tuginenud standardile, milles asjaolu peab olema tõendatud, et selle tõesus oleks väljaspool mõistlikku kahtlust (*beyond reasonable doubt*).[146]

Üldiselt võib öelda, et tõendamisstandard sõltub Rahvusvahelises Kohtus nii konkreetse vaidluse esemest ning menetluse etapist. Näiteks õiguskaitsevahendite kohaldamise etapis piisab sellest, kui kaebaja suudab esitada piisavalt veenvaid tõendeid näitamaks, et *prima facie* kuulub vaidlus Rahvusvahelise Kohtu jurisdiktsiooni alla.[147] Kui vaidluse ese on mingi asjaolu kehtivuse tunnistamine Rahvusvahelise Kohtu poolt - näiteks riigipiiri asukoha tuvastamine või konkreetse riigi suveräänsuse tunnistamine teatud ala üle – siis on tegemist deklaratiivse otsusega, mille puhul on nõutav tõendamisstandard madalam. Deklaratiivse otsuse näitena võib tuua Põhjamere mandrilava kaasuse, kus Rahvusvaheline Kohus sedastas, alljärgnevat: "Piiritlemine on protsess, mis hõlmab piiride määramist alale, mis põhimõtteliselt kuulub juba mingile rannikuäärsele riigile ja ei ole selle ala kindlaks määramine alustades täiesti

[142] Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Kooijmans, lk 108, para. 63. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9725.pdf. (04.05.2015)

[143] Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia), Judgment, I.C.J. Reports 2002, p. 625, lk 57, para. 124. Arvutivõrgus: http://www.icj-cij.org/docket/files/102/7714.pdf (04.05.2015).

[144] Oil Platforms (Islamic Republic of Iran v. United States of America), lk 38, para. 71.

[145] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), lk 90 para. 209.

[146] Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Kooijmans, lk 106, para. 56. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9725.pdf (04.05.2015); Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea intervening), Judgment, I.C.J. Reports 2002, p. 30, Dissenting Opinion of Judge Ajibola, lk 300, para. 194. Arvutivõrgus: http://www.icj-cij.org/docket/files/94/7471.pdf (04.05.2015); Maritime Delimitation and Territorial Questions between Qatar and Bahrain, Merits, Judgment, I.C.J. Reports 2001, p. 40, Separate Opinion of Judge Torres Bernárdez, lk 277 para. 157, lk 289 para. 195, lk 317 para. 268, lk 337 para. 324, lk 338 para. 327 ning lk 353 para. 369. Arvutivõrgus: http://www.icj-cij.org/docket/files/87/7047.pdf (04.05.2015); Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua intervening), Separate opinion of Judge Torres-Bernárdez, lk 336 para. 110, lk 378 para. 198. Arvutivõrgus: http://www.icj-cij.org/docket/files/75/6679.pdf (04.05.2015); South West Africa Cases (Ethiopia v. South Africa; Liberia v. South Africa), Preliminary Objections, Judgment of 21 December 1962: I.C.J. Report; 1962, p. 319, Joint Dissenting Opinion of Sir Percy Spender and Sir Gerald Fitzmaurice, lk 158, lk 196. Arvutivõrgus: http://www.icj-cij.org/docket/files/47/4925.pdf (04.05.2015); Case of Certain Norwegian Loans, Judgment of July 6th, 1957: I.C. J. Reports 1957, p. 9, Separate Opinion of Judge Sir Hersch Lauterpacht, lk 53. Arvutivõrgus: http://www.icj-cij.org/docket/files/29/4781.pdf (04.05.2015).

[147] Zimmermann, Andreas; Tomuschat, Christian; Oellers-Frahm, Karin (toim). The Statute of the International Court of Justice: A Commentary. Oxford: Oxford University Press, 2006, lk 829-830.

algusest."[148] Deklaratiivsete otsuste tegemisel on Rahvusvaheline Kohus lugenud asjaolu tõendatuks lähtudes tõenäosuste kaalumisest, kuigi puudub arvukalt tõendeid kummagi poole kasuks,[149] kohtunik Oda sõnas oma deklaratsioonis, et kuigi kumbki vaidluse pooltest ei suutnud piisavalt tõendada oma õigust vaidlusalustele saartele, suutis Malaisia esitada veenvamad argumendid (*more persuasive case*), mis ei olnud siiski väga tugevad absoluutses tähenduses.[150]

Tõendamisstandardi lävend muutub märkimisväärselt kõrgemaks, kui kohus peab tegema määrava otsuse (*determinative decision*). Määrava otsuse korral peab kohus otsustama, kas vaidluse pool on rikkunud oma juriidilisi kohustusi.[151] Erinevalt deklaratiivsest otsusest ei pea Rahvusvaheline Kohus määrava otsuse puhul tingimata otsusele jõudma. Kohus võib otsustada, et tulenevalt tõendite ebapiisavusest või ebaveenvusest, ei saa kohus nõuet rahuldada.[152] Küll aga pole Rahvusvaheline Kohus oma lahendites kunagi väga põhjalikult selgitanud, miks ta leiab, et teatud tõendid on ebapiisavad või ebaveenvad, eriti torkab see silma lahendites, kus mõlemad vaidluse pooled on esitanud väga arvukalt tõendeid.

Kohtunikud Rosalyn Higgins ja Thomas Buergenthal kritiseerisid oma eriarvamustes Naftaplatvormide kaasuses Kohut selle eest, et kuigi Kohus tugines tõendite ebapiisavusele, siis ei sõnastanud Kohus selgelt, millist tõendamisstandardit kasutati ja miks ta leidis, et see standard ei ole vaidluse poolte poolt täidetud.[153] Rosalyn Higgins sõnas oma eriarvamuses: "Peale üldise nõustumise, et mida tõsisem süüdistus, seda suurem peab olema kindlus tõendite osas, eksisteerib vähe abi pooltele, kes seisavad kohtu ees (ja kes teavad, et nad kannavad tõendamiskoormist) selles osas, et mis on tõenäoliselt Kohtu jaoks piisavateks tõenditeks. /.../ ÜRO põhiline kohus peaks /.../ tegema selgeks, millist tõendamisstandardit ta kasutab milliste asjaolude tuvastamiseks. Isegi kui Kohus ei soovi sõnastada üldist tõendamisstandardit kõikide

[148] North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3, lk 23, para. 18. Arvutivõrgus: http://www.icj-cij.org/docket/files/52/5561.pdf (04.05.2015).

[149] Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua intervening), lk 159, para. 248.

[150] Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia), Judgment, I.C.J. Reports 2002, p. 625, Declaration of Judge Oda, lk 66. Arvutivõrgus: http://www.icj-cij.org/docket/files/102/7716.pdf.

[151] Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14, Separate Opinion of Judge Keith, lk 111, para. 2. Arvutivõrgus: http://www.icj-cij.org/docket/files/135/15881.pdf.

[152] Del Mar, Katherine. The International Court of Justice and Standards of Proof, lk 104.

[153] Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Buergenthal, lk 129, para. 41. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9729.pdf (04.05.2015).

mitte-kriminaalkaasuste jaoks, siis peaks Kohus /.../ siiski otsustama, ja olema läbipaistev, tõendamisstandardi osas, mis on nõutud konkreetses vaidluses."[154]

Kohtunik Higginsi eriarvamuses sõnastatud põhimõttele, et mida tõsisem süüdistus, seda suurem kindlus tõendite osas, on viidanud Rahvusvaheline Kohus ka Bosnia Genotsiidi lahendis, kus sedastas, et nõuded riigi vastu, mis sisaldavad erakordselt tõsiseid süüdistusi peavad olema tõendatud täielikult vaieldamatute tõenditega.[155] Süüdistuse erakordne tõsisus sisaldab kahte elementi – viis, kuidas normi on väidetavalt rikutud ja väidetavalt rikutud normi olulisus. [156] Rahvusvaheline Kohus kohaldanud näiteks madalamat tõendamisstandardit olukordades, kus riigile heidetakse ette millegi tegematajätmist, mille tõttu on teisel riigil tekkinud kahju ning kõrgemat standardit, kui riigile heidetakse ette "aktiivselt" kahju tekitamist. Seda võib selgitada sellega, et üldiselt peetakse kahju tekitamist tõsisemaks rikkumiseks, kui kahju tekkimise ära hoidmata jätmist. Rikutud normi olulisus tuleneb eelkõige sellest, kas rikutud normi näol on tegemist *ius cogens* normiga või mitte. Seega on Rahvusvaheline Kohus kohaldanud ülikõrget tõendamisstandardit olukorras, kus riigile heidetakse ette aktiivse tegevusega *ius cogens* normi rikkumist (näiteks Bosnia Genotsiidi kaasus või Naftaplatvormide kaasus).

1.7. Vahekokkuvõte

Riikide rahvusvaheline vastutus on võrdlemisi noor õigusharu. Enne 19. sajandi lõppu tegeleti riigivastutuse küsimusega kaootiliselt ning enamasti läbi konkreetse õigusharu prisma. Riigivastutuse põhimõtete kodifitseerimist püüti alustada juba 20. sajandi esimesel poolel, kuid tulemusteta. Tänapäevase riigivastutuse instituudi kodifitseerimine sai hoo sisse alles 1960-aastatel. Riigivastutuse artiklite eelnõu kiideti heaks 2001. aastal toimunud ÜRO Peaassamblee istungil, mis lõplikult tsementeeris riigivastutuse doktriini kuulumise rahvusvahelise õiguse põhialuste hulka.

Riigivastutuse artiklite alusel vastutavad riigid tegude eest, mis rikuvad selle riigi mingit rahvusvahelist kohustust ning mis on riigile omistatavad. Üldtunnustatud rahvusvahelise õiguse põhimõtte alusel on riigile omistatavad eelkõige tema ametlike organite teod. Teatud puhkudel on riigile omistatavad ka mitteriiklike organite poolt toime pandud rahvusvahelise õiguse

[154] Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Higgins, lk 77, para. 33. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9721.pdf (04.05.2015).

[155] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), lk 90, para. 209.

[156] Del Mar, Katherine. The International Court of Justice and Standards of Proof, lk 106.

rikkumised. Näiteks on riigile omistatavad mitteriiklike üksuste teod juhul kui need üksused käitusid riigi juhendamise või suuniste või kontrolli all. Rahvusvahelises õiguses on sõnastatud kaks erinevat kontrollistandardit, mille puhul on rikkumised riigile omistatavad. Rahvusvahelise Kohtu efektiivse kontrolli standard nõuab, et lisaks olulise toetuse pakkumisele peab riik omama kontrolli ka iga operatsiooni üle, mille raames rahvusvahelise õiguse rikkumised toime pannakse. Sellele vastukaaluks lõi Endise Jugoslaavia Rahvusvaheline Kriminaaltribunal organiseeritud rühmituste jaoks oma kontrollistandardi, mille kohaselt piisab sellest, kui riigil on kontroll nende organiseeritud üksuste üle üldiselt ning ei ole nõutav et kontroll oleks olnud ka iga üksiku operatsiooni üle. Rahvusvaheline Kohus kinnitas Bosnia Genotsiidi lahendis, et efektiivse kontrolli standard on rahvusvaheline tavaõigus, mistõttu üksnes selle kohaldamine on õigustatud. Selline seisukoht pälvis laialdast vastukaja õigusteadlaste seas, kes sisuliselt leidsid, et efektiivse kontrollistandard on liigselt piirav ning vastuolus rahvusvahelise õiguse üldpõhimõtetega, mille kohaselt ei tohi riik kasutada mitteriiklike üksuseid, et oma vastutust välistada.

Rahvusvahelises õiguses (v.a. kriminaalõigus) kehtib üldjuhul tsiviilõigusest tuntud põhimõte, et tõendamiskoormis on sellel riigil, kes mingile asjaolule tugineb. Tõendamiskoormist ei mõjuta see, et tõendid asuvad näiteks üksnes teise riigi käes. Rahvusvahelisel Kohtul on näiteks õigus nõuda teatud tõendeid vaidluse poolteks olevatelt riikidelt välja, kuid praktikas ei ole ta seda võimalust eriti kasutanud. Rahvusvahelises õiguses puudub üks tõendamisstandard ning erinevad kohtud ja tribunalid kohaldavad erinevat tõendamisstandardit. Rahvusvahelised kriminaalkohtud ja –tribunalid nõuavad üldjuhul et asjaolud oleksid tõendatud väljaspool mõistlikku kahtlust olevatena. Kriminaalasjadega mittetegelevad kohtud on sõnastanud erinevaid standardeid. Siiski võib ilmselt lugeda üldtunnustatuks Rahvusvahelise Kohtu kohtunik Higgins'i sõnastatud põhimõtte, et mida tõsisem on süüdistus, seda suurem kindlus peab tõendites olema. Rahvusvaheline Kohtu tõendamisstandard oleneb paljuski sellest, kas kohus teeb deklaratiivse või määrava otsuse, millise menetlusetapiga on tegemist ning kui oluline on väidetavalt rikutud norm rahvusvahelise õiguse hierarhias. Bosnia Genotsiidi lahendis nõudis Kohus, et riigi vastutuse kohaldamiseks peavad asjaolud olema tõendatud väljaspool igasugust kahtlust olevatena.

2. Küberrünnakud ja omistamise tehnilised aspektid

2.1. Küberrünnaku definitsioon

Küberrünnaku, nagu ka kübersõja, ametlikku definitsiooni hetkel veel ei eksisteeri, küll aga on erinevad autorid välja pakkunud mitmeid erinevaid definitsioone. Kübersõda on defineeritud kui: "rahvusriigi tegevust teise riigi arvutitesse või võrkudesse tungimiseks eesmärgiga põhjustada kahjusid või segadust."[157] See definitsioon on praktilistel eesmärkidel kasutamiseks liiga kitsas, sest käsitleb üksnes rahvusriikide poolt toimepandud rünnakuid, selle definitsiooni kohaldamisalast jääks välja rünnakuid, mida võivad toime panna näiteks *Anonymous*[158] või al-Qaeda. Clarke ja Knake pakkusid välja ka täpsema definitsiooni, mille kohaselt "kübersõda on valitsuse poolt või valitsuse toetusel teise riigi arvutisse või võrku sissetungimine, või mingi muu tegevus, mis mõjutab arvutisüsteemi, mille eesmärk on lisada, muuta või võltsida andmeid või põhjustada katkestusi või kahjustada arvuteid, võrguseadmeid või esemeid, mida arvutisüsteem kontrollib."[159] Selle definitsiooni miinuseks on aga asjaolu, et selles ei ole eristatud küberkuritegevust, küberrünnakut ja kübersõda, ning on seetõttu liialt laialt defineeritud.[160]

Tallinn Manual defineerib küberrünnaku kui "küberoperatsioon, nii ründav kui ka kaitsev, mille puhul mõistlikult eeldatakse, et sellega põhjustatakse inimestele vigastusi või surm või kahjustatakse või hävitatakse esemeid.[161] *Tallinn Manual'ist* ei selgu, mida tähendab termin "küberoperatsioon" ning milliseid tegevusi see hõlmab. Lisaks võib mitte nõustuda *Tallinn Manual'*i koostanud ekspertide seisukohaga, et rünnakuks kvalifitseerub üksnes selline sekkumine arvutisüsteemidesse, mille tagajärjel tuleb füüsiliselt süsteemi osad asendada. On küsitav, miks ei saa küberrünnakuks kvalifitseeruda rünnak, mille tagajärjel kustutatakse

[157] Clarke, Richard A.; Knake, Robert K. Cyber War: The Next Threat to National Security and What To Do About It. New York: Ecco, 2010, lk 6.

[158] Anonymous on vabatahtlike häkkerite "rühmitus", mis korraldab aeg-ajalt DDoS rünnakuid riiklikele, usuorganisatsioonide või äriühingute kodulehtekülgedele. Vt ka: Kelly, Brian B. Investing In a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform. Boston University Law Review, Vol 92, 2012, lk 1678.

[159] Clarke, Richard A. jt. Cyber War: The Next Threat to National Security and What To Do About It, lk 228.

[160] Hathaway, Oona A.; Crootof, Rebecca; Levitz, Philip; Nix, Haley; Nowlan, Aileen; Perdue, William; Spiegel, Julia. The Law of Cyber-Attack. California Law Review, Vol 100, 2012, lk 823.

[161] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge; New York: Cambridge University Press, 2013, lk 106. Arvutivõrgus: https://issuu.com/nato_ccd_coe/docs/tallinnmanual/1?e=0/1803379 (05.04.2015).

arvutisüsteemist olulised failid infoga, mille taastamine võib osutuda keeruliseks või võimatuks, kuid süsteem ise asendamist ei vaja. Mõningad *Tallinn Manuali* eksperdid leidsid siiski ka, et oluline pole mitte viis, kuidas arvutisüsteemi kahjustatakse, vaid asja kasutamatuks muutumine on piisavaks kahjuks.[162]

Küberrünnakut on defineeritud kui "vaenulikku tegu, mis on toime pandud kasutades arvutit või sellega seotud võrkusid või süsteeme ja mille eesmärk on katkestada ja/või hävitada vastase olulisi kübersüsteeme, -varasid, -funktsioone." Soovitavad tagajärjed ei ole tingimata piiratud üksnes rünnatavate arvutisüsteemide või infoga – ka rünnakud arvutisüsteemidele, mille eesmärk on rikkuda või hävitada infrastruktuuri /.../ võivad olla küberrünnakud.[163] Selle definitsiooni miinuseks on asjaolu, et see seob küberrünnaku definitsiooni selle eesmärgiga. See tähendab, et selleks, et tuvastada, kas tegemist oli küberrünnakuga või mitte, tuleb välja selgitada ründaja täpne eesmärk, mis on praktikas keeruline ning aeganõudev. Seda arvesse võttes on püütud pakkuda välja alternatiivne definitsioon, mille kohaselt "küberrünnak koosneb igasugusest tegevusest, millega õõnestatakse arvutivõrgu toimimist poliitilise või rahvusliku julgeoleku eesmärgil."[164] Selle definitsiooni autorite silmis on igasugune riigi poolt kübermaailmas toime pandud rünnak seotud rahvusliku julgeolekuga,[165] mistõttu igasugune rünnak, mida saab riigile omistada (mis täidab eelnevad kriteeriumid), on küberrünnak.

Küberrünnaku definitsioon, mille kohaselt küberrünnak koosneb igasugusest tegevusest, millega õõnestatakse arvutivõrgu toimimist poliitilise või rahvusliku julgeoleku eesmärgil, on ka definitsioon, millele käesolevas töös tuginetakse. Seda eelkõige põhjusel, et "rahvusvahelise õiguse vastane tegu" riigivastutuse artiklite eelnõu artikkel 2 mõttes ei pea tingimata olema jõu kasutamine ÜRO harta artikkel 2 lõige 4 alusel või relvastatud rünnak harta artikkel 51 mõttes. Käesoleva magistritöö maht ja fookus ei võimalda analüüsida, millised küberrünnakud kvalifitseeruksid rahvusvahelise kohustuse rikkumiseks, kuid selleks võib teoreetiliselt olla ka näiteks teise riigi suveräänsuse rikkumine riigi arvutisüsteemidesse sissetungimise tõttu, mahukate teenusetõkestusrünnakute läbiviimine eesmärgiga takistada teise riigi elektroonilisi valimisi, mis kujutada endast teise riigi siseasjadesse sekkumist. Ka nö. madala intensiivsusega

[162] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 109.

[163] Cartwright, James E. Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories on Joint Terminology for Cyberspace Operations. 2011, lk 5. Arvutivõrgus: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (04.05.2014).

[164] Hathaway, Oona A. jt. The Law of Cyber-Attack, lk 826.

[165] Hathaway, Oona A., jt. The Law of Cyber-Attack, lk 830.

küberrünnakute jaoks on omistamise reeglite kohaldamine õigustatud, seega peab kasutatav terminoloogia seda peegeldama. Autor kahtles pikalt, kas termini "küberintsident" kasutamine oleks käesoleva töö raames täpsem, kuid see definitsioon hõlmab ka küberoperatsioone, mida panevad toime eraõiguslikud isikud teiste eraõiguslike isikute vastu üksnes erakasu eesmärgil, mistõttu langes valik termini küberrünnak kasuks.

2.3. Küberrünnakute liigid

2.3.1. Teenusetõkestusrünnakud

Teenusetõkestusrünnakud (*distributed-denial-of-service* ehk *DDoS attacks*) on rünnakud, mille puhul suur arv arvuteid üle terve võrgu ründavad mingit konkreetset Internetilehekülge. Sellise rünnaku eesmärgiks on serveri ülekoormamine ning seeläbi rünnatava lehekülje toimimise takistamine. Enamasti pannakse rünnak toime esmalt suurde hulka arvutitesse "sissetungimisega" ning nende arvutite viirusega nakatamisega, moodustades nakatunud arvutitest nö. *botnet*'i. *Botnet'*i on võimalik luua ka üksnes tarkvara võimaldamisega, mida inimesed võivad vabatahtlikult enda arvutisse laadida, et teatud eesmärgil *botnet'*is osaleda. Teenusetõkestusrünnak on seega mitmeastmeline, koosnedes esmalt *botnet*'i "ehitamisest" ja seejärel nakatunud arvutitele ühise ründamiskäskluse andmisest.[166] Laia *botnet*'i võrgustiku loomine on vajalik seetõttu, et kui ühest arvutist, serverist või isegi riigist tulevaid korduvaid päringuid on võimalik üsnagi lihtsalt blokeerida, siis juhul kui teenusetõkestusrünnakute puhul tulevad päringud väga paljudest erinevatest allikatest, ei suuda server ründajaid eristada legitiimsetest päringutest ning üksnes ründajate blokeerimine on peaaegu võimatu.[167] Serveri ülekoormamise tõttu ei ole Internetileheküljel võimalik täita ka legitiimsete kasutajate poolt saadetuid päringuid, mistõttu lehekülje töö on kas häiritud või täielikult katkestatud olenevalt saadetavate päringute hulgast ning .

Teenusetõkestusrünnakud on enamasti avalikud ning nende eesmärk ongi silma paista. See asjaolu ei lihtsusta aga kuidagi rünnakute päritolu tuvastamist. Seda eelkõige seetõttu, et kui tavapäraselt sisaldavad päringu teostamiseks saadetud paketid saatja IP-aadressi, sest saatja eesmärgiks on saada oma päringule vastus, siis teenusetõkestusrünnakute puhul võltsitakse enamasti pakettides saatja IP-aadressi, sest sihtkohalt vastust ei oodata. Seda probleemi

[166] Clark, David D.; Landau, Susan. Untangling Attribution. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press, 2010, lk 28.

[167] Nguyen, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare. California Law Review, Vol 101, 2013, lk 1097.

ilmestab eredalt järgnev olukord: 4. juulil 2009. aastal algas teenusetõkestusrünnak, mille sihtmärgiks oli kuni kakskümmend seitse Ameerika Ühendriikide ja Lõuna-Korea valitsusasutuste ning ettevõtete kodulehekülge, millest mitmed muutusid rünnakute tõttu ligipääsmatuteks. Lõuna-Korea valitsus vihjas, et rünnakud võis toime panna Põhja-Korea.[168] Mõned autorid leidsid, et rünnaku taga võis olla Hiina.[169] Rünnakus osales kokku rohkem kui 166 000 arvutit rohkem kui 74 riigis, mis teatud aja jooksul püüdsid luua iga 3 minuti jooksul ühendust kaheksa "juhtimise ja kontrolli serveriga". Võttes arvesse rünnakus osalenud arvutite kogust ning asjaolu, et need asusid niivõrd mitmes riigis, siis üksnes niiöelda masspäringuid teinud arvutite tuvastamisest kasu ei oleks olnud. Uurijad keskendusid rünnakute algallika otsimisele ning nad suutsid tuvastada serveri asukoha, mida kasutati nende kaheksa serveri kontrollimiseks. Server asus uurimistulemuste kohaselt Ühendkuningriikides, Brightoni linnas. Ekspertide hinnangul oli siiski väheusutav, et rünnaku põhiline organiseerija võis olla keegi Ühendkuningriikidest. Üksnes juhtserveri asukoha tuvastamisega uurimistulemused piirdusidki, ühtegi konkreetset isikut, rühmitust või riiki, kes võis rünnaku taga olla, tuvastada ei suudetud.[170] Seega ei ole siiani teada, kes rünnakuid koordineeris ning korraldas ning millistel eesmärkidel, hoolimata sellest, et ekspertidel oli andmeid nii rünnakus osalenud arvutite asukohtade, serverite ja põhiserveri asukoha kohta.

Kui algselt peeti teenusetõkestusrünnakuid üksnes väheolulisteks ja pigem lihtsalt tüütuks nähtuseks,[171] mille eesmärk oli lihtsalt segada ajutiselt arvutisüsteemide poolt pakutavaid teenuseid, siis üha suurem sõltuvus internetiteenuste kättesaadavusest on suurendanud teenusetõkestusrünnakute võimekust põhjustada suuri kahjusid.[172] Üheks esimeseks suuremaks teenusetõkestusrünnakuks riigi vastu[173] võib pidada Eesti vastu 2007. aasta aprillis ja mais, vahetult pärast Pronkssõduri teisaldamist, toime pandud rünnakuid. Teenusetõkestusründed toimusid Eesti valitsusasutuste, pankade ja *online*-meedia Interneti lehekülgede vastu. Rünnete

[168] Sang-Hun, Choe; Markoff, John. Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea. New York Times, 8.07.2009. Arvutivõrgus: http://www.nytimes.com/2009/07/09/technology/09cyber.html (04.05.2015).

[169] Hollis, Duncan B. An e-SOS for Cyberspace. Harvard International Law Journal, Vol 52, Issue 2, 2011, lk 397.

[170] Clarke, Richard A. jt. Cyber War: The Next Threat to National Security and What To Do About It, lk 25.

[171] Clarke, Richard A. jt. Cyber War: The Next Threat to National Security and What To Do About It, lk 13.

[172] Nguyen, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare, lk 1097.

[173] See ei tähenda, et tegemist oleks olnud kõige esimese poliitiliselt motiveeritud teenusetõkestusrünnakuga. Esimesed sellelaadsed rünnakud toimusid juba 1990-aastate lõpus. Vt ka: Nazario, Jose. Politically Motivated Denial of Service Attacks. The Virtual Battlefield: Perspectives on Cyber Warfare. IOS Press: Amsterdam, 2009.

tagajärjel oli takistatud neile lehekülgedele ligipääs ning pärsitud oli internetipankade töö. Tehniliselt küllaltki lihtsate rünnete tulemusena oli ohustatud ja takistatud riigi toimimine, seati ohtu ühiskonna eluviis ning sellega tekitati ulatusliku majandusliku kahju.[174] Rünnakutes osales umbes 85 000 arvutit, mis asusid rohkem kui 178 riigis, mis teeb rünnakutes osalenud arvutite kasutajate ning eelkõige rünnakute tegeliku väljatöötaja ja koordineerja tuvastamise vägagi keeruliseks.[175] Rünnakute toimepanemise eest võttis vastutuse hiljem Kremlimeelne noorteorganisatsioon Nashi, millel oli tol ajal küll ulatuslik Venemaa valitsuse toetus, kuid mis siiski oli iseseisev vabatahtlike ühendus.

Teenusetõkestusrünnakuid pandi toime ka 2008. aastal Gruusia vastu pärast Venemaa sissetungi Lõuna-Osseetiasse. Rünnakute tagajärjel koormati Gruusia küberinfrastruktuur üle automatiseeritud masspäringutega. Gruusia Internetiliiklus suunati läbi Venemaa serveritesse, kus need seejärel blokeeriti.[176] Rünnakute ajal ei olnud grusiinidel võimalik pääseda ligi näiteks välismaistele uudisteportaalidele ning ka e-kirjade riigist välja saatmine oli pärsitud. Rünnakute üheks sihtmärgiks olid Gruusia pangad, mis olid sunnitud rünnakute takistamiseks sulgema oma internetileheküljed, mistõttu ei olnud Gruusia Internetipankade kasutamine võimalik. Kuna pankade leheküljed olid suletud ning rünnete jätkamine osutuks võimatuks, siis sellele sammule vastasid ründajad rahvusvaheliste pankade vastu rünnakute alustamisega, maskeerides päringut teinud arvutite IP-aadressid selliselt, et jäi mulje nagu need tuleksid Gruusiast. Selle peale keelasid suuremas välismaised pangad igasugused internetipäringud Gruusiast, mis halvas sisuliselt kogu Gruusia panganduse.[177] Rünnakute toimepanijaid ei ole ametlikult tuvastatud, kuid üldiselt nõustutakse, et keegi siiski rünnakuid koordineeris ning juhiseid andis[178] ning on tõenäoline, et Venemaa oli mingil määral rünnakutega seotud.

Hiljutine teenusetõkestusrünnak riigi vastu toimus 2010. aastal Birmas, vahetult enne valimisi. Küberrünnaku raames rünnati Birma võrkusid, mille tagajärjel katkes Birmas sisuliselt igasugune internetiühendus välismaailmaga. Rünnaku toimepanemises kahtlustatakse eelkõige Birma sõjaväejuntat, mis suure tõenäosusega seda rünnakut koordineeris, et takistada

[174] Tikk-Ringas, Eneken. Küberjulgeoleku õiguslik raamistik. Juridica IV/2012, lk 277.

[175] Tsagourias, Nicholas. Cyber-attacks, Self-defence and the Problem of Attribution. Journal of Conflict and Security Law, Volume 17, Issue 2, 2012, lk 233.

[176] Ryan, Daniel J.; Dion, Maeve; Tikk, Eneken; Ryan, Julie J. C. H. International Cyberlaw: A Normative Approach. Georgetown Journal of International Law, Vol. 42, Issue 4, 2011, lk 1165.

[177] Clarke, Richard A. jt. Cyber War: The Next Threat to National Security and What To Do About It, lk 20.

[178] Tikk, Eneken, Kaska, Kadri, and Vihul, Liis. International Cyber Incidents - Legal Considerations, 2010, lk 74. Arvutivõrgus: https://ccdcoe.org/publications/books/legalconsiderations.pdf (04.05.2015).

informatsiooni vaba liikumist[179] ja mõjutada valimistulemusi.

2.3.3. Rünnakud operatsioonisüsteemide ja kontrollisüsteemide vastu

Lisaks teenusetõkestusrünnakutele on võimalik rünnata arvutisüsteeme ka sissetungimisrünnakutega. Sissetungimisrünnakud kasutavad ära süsteemi nõrkusi, et saada ligipääs arvutisüsteemile – see võib toimuda nii otsese süsteemi sissetungimisena kasutades ära süsteemi nõrkusi või kaudse sissetungimisena sisestades pahatahtliku arvutikoodi või pahavara (*malware*) arvutisüsteemi. Pahavara on tarkvara või kood, mis on spetsiaalselt loodud selleks, et kahjustada või takistada, varastada või tekitada muid kahjulikke tagajärgi sihtmärgiks oleva arvuti andmetele, võrkudele jne. Pahavara võib nakatada arvutisüsteeme kasutades ära operatsioonisüsteemi, võrguseadmete või tarkvara nõrkusi.[180] Pahatahtliku koodi näideteks on viirused, ussviirused (*worms*) ja "Trooja hobused".[181]

Viirused on arvutiprogrammid, mis seovad end tarkvara külge, kasutades seda tarkvara, et saavutada oma eesmärke, milleks võib olla kas arvutisüsteemi toimimise muutmine või kahjustamine, enda taastootmine ja levimine teistesse arvutitesse. Arvutiviirused levivas näiteks juhul kui viirusega nakatunud nö. emafaili või programmi saadetakse ühest arvutist teise.[182] Üks palju tähelepanu pälvinud viirus, nimega Shamoon, nakatas 2012. aastal rohkem kui 30 000 Saudi-Araabia naftaettevõttele, Saudi Aramcole, kuuluvat arvutit.[183] Shamoon võimaldas selle loojatel kustutada dokumente pealtnäha suvaliselt valitud Aramco arvutitest. Viirus rikkus nakatunud arvutites faile ja muutis masinad kasutuskõlbmatuteks. Viirusesse oli sisse ehitatud raporteerimisfunktsioon, mis saatis teatud informatsiooni tagasi viiruse loojale.[184] Shamoon ei tekitanud küll füüsilisi kahjustusi näiteks Aramco naftapuurimistehastes, kuid see rünnak näitab selgelt, et riigi olulised infrastruktuuriüksused on küberrünnakute poolt haavatavad. Viiruse väljatöötamise ja levitamise eest võttis vastutuse rühmitus *The Cutting*

[179] BBC News. Burma Hit by Massive Net Attack Ahead of Election. BBC News, 4.11.2010. Arvutivõrgus: http://www.bbc.co.uk/news/technology-11693214 (04.05.2015).

[180] Nguyen, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare, lk 1094.

[181] Antolin-Jenkins, Vida M. Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places? Naval Law Review, Vol 51, 2005, lk 139-140. Arvutivõrgus: http://www.jag.navy.mil/documents/navylawreview/nlrvolume51.pdf (04.05.2015).

[182] Nguyen, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare, lk 1095.

[183] Bronk, Christopher; Tikk-Ringas, Eneken. The Cyber Attack on Saudi Aramco. Survival: Global Politics and Strategy, Vol 55, Issue 2, 2013, lk 81.

[184] Bronk, Christopher jt. The Cyber Attack on Saudi Aramco, lk 85.

Sword of Justice, kuid rünnaku tegelikuks koordineerijaks peetakse Iraani.

Ussviirused, nagu teisedki arvutiviirused, levivad läbi enese taastootmise. Erinevalt viirustest on ussviirused iseseisev tarkvara, millel on võime end iseseisvalt kopeerida. Ussviirused kasutavad iseseisvalt nakatunud arvuteid, et leida uusi arvuteid, mida nakatada. Ussviiruste levimiseks ei ole vaja, et neid saadetaks teistese arvutitesse arvutikasutajate endi poolt vaid need sisenevad arvutisse läbi süsteemis esinevate nõrkuste ning kasutavad ära süsteemi failitranspordi või informatsioonitranspordi võimekust.[185] Üheks tuntuimaks ussviiruse näiteks on (väidetavalt) Ameerika Ühendriikide ja Iisraeli poolt välja töötatud ussviirus Stuxnet,[186] mille sihtmärgiks oli Iraanis, Natanzi linnas asuva tuumaenergeetika uurimisjaama arvutid. Viirus muutis gaasitsentrifuugide väljundsagedust lühikese perioodi jooksul 1410 Hz-ni, siis 2Hz-ni ja seejärel 1046Hz-ni. Väljundsageduse muutmine saboteeris sisuliselt automatsioonisüsteemi korrapärast toimimist[187] ning vaid mõne kuuga õnnestus viirusel kahjustada või hävitada rohkem kui üheksasadat tsentrifuugi. Gaasitsentrifuugide tööprotsessi kontrollinud isikud aga sageduse muutumist jooksvalt oma arvutisüsteemidest ei näinud.

Trooja hobused on arvutiprogrammid, mis varjavad oma tegelikku olemust, jättes endast mulje kui legitiimsest programmist. Kui kasutaja aktiveerib programmi, siis aktiveerub pahatahtlik kood ning see hakkab täitma teatud ülesandeid, näiteks koguma ja saatma sisestatud paroolid, kustutama või muutma faile, et muuta need kasutamatuteks või saadab viiruse omanikule paroolid, mis võimaldavad arvutisüsteemile kaugligipääsu.[188] Erinevalt viirustest ja ussidest, Trooja hobused ei kopeeri end ise ning ei levi teistesse arvutitesse.

2.2. Küberrünnakute omistamise tehnilised probleemid

Rünnakute toimepanija tuvastamine on rünnakute ärahoidmiseks ja nende eest karistamiseks

[185] Nguyen, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare, lk 1095.

[186] David E. Sanger, Obama Order Sped Up Wave of Cyberatacks Against Iran. Kuigi rünnaku algataja ja viiruse looja on ametlikult teadmata, siis arvestades viiruse erakordset täpsust ning sihtmärgi erakordset spetsiifilisust, on võimalike kahtlusaluste nimekiri lühike. Vt nt: Richardson, John. Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, lk 3. Kahtlustatakse, et Ameerika Ühendriigid ja Iisrael testisid Stuxnet'i mõju tsentrifuugidele Iisraelis Negevi kõrbes asunud salajases tuumarelvastusprogrammi kompleksis. Vt ka: Broad, William J.; Markoff, John; Sanger, David E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. The New York Times, 15. jaanuar 2011. Arvutivõrgus: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0. (04.05.2015)

[187] Richardson, John. Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. Journal of Computer & Information Law, Vol 29, 2011-2012, lk 7.

[188] Antolin-Jenkins, Vida M. Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?, lk 139.

ülioluline. Omistamise element, ehk võimalus öelda kes midagi tegi, on see, mis tagab õiguse töötamise.[189] Teo omistamine selle toimepanijale on keskne ka rünnakute tõrjumisel. Mõte võimalikust kättemaksust hoiab võimalikke ründajaid tagasi ning nad loobuvad rünnakute toimepanemisest. Teatud tegude tehniline omistamine riikidele on keeruline ka konventsionaalsete rünnakute puhul, kuid see muutub veelgi keerulisemaks kübermaailmas. Internet ei ole loodud eesmärgiga kedagi tagasi hoida,[190] seega ei ole see ka üles ehitatud nii, et küberrünnakute toimepanijate tuvastamine ja nende identifitseerimine oleks võimalikult lihtne.

Üheks olulisemaks takistuseks küberrünnaku tehnilise omistamise jaoks on üsnagi suur anonüümsus, mis võimaldab ründajal oma tegelikku identiteeti varjata. Internet on, väga lihtsustatult öeldes, pakettide vahetamise võrgustik, mis koosneb omavahel ühendatud sõlmedest, millest igaühele on antud teatud number, mida nimetatakse IP-aadressiks. IP-aadress indikeerib asukohta, aga ei anna infot selle kohta, kes on kasutaja. Teatud juhtudel on interneti teenusepakkujatel andmebaas, kus nähtuvad kõikide klientide andmed ning igale konkreetsele kliendile antud IP-aadress. Sellisel puhul on võimalik tuvastada Interneti kasutaja tema IP-aadressi alusel nõudes kohtuordeniga Interneti teenusepakkujalt vastav info välja. Teatud puhkudel aga on konkreetse kasutaja tuvastamine võimatu, sest võrk on kõikidele avalik ning isik on olnud võrgus väga lühikest aega, näiteks lennujaamades, hotelli aatriumites või kohvikutes.[191] Lisaks on oluline meeles pidada, et ühel ettevõttel võib olla näiteks tuhandeid arvuteid, kuid ainult üks väline sõlm, mis ühendab Internetiga ja seega ka üks IP-aadress.[192]

Internetis päringut tehes edastab päringu teinud arvuti teatud informatsiooniühiku, mis omakorda tükeldatakse väiksemateks ühikuteks, mida nimetatakse pakettideks. Igal paketil on pealkiri, mis sisaldab saatja kui ka sihtkoha IP-aadressi ning muud informatsiooni. Need paketid saadetakse ruuteritesse, mis on spetsialiseeritud arvutid, mis omakorda saadavad need edasi järgmisesse kõige mõistlikumasse ruuterisse kuni lõpuks jõuab informatsioon lõppsihtkohta. Lõppsihtkoht vastab päringule saates informatsioonipaketid tagasi päringu

[189] Glennon, Michael J. The Road Ahead: Gaps, Leaks and Drips. International Law Studies, Vol 89, 2013, lk 380.

[190] Clark, David D. jt. Untangling Attribution, lk 25.

[191] Clark, David D. jt. Untangling Attribution, lk 32.

[192] Pihelgas, Mauno. Back-Tracing and Anonymity in Cyberspace. Artikkel raamatus: Ziolkowski, Katharina (toim). Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCD COE Publication: Tallinn, 2013, lk 34.

teinud aadressile taaskord läbi ruuterite.[193] Juhul kui Internetti kasutatakse ilma internetiliikluse anonümiseerimisprogrammideta nagu näiteks Tor, siis on pakettide lähte- ning sihtkoha aadressid nähtavad igale ruuterile, mis paketi edastab ning igale muule monitoorimisseadmele, mis paketi liikumisteele jääb. Kui edastatud informatsioon on krüpteeritud, siis on paketi vahetamine lõpp- ning sihtkoha vahel anonüümne.[194] Kuna ruuterid ei kasuta paketis sisalduvat lähteaadressi,[195] siis on üsna lihtne saatja IP-aadressi võltsida nii, et jääb mulje, et päringu saatis hoopis teine masin.[196] See tähendab, et kõrgetasemelised ründajad võivad jätta mulje, et rünnaku taga on ükskõik milline indiviid, rühmitus või valitsus.[197]

Kasutusel on ka väga mitmeid erinevaid tehnilisi lahendusi, millega on võimalik tagada üsnagi suur anonüümsus kübermaailmas. Laialdaselt on kasutusel erinevad proksiserverid (*proxy servers*). Proksiserverid võimaldavad varjata päringu teinud isiku IP-aadressi seeläbi, et esialgu saadetakse päring proksiserverisse, seejärel saadab proksiserver päringu edasi lõppsihtkohta, kes saadab vastuse üksnes proksiserverile, mis omakorda edastab vastuse kliendile. See toob kaasa olukorra, kus veebiserver, millele sooviti päringut saata ei näe esialgse kliendi IP-aadressi, tal on informatsioon üksnes proksiserveri kohta.[198] Teine laialdaselt kasutusel olev võimalus on virtuaalse privaatvõrgu serverite (*virtual private network servers*) kasutamine. Virtuaalse privaatvõrgu serverite kasutamisel krüpteeritakse kogu info, mis edastatakse kliendilt serverisse ning olenevalt eesmärgist saadetakse kliendile tagasi või edastatakse Internetti. Virtuaalse privaatvõrgu serverid on kasulikud varjamaks kasutaja Interneti kasutamist ebaturvaliste ühenduste korral,[199] kuid neid on võimalik ka kuritarvitada, sest kõik päringud, mis tehakse läbi virtuaalse privaatvõrgu serverite kannavad üksnes serveri IP-aadressi, mistõttu võib rünnakute korral olla tegeliku kasutaja andmed tuvastamatud.

Kõige suuremat anonüümsust pakub aga nn. anonüümsusvõrgustiku kasutamine (*onion*

[193] Boebert, W. Earl. A Survey of Challenges in Attribution. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press, 2010, lk 41-42.

[194] Clark, David D jt. Untangling Attribution, lk 33.

[195] Clark, David D jt. Untangling Attribution, lk 27.

[196] Margulies, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. Melbourne Journal of International Law, Vol 14, 2013, lk 8.

[197] Hollis, Duncan B. An e-SOS for Cyberspace, lk 399.

[198] Pihelgas, Mauno. Back-Tracing and Anonymity in Cyberspace, lk 42.

[199] Pihelgas, Mauno. Back-Tracing and Anonymity in Cyberspace, lk 44.

routers). Anonüümsusvõrgustikud lõikavad kasu mitmetest avalikest või privaatsetest proksiserveritest, mis edastavad krüpteeritud informatsiooni läbi suvaliselt valitud võrgustiku sõlmede.[200] Iga sõlm, mis saab paketi suudab tuvastada ainult kaks asja – järgmise sõlme aadressi ja et pakett sisaldab teatud infot, millele sõlmel ligipääsu ei ole. Seega mitte ükski vahepealne sõlm ei tea paketi päritolu, selle lõppsihtpunkti ning selles sisalduvat infot. Paketis sisalduv info on krüpteeritud mitmetasandilisena nii, et iga paketi "liikumisteele" jääv sõlm "koorib" paketilt ühe kihi informatsiooni, kuniks pakett jõuab lõppserverisse, mis suudab tuvastada paketis sisalduva informatsiooni.[201]

Anonümiseerimisvõrgustike, proksiserverite, virtuaalse privaatvõrgu serverite ja muude samalaadsete süsteemide kasutamine muudab rünnaku algallika tuvastamise praktikas äärmiselt keeruliseks. Mõned autorid leiavad, et üksnes tehniliste indikaatorite ja informatsiooni põhjal isiku, keda saab pidada küberrünnaku eest vastutavaks, tuvastamine ei ole võimalik ning mitte keegi ei ole sellele lähedalegi jõudnud.[202] Teised jällegi leiavad, et omistamise probleem on ülehinnatud.[203] Ameerika Ühendriikide endine kaitseminister Leon Panetta leidis oma kõnes 2012. aastal, et Ühendriikide kaitseministeerium on teinud märkimisväärseid investeeringuid, et lahendada omistamise küsimust ning need on olnud tema sõnul tulemuslikud. Panetta hoiatas võimalikke ründajaid, et Ameerika Ühendriikidel on võimekus tuvastada nende asukoht ning võtta nad vastutusele.[204] Tehnilisi võimalusi rünnakute algallikate tuvastamiseks uuritakse ning arendatakse pidevalt, mõne näitena võib välja tuua külastuste salvestamise (*logging*) ning salvestuste tagasijälitamise (*traceback*), ruuterite poolt pakettide märgistamise või paketiga koos eraldi teate saatmine, mis võimaldavad paketi teekonda tuvastada.[205] Uuritakse ka uuenduslike võimaluste kasutuselevõttu nagu näiteks sissetulevate pakettide "vesimärgistamist", kus rünnaku korral märgib rünnatav sisse tulnud paketid ning need paketid saadetakse tagasi ründajale. Teatud sensorid erinevates asukohtades otsivad seejärel neid

[200] Pihelgas, Mauno. Back-Tracing and Anonymity in Cyberspace, lk 45.

[201] Boebert, W. Earl. A Survey of Challenges in Attribution, lk 46.

[202] Lin, Herbert S. Offensive Cyber Operations and the Use of Force. Journal of National Security Law and Policy, Vol 4, 2010, lk 77.

[203] McGhee, James E. Hack, Attack or Whack; The Politics of Imprecision in Cyber Law. Journal of Law & Cyber Warfare, Vol. 4, Issue 1, 2014, lk 37.

[204] Panetta, Leon E. Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York 11.10.2012. Transkriptsioon arvutivõrgus: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (04.05.2015).

[205] Wheeler, David A.; Larsen, Gregory N. Techniques for Cyber Attack Attribution. Institute for Defense Analyses, IDA Paper P-3792, October 2003, lk 10.

märgistatud pakette, mis võimaldab ära jätta aeganõudva tagasijälituse läbi sõlmede läbi mille pakett kohale jõudis.[206] Tuvastamiseks otsitakse vihjeid ka pahavara programmikoodist. Sealjuures tuleb arvestada, et igasugune turvalisuse tõstmine Internetis võib endaga kaasa tuua suure privaatsuse riive kodanikele ja kõige turvalisemate lahenduste rakendamine on tihtipeale väga ressursimahukad. Teiseks on tõsiasi, et ka küberründajad töötavad välja uusi ja kavalamaid võimalusi enda tuvastamise vältimiseks. Lisaks tehnilistele omistamise võimalustele kasutatakse omistamiseks ka teiseseid allikaid nagu näiteks luureinfot, poliitilist informatsiooni, sarnasusi eelnevate rünnakutega, mille läbiviija on tuvastatud varasemalt jne. Tihtipeale võib teisesed andmed osutudagi ainsaks informatsiooniks, mille põhjal on võimalik rünnaku korraldamine riigile omistada.

Mõned autorid leiavad sootuks, et kuigi Interneti toimimismehhanismidega seonduvate probleemidega tuleb tegeleda, siis ei maksa omistamise tehnilist külge ületähtsustada, sest käesoleval ajal on kübersõja vaagimise võimekus üksnes umbes kahekümnel üksusel üle terve maailma, millest pooled on riiklikud ja pooled on kriminaalsed rühmitused, millel on riikidega tihe side. Sellest tulenevalt on võimalike küberrünnakute korral kahtlusaluste ring väikene.[207] Niivõrd optimistiliku vaatenurgaga on aga siiski keeruline nõustuda. Lisaks küberrünnakute tehnilise omistamise probleemistikule on kübermaailmas ka tõendite kogumine väga suur väljakutse, sest digitaalsed tõendid on oma olemuselt väga erinevad mitte-digitaalsetest tõenditest. Oma olemuselt on digitaalsed tõendid kaduvad ja kergesti manipuleeritavad.[208] Digitaalsete tõendite muutmine on niivõrd lihtne, et see võib juhtuda ka kogemata. Lisaks on nende muutmine sisuliselt tasuta, kasutades arvutis juba olemasolevat tarkvara. Füüsiliste tõendite muutmine on seevastu kallim, nõuab rohkem teadmisi ja oskusi ning tahtlust. Teiseks on digitaalsete tõendite muutmist keerulisem tuvastada kui füüsiliste tõendite puhul. Kolmandaks on tekib digitaalset infot arvutites ning võrkudes meeletus koguses. Kogu selle informatsiooni läbitöötamine on võrreldav elektroonilisest heinakuhjast nõela otsimisega.[209]Võrgupõhised tõendid on veelgi problemaatilisemad, sest need on püsimatud,

[206] Kantzer, Kenneth Han-Wei. Cyber Attack Attribution: An Asymmetrical Risk to U.S. National Security. Bakalaureusetöö. Princeton: Princeton University 2011, lk 83. Vt ka: Wheeler, David A jt. Techniques for Cyber Attack Attribution; Lipson Howard F. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Carnegie Mellon University, 2002.

[207] Knake, Robert K. Internet Governance in an Age of Cyber Insecurity. Council Special Report, No. 56, September 2010, lk 14. Arvutivõrgus: http://www.cfr.org/internet-policy/internet-governance-age-cyber-insecurity/p22832 (04.05.2015).

[208] Schreier, Fred. On Cyberwarfare. DCAF Horizon 2015 Working Paper No. 7, lk 65.

[209] Chaikin, David. Network Investigations of Cyber Attacks: the Limits of Digital Evidence. Crime, Law and Social Change, Volume 46, Issue 4-5, December 2006, lk 241-242.

lühikese elueaga ning tihtipeale asuvad teistes riikides.[210] Üldiselt võib öelda, et rünnakute tehniline omistamine ei ole küll võimatu, kuid küberrünnaku omistamine vastasele lõplikult ja kindlalt, ei ole siiski alati võimalik.[211]

2.3. Vahekokkuvõte

Küberrünnakut on defineeritud mitmel erineval moel, olenevalt selle kasutamise konteksti poolt esitatud nõuetest. Ühtset ametlikku definitsiooni küberrünnaku kohta ei ole. Käesolevas töös mõeldakse küberrünnaku all igasuguseid tegevusesi, millega õõnestatakse arvutivõrgu toimimist poliitilise või rahvusliku julgeoleku eesmärgil. Selle definitsiooni alla kuuluvad nii teenusetõkestusrünnakud kui ka arvutisüsteemidesse "sissetungimine", kuid selle alla ei kuulu rünnakud ettevõtete või üksikisikute vastu, mille eesmärgiks on üksnes erakasu saamine.

Teenusetõkestusrünnakud on enamlevinumaiks küberrünnaku viisiks selle tehnilise lihtsuse tõttu. Teenusetõkestusrünnakute puhul nakatatakse arvutiviirusega arvuteid üle maailma, kes moodustavad *botnet*'i. Küberrünnakut alustades saadab *botnet* sihtmärgi Internetileheküljele masspäringuid, mis koormavad süsteemi. Hoolimata teenusetõkestusrünnaku tehniliselt lihtsat ülesehitusest on nende toimepanijate tuvastamine ülikeeruline. Internet on lihtsustatult öeldes pakettide võrgustik, kus kasutajad Internetis päringuid tehes saadavad päringud teatud IP-aadressile, mis seejärel "hakitakse" väiksemateks pakettideks ja edastatakse läbi ruuterite. Internet ei ole ehitatud eesmärgiga võimalikult lihtsalt ning tõsikindlalt teada saada, kes päringu on saatnud. Välja on töötatud ka palju erinevais viise, kuidas on võimalik oma identiteeti Internetis varjata. Selleks modifitseeritakse saadetud pakettide lähtekoodi, kasutatakse erinevaid proksivõrke või anonüümsusvõrgustikke. Lisaks on pahatahtlike teenusetõkestusrünnakute organiseerijate tuvastamine on keeruline, sest teenusetõkestusrünnakusse on arvutiviiruste levitamise teel kaasatud tihtipeale kümneid tuhandeid arvuteid üle kogu maailma. Riikide vastu toime pandud teenusetõkestusrünnakute näidetena võib välja tuua Eesti vastu 2007. aastal ning Gruusia vastu 2008. aastal toimepandud rünnakuid. Need rünnakud ilmestasid teravalt, et tulenevalt riikide ja nende elanike üha suuremast sõltuvusest Internetis pakutavate teenustest on teenusetõkestusrünnakud muutunud lihtsalt tüütust nähtusest rünnakuteks, millel on reaalne võimekus põhjustada suuri varalisi kahjusid ning sisuliselt halvata mõneks ajaks kogu riigi normaalne toimimine.

[210] Schreier, Fred. On Cyberwarfare, lk 65.

[211] Owens, William A.; Dam, Kenneth W.; Lin, Herbert S. (toim). Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. The National Academies Press: Washington, DC, 2009, lk 41.

Teiseks levinud küberrünnaku toimepanemise viisiks on arvutisüsteemidesse sissetungimine mingi pahavara teel. Pahavarasse on kodeeritud tema eesmärgid, milleks võib olla nii arvutisüsteemide töö muutmine, süsteemis leiduva info edastamine jne. Sissetungimisrünnaku näitena võib tuua ussviiruse Stuxnet, mis muutis Iraani tuumaprogrammis kasutusel olnud gaasitsentrifuugide töösagedust ning seeläbi kahjustas või rikkus üheksasada tsentrifuugi. Stuxnet'i viirus edastas gaasitsentrifuugide tööd kontrollinud arvutitele valeinformatsiooni, mistõttu ei olnud töösageduse muutumist võimalik tuvastada. Teiseks sissetungimisrünnaku näiteks on viirus Shamoon, mis kahjustas rohkem kui 30 000 Saudi-Araabia riikliku naftafirma arvutit.

Rünnakute kohta tõendite kogumine on keeruline, sest digitaalsete tõendite eluiga on lühike, nende muutmine lihtne ning nad võivad asuda üle terve maailma. Uusi tehnoloogiaid küberrünnakute lähtekohtade väljaselgitamiseks töötatakse pidevalt välja ning juba praegu on mitmeid erinevaid võimalusi nagu külastuste salvestamine ja tagasijälitamine, et ründajaid tuvastada. Tehniline omistamine on segu tehnilisest infost, luureinfost ning eksperthinnangutest poliitilisele olukorrale. Kuigi mõned autorid leiavad, et tehnilise omistamisega seonduvad probleemid on ülehinnatud, siis praktika on näidanud, et ainuüksi tehniliste vahenditega küberrünnakute tegelike toimepanijate tuvastamine väljaspool mõistlikku kahtlust olevana, ei ole tänasel päeval veel võimalik.

3. Küberrünnakute omistamine riigile

3.1. Riigiorganite küberrünnakud

Nagu esimeses peatükis juba selgitati vastutab riik riigivastutuse artiklite alusel oma organite poolt toime pandud tegude eest. Seega vastutab riik ka küberrünnakute eest, mille on läbi viinud tema organid või riigi poolt volitatud üksused. See rahvusvaheliselt üldtunnustatud rahvusvahelise õiguse põhimõte on kajastatud ka *Tallinn Manual*'i reeglis 6, mis näeb ette, et riik vastutab küberoperatsioonide eest, mis on talle omistatavad ja mis kujutab endast rahvusvahelise kohustuse rikkumist. Sellest tulenevalt on igasugune küberettevõtmine, mis on toime pandud riigi luureorganite, sõjaväe, sisejulgeoleku üksuste, tolli või mõne muu riigiorgani poolt, sellele riigile omistatav.[212]

Ka on mitmetel riikidel on olemas spetsialiseerunud sõjaväelised küberüksused nagu näiteks Iraani Küberarmee, Ameerika Ühendriikide Küberväejuhatus, Iisraeli Üksus 8200, Hiina Rahva Vabastusarmee Üksus 61398[213] ja Suurbritannia Ühendvägede Kübergrupp. Selliste üksuste poolt toimepandud rahvusvahelise õiguse vastased tegusid on võimalik vastavatele riikidele riigivastutuse artiklite alusel omistada.

Riigivastutuse artiklite artikkel 7 alusel on küberrünnakud riigile omistatavad ka siis, kui riigiesindajad, kes küberrünnakuid riigi nimel läbi viivad, ületavad oma ametlike volituste piire või lähevad vastuollu neile antud juhistega. Seega on riikidele omistatavad näiteks nende küberüksuste enda initsiatiivil toime pandud rünnakud, isegi juhul kui neil mõne konkreetse küberrünnaku alustamiseks puudub otsene riiklik ettekirjutus.

Artikli 5 alusel on riigile on omistatavad ka selle riigi poolt kübereesmärkide saavutamiseks palgatud erafirmade tegevus juhul kui need firmad täidavad mingisugust riiklikku funktsiooni – näiteks tagavad riigi küberjulgeolekut, tegelevad küberjulgeoleku tagamiseks vajalike vahendite arendamisega, koguvad küberruumis luureinfot jne. Artikkel 5 kohaldub siiski üksnes sellistele küberrünnakutele, mis on andud toime neile üksustele antud ametliku volituse

[212] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 31.

[213] Sanger, David E.; Barboza, David; Perlroth, Nicole. Chinese Army Unit Is Seen as Tied to Hacking Against U.S., The New York Times, 18. veebruar 2013. Arvutivõrgus: http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html (04.05.2015).

raames. Kui mõni küberjulgeoleku ülesannet täitev firma kasutab oma oskusi omakasu eesmärgil, siis see tegevus neid volitanud riigile omistatav ei ole.

Kui traditsiooniliste rünnakute puhul, mille toimepanemiseks kasutatakse riiklikke vahendeid, eelkõige riigi sõjaväelist varustust, ei teki enamjaolt küsimustki, kas rünnakuid on võimalik omistada sellele riigile, kelle vahendeid kasutatakse, siis küberrünnakute puhul see nii lihtne ei ole. Traditsiooniliste rünnakute puhul on üsna ebatõenäoline, et isikutel, kes ei ole mingi riikliku struktuuriüksuse osad, on võimalus kasutada riiklikke vahendeid – relvastust, vormi, ametitunnistust jms. Kuna kübermaailm erineb selles osas märkimisväärselt reaalsest maailmast, siis tõenäosus, et riiklikku küberinfrastruktuuri kasutatakse mitte-riiklike rühmituste poolt kasvab oluliselt.[214] Seetõttu ei ole võimalik omistada riigile automaatselt kõiki tegusid, mis pannakse toime riigi küberinfrastruktuuri kasutades.

Seda asjaolu peegeldab ka *Tallinn Manual*'i reegel 7, mis sätestab, et üksnes asjaolu, et küberrünnakut alustati või see pärineb mingi riigi riiklikust küberinfrastruktuurist ei tähenda automaatselt, et rünnakut oleks võimalik sellele riigile omistada, see asjaolu üksnes viitab sellele, et riik võib rünnakuga seotud olla.[215] Reegli 7 kohaldamiseks ei ole oluline, kas riikliku küberinfrastruktuuri omanikuks on riik või on omanikuks eraõiguslik ühendus ja riik üksnes üürib neilt seda taristut. Ka ei ole oluline milliseks riiklikuks ülesandeks taristut kasutatakse ja millise võimuharu poolt.[216] *Tallinn Manual'is* kahjuks ei selgitata kas ja millistel tingimustel oleks küberoperatsiooni omistamine riigile, kelle infrastruktuuri rünnakute toimepanemiseks kasutatakse, õigustatud tulenevalt selle riigi tegevusetusest juba toimuva küberoperatsiooni peatamisel või takistamisel. [217] Kuna riikidel on enamasti suur võimalus kontrollida omaenda küberinfrastruktuuri, siis riigi tegevusetust toimuva küberrünnaku takistamiseks saab ilmselt pidada veel üheks vihjeks, et riik tõenäoliselt on küberrünnakuga seotud. Siiski oleks ilmselt ebaõige üksnes selle asjaolu põhjalt väita, et see riik on tingimata küberrünnaku korraldamise taga.

Tallinn Manual'i reeglit 7 ei saa kohaldada aga juhul, kui küberrünnak on üksnes suunatud läbi mingi riikliku kübertaristu, mitte ei pärine sealt algselt. Sellist olukorda puudutab *Tallinn*

[214] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 35.

[215] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 34.

[216] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 35.

[217] Fleck, Dieter. Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual. Journal of Conflict & Security Law, Volume 18, Issue 2, 2013, lk 339.

Manual'i reegel 8, mis sätestab, et üksnes asjaolu, et rünnak on suunatud läbi mingis riigis asuva küberinfrastruktuuri ei ole piisavaks tõendiks, et omistada rünnak riigile, mille küberinfrastruktuuri kasutatakse.[218]. See tähendab, et isegi kui rünnatav riik suudab tuvastada, et rünnak tuleb mõne teise riigi kübertaristust, siis on tal vaja ka tuvastada, et rünnak ei ole üksnes suunatud läbi selle taristu.

Küberrünnaku "tagasijälitamine" selle algallikani on väga keeruline tehniline väljakutse, kuid juhul kui küberrünnaku sihtmärgiks olev riik suudab edukalt jälgi ajades tuvastada, et rünnaku toimepanijaks on näiteks teise riigi küberüksus või riiklike ülesandeid täitev erafirma, siis on võimalik sellele teisele riigile küberrünnakut omistada ning teda selle eest vastutusele võtta.[219] Senise praktika kohaselt pannakse siiski enamus küberrünnakuid toime mitteriiklike rühmituste poolt ja on üsna ebatõenäoline, et see lähiajal drastiliselt muutuks. [220]

3.2. Mitteriiklike organite küberrünnakud

Teatud juhtudel on riikidele omistatavad ka riigiväliste isikute poolt toime pandud teod. Mitte-riiklike rühmituste poolt toimepandud küberrünnakute omistamiseks riigile riigivastutuse artiklite artikkel 8 alusel on vaja, et küberrünnakud oleksid toime pandud riigi juhendamisel või riigi suunamise või kontrolli all. Riigid võivad palgata küberoperatsioonide läbiviimiseks erafirmasid, kasutada mitteriiklike küberüksuseid [221] või kutsuda üles eraisikuid, nn. "häktiviste", et nood viiksid läbi küberoperatsioone mõne teise riigi vastu.[222]

Kui mitte-riiklikud rühmitused on täielikult sõltuvad neid toetavast riigist, ning riigil on rühmituse üle täielik kontroll, siis on selle rühmituse näol tegemist *de facto* riigiorganiga. Kui rühmitus loetakse *de facto* riigiorganiks, siis on võimalik selle poolt toimepandud

[218] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 36.

[219] Gervais, Michael. Cyber Attacks and the Laws of War. Berkeley Journal of International Law, Vol 30, Issue 2, 2012, lk 545.

[220] Shackelford, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkeley Journal of International Law, Volume 27, Issue 1, 2009, lk 234.

[221] Näiteks Eesti Kaitseliidu Küberkaitse üksuse poolt toimepandud võimalikud küberrünnakud oleksid tõenäoliselt Eesti riigile omistatavad. Vt ka: Shackelford, Scott J.; Andres, Richard B. State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. Georgetown Journal of International Law, Vol 42, 2001, lk 987.

[222] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 32. Vt ka: Hoffman, David E. The New Virology. From Stuxnet to biobombs, the future of war by other means. Foreign Policy, 21. veebruar 2011, milles autor on seisukohal, et riigid nagu Hiina ja Venemaa julgustavad vabakutselisi häkkereid küberoperatsioone elluviima, mis võimaldab riikidel usutavalt eitada enda osalust. Arvutivõrgus: http://foreignpolicy.com/2011/02/21/the-new-virology/ (04.05.2015).

küberrünnakud omistada riigile samade põhimõtete alusel nagu ametlike organite poolt korraldatud rünnakuid – s.h kui rahvusvahelise õiguse rikkumised pandi selle rühmituse poolt toime *ultra vires*.

Kui täielikku sõltuvust riigi ja küberrünnaku toimepannud mitte-riikliku rühmituse vahel ei esine või ei suudeta tõendada, siis lähtuvalt Rahvusvahelise Kohtu poolt Nicaragua lahendis sõnastatud ja Bosnia Genotsiidi lahendis kinnitatud, efektiivse kontrolli standardis alusel oleksid küberrünnakud riigile omistatavad, kui riik konkreetselt juhendab või nõuab küberrünnakute toimepanemist, riik täielikult kavandab operatsiooni strateegia või taktika, kontrollib igat küberoperatsiooni ja kõiki konflikti faase, s.t. efektiivse kontrolli standardi kohaldamisel peab esinema efektiivne kontroll terve konflikti jooksul ning kõigi toimepandud küberoperatsioonide üle. Efektiivse kontrolli standard on sellest tulenevalt väga kõrge. Nagu käesoleva magistritöö esimeses peatükis juba mainitud, on efektiivse kontrolli standard saanud teatava kriitika osaliseks ning mõningate autorite arvates ka praktikas ebarealistlik ning ebaõiglane.[223]

Võttes arvesse kübermaailma eripärasid on efektiivse kontrolli standardi kohaldamise teel riigile küberrünnaku omistamise teel riigivastutuse kohaldamine veelgi ebarealistlikum võrreldes traditsiooniliste rünnakutega. Esiteks võivad riigid kasutada küberrünnakute toimepanemiseks mitteriiklike rühmitusi justnimelt seetõttu, et kasutada ära selliste rühmituste oskusteavet kübermaailmast. Kui traditsiooniliselt on olnud riikidel sisuliselt monopol teatud sorti oskusteabe, relvastuse ning luureinfo osas, mis annab riikidele märkimisväärse eelise rünnakute organiseerimiseks, strateegia välja töötamiseks ning isikute koordineerimiseks, siis küberrünnakute toimepanemiseks on vaja üksnes arvutit, internetti ning teadmisi kuidas kübermaailm töötab. Teadmised arvutisüsteemide tehnilistest aspektidest, nende nõrkustest, arvutiviiruste jaoks koodi kirjutamisest ja efektiivsete levitusviiside leidmisest on kättesaadavad sisuliselt igaühele, kes sellest vähegi huvitatud on. Kui riik annab mitteriiklikule "häktivistide" ühendusele raha, luureinfot rünnaku sihtmärgi kohta, varustust ning seab ette eesmärgid, mida rünnakuga saavutada tuleks, kuid jätab konkreetse rünnaku tehnilise organiseerimisega seotud võimaluste valiku sellele rühmitusele ning riik teostab rühmituse üle järelvalvet, kuid ei anna konkreetseid juhiseid konkreetse operatsiooni jaoks, siis efektiivse kontrolli standardi alusel riigile küberrünnakute omistamine võimalik ei oleks.

[223] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Dissenting opinion of Judge Sir Robert Jennings, lk 533.

Teiseks on Rahvusvaheline Kohus püstitanud riigi vastutusele kõrge tõendamisstandardi, Näiteks Bosnia Genotsiidi lahendis leidis kohus, et asjaolu tuleb tõendada väljaspool igasugust kahtlust olevana ja mitte üksnes väljaspool mõistlikku kahtlust.[224] See tähendab, et küberrünnaku ohvriks langenud riik peab tõendama väljaspool igasugust kahtlust olevana selle, kust rünnak pärines, kes rünnaku toime pani, milline riik rünnakut kontrollis ning selle, et rünnaku toimepannud isikute rühmituse üle rakendati efektiivset kontrolli iga küberrünnaku aspekti üle. Nagu mainitud käesoleva magistritöö teises peatükis, ei ole tänasel päeval võimalik üksnes tehnilistele tõenditele tuginedes tuvastada küberrünnaku toimepanijat. Kuigi Rahvusvaheline Kohus on oma praktikas aktsepteerinud ka kaudseid tõendeid, siis asjaolu tõendamiseks väljaspool igasugust kahtlust kaudsetest tõenditest suure tõenäosusega ei piisa ning efektiivse kontrolli standardi kohaldamiseks vajalikku tõendamiskoormise täitmine on seetõttu praktiliselt võimatu.

Seda probleemi võib aidata ületada kohtunik Higginsi poolt sõnastatud põhimõte, et mida tõsisem süüdistus, seda suurem kindlus peab tõendite osas olema. See tähendab, et mida tõsisem on toimepandud küberrünnak, seda rohkem tõendeid peab küberrünnaku ohvriks langenud riik esitama. Näiteks kui riik süüdistab teist mõne *jus cogens* normi rikkumises (nt jõu kasutamises ja seeläbi ÜRO harta artikkel 2 lõige 4 rikkumises), siis on sellisel puhul peab olema suurem kindlus tõendites kui näiteks juhul kui küberrünnakuga rikuti riigi suveräänsust.

Mitmete autorite silmis on küberrünnakute omistamiseks riigile sobilikum kasutada Endise Jugoslaavia Kriminaaltribunali poolt sõnastatud üldise kontrolli standardit.[225] See seisukoht ei ole aga kindlasti universaalne. Mõned autorid leiavad, et võttes arvesse asjaolu, et küberrünnakute puhul on ründaja identifitseerimine problemaatiline, siis kaitseb üksnes efektiivse kontrolli standard riike asjatute nõuete eest.[226] Mõningad autorid toetavad Tribunali

[224] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), lk 179, para. 442.

[225] Shackelford, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, lk 235; Shackelford, Scott J.; Andres, Richard B. State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, lk 988.

[226] Roscini, Marco. World Wide Warfare: Jus ad bellum and the Use of Cyber Force. Max Planck Yearbook of United Nations Law, Volume 14, 2010, lk 100. Lisaks ei ole Roscini arvates üldise kontrolli test asjakohane, sest seda saab kohaldada üksnes organiseeritud ja hierarhilise struktuuriga ühendustele ning peaaegu ühtegi sellist organiseerunud küberrühmitust ei eksisteeri. Michael Gervais seevastu leiab aga, et paramilitaarsel rühmitusel Russian Business Network, kes on tõenäoliselt seotud Eesti ja Gruusia vastu toimepandud teenusetõkestusrünnakutega, on Venemaa võimu- ja sõjaväeeliidiga niivõrd tihedad sidemed, et RBN'i poolt toimepandud teod oleksid Venemaale omistatavad. Vt ka: Gervais, Michael. Cyber Attacks and the Laws of War, lk 548

seisukohta mille kohaselt võib kasutatav kontrollistandard oleneda konkreetsetest asjaoludest.[227]

Endise Jugoslaavia Kriminaaltribunali apellatsioonikoda leidis, et riigile teatud tegevuse omistamiseks ei pea sellel riigil olema kontroll iga konkreetse operatsiooni üle, mille käigus rahvusvahelise õiguse vastased teod toime pandi, vaid piisab sellest, et riik kontrollib rühmituse sõjalist tegevust üldiselt. Riik peab lisaks rühmituse rahastamisele, treenimisele, varustamisele ja muule operatiivse toetuse pakkumisele ka üldiselt organiseerima, koordineerima või planeerima rühmituse sõjalist tegevust. Professor Nicholas Tsagourias leiab, et üldise kontrolli standardit kohaldades oleks võimalik omistada riigile küberrünnakud, mille on elluviinud "häktivistide" rühmitus, kellele riik on pakkunud tehnilist või muud tuge ja kelle tegevust riik organiseeris, isegi kui riigi osalust konkreetses küberrünnaku etapis ei ole võimalik rahuldavalt tõendada.[228]

Riigivastutuse artiklite artikkel 11 alusel on üksikisikute ja mitteorganiseerunud rühmituste puhul on küberrünnakud riigile omistatavad ka juhul kui riik on küberrünnaku heaks kiitnud ja enda omaks tunnistanud *ex post facto*. Riigivastutuse artiklite artikkel 11 alusel on võimalik küberrünnakut riigile omistada kui riik on seda küberrünnakut, olgu siis organiseerunud või mitteorganiseerunud rühmituse või üksikisikute poolt toime pandud, tingimusteta heaks kiitnud või tunnustanud seda kui enda poolt toime pandud rünnakut. Riigivastutuse artiklite artikli 11 alusel ei piisa omistamiseks siiski üksnes sellest, kui riik kiidab küberoperatsiooni vaikivalt heaks või ei tee seda ametlikult. Näiteks olukorras, kus riigi A "häktivistid" alustavad riigi B vastu väga suuremahulise teenusetõkestusrünnakut (sest nad ei nõustu riigi B hiljutise poliitilise väljaütlemisega) ning riigi A valitsus ei mõista "häktivistide" omaalagatuslikku rünnakut avalikult hukka ega ei tee selle rünnaku takistamiseks või lõpetamiseks mingisuguseidki pingutusi, siis sellest olenemata ei ole võimalik väita, et riik A oleks "häktivistide" küberrünnaku vaikivalt heaks kiitnud ja omaks võtnud. Sellisel juhul oleks võimalik hinnata, kas riik A on rikkunud oma hoolsuskohustust, kuid küberrünnakut riigile A otse omistada ei saaks.

Riik võib heaks kiita ja omaks võtta ka üksnes teatud osa küberrünnakust. Praktika on näidanud, et väljaspool riikliku järjepidevuse raamistikku on riikide poolt vabatahtlikult vastutuse

[227] Tsagourias, Nicholas. Cyber-attacks, Self-defence and the Problem of Attribution, lk 238; Cassese, Antonio. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, lk 657.

[228] Tsagourias, Nicholas. Cyber-attacks, Self-defence and the Problem of Attribution, lk 238.

võtmine haruharv nähtus.[229] Kui lisada veel küberrünnakute tehnilise omistamise probleemid ning tõendite kogumisega seonduvad probleemid, mis üsna lihtsalt võimaldavad riigil seotust mingi küberrünnakuga eitada, siis on üsna vähetõenäoline, et mõni riik võtaks vabatahtlikult vastutuse mingite mitteriiklike üksuste poolt toimepandud küberoperatsioonide eest.

Võttes arvesse omistamise tehnilist keerukust, riigivastutuse doktriini ülikõrget tõendamisstandardit, digitaalsete tõendite kogumisega ning usaldusväärsusega seotud probleeme, siis võib väita, et küberrünnakute omistamine riikidele riigivastutuse sätete alusel on vähemalt praegu sisuliselt peaaegu võimatu. Näiteks pärast Eesti vastu toime pandud teenusetõkestusrünnakut 2007. aastal, suudeti see rünnak tagasijälitada Venemaani, kuid Venemaa valitsusega neid rünnakuid siduda ei õnnestunud. Sarnaselt tuvastas Gruusia, et tema vastu 2008. aastal toime pandud teenusetõkestusrünnakud tulenesid Venemaalt, kuid ka Gruusia ei suutnud neid rünnakuid Venemaa valitsusele ametlikult omistada. Ameerika Ühendriikide kõrged ametnikud olid seisukohal, et 2007. aastal toimepandud küberrünnak Pentagoni vastu oli sponsoreeritud Hiina poolt, kuid piisavat sidet Hiina ja rünnaku toimepanijate vahel ei suudetud siiski tõendada.[230] See näitab, et ka üksnes tehniline omistamine ei ole praktikas eriti lihtne. Juhul kui riigil õnnestuks küberrünnak riigile tehniliselt omistada, siis õiguslik omistamine toob kaasa veelgi probleeme.

Efektiivse kontrolli standardi kohaldamine tuvastamaks, kas riigile on võimalik omistada teatud organiseeritud rühmituse poolt toime pandud küberrünnakuid on väga piirav ning see võib muuta küberrünnakute omistamise sisuliselt võimatuks. Üldise kontrolli standard on küll veidikene vähem piiravam, sest tõendada ei ole vaja, et riigil oli kontroll iga konkreetse operatsiooni üle, kuid üldise kontrolli standard kohaldub üksnes organiseeritud rühmituste poolt toime pandud rahvusvahelise õiguse rikkumistele. Kübermaailmas on mitmeid "häktivistide" rühmitusi, kõige tuntum neist *Anonymous*, millel puudub selge hierarhia ja käsuliin, kuid mis sellest hoolimata on arvestatavaks ohuks riikide küberturvalisusele. Hoolimata püüetest ühtse poliitika kujundamiseks on suurimatel küberriikidel nagu Ameerika Ühendriigid, Hiina ning Venemaa vägagi erinevad vaatenurgad kübermaailma korraldamisele,

[229] United Nations. Materials on the Responsibility of States for Internationally Wrongful Acts. New York: United Nations, 2012, lk 93.

[230] Sklerov, Matthew J. Solving The Dilemma Of State Responses To Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent. Military Law Review, Volume 201, Fall 2009, lk 8.

mistõttu ei ole usutav, et lähitulevikus leitaks üksmeel seoses küberrünnakute omistamise standardite osas.

Küberrünnakute omistamise praktiline võimatus riigivastutuse artiklite alusel ei tähenda aga, et riike ei saaks küberrünnakute eest üldse vastutusele võtta. Nagu esimeses peatükis mainitud, riigivastutuse artiklite eelnõu koosneb rahvusvahelise õiguse teisestest normidest. Vastutus rahvusvahelise õiguse vastaste tegude eest võib tuleneda ka primaarnormide alusel. Riigi vastutus küberrünnakute eest võib tekkida ka seetõttu, et ta ei täitnud oma primaarnormist tulenevat hoolsuskohustust.

3.3. Kaudne vastutus küberrünnakute eest

Otsese vastutuse doktriini kohaselt vastutab riik juhul kui riigi rahvusvahelist kohustust rikkunud teo pani toime (või jättis tegemata) riigi esindaja või agent või juhul kui teo pani toime mitteriiklik üksus, kelle üle on riigil kontroll. Kaudset vastutust saab kohaldada juhul kui riigi ja teo toimepanija vahel ei ole ametlikku seost või kontrolli või seda ei suudeta tõendada.[231] Riigi ükskõiksus oma territooriumil toimuva (terroristliku) tegevuse vastu või suutmatus sellist tegevust kontrollida toob kaasa riigi vastutuse nende rünnakute eest justkui oleks riik otseselt selles rünnakus osalenud.[232] Kaudse omistamise korral ei omistata riigile seega mitte mingisugust konkreetset rahvusvahelist kohustust rikkunud tegu või tegevusetust vaid riigile omistatakse tema suutmatus täita rahvusvahelisest õigusest tulenevaid kohustusi, mis rikub teiste riikide õiguseid.[233]Näiteks juhul kui riik palkas mitte-riikliku rühmituse teises riigis mingit sõjaväelist operatsiooni ellu viima, kuid riigi rakendatud efektiivset kontrolli selle rühmituse poolt toimepandud tegude üle ei suudeta tõendada, mistõttu otsene omistamine on välistatud, siis riik võib kaudse omistamise teel vastutada selle eest, et ta sekkus selle mitte-riikliku rühmituse palkamisega keeldu sekkuda teise riigi siseasjadesse.

Mõningate autorite silmis on riikide pühendumine terrorismivastasele võitlusele muutnud kaudse vastutuse doktriini rahvusvahelise vastutuse määramisel valdavaks ning otsene

[231] Proulx, Vincent-Joël. Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks? Berkeley Journal of International Law, Volume 23, Issue 3, 2005, lk 623.

[232] Vt ka: Ahmed, Dawood I. Defending Weak States against the Unwilling or Unable Doctrine of Self-Defense. Journal of International Law and International Relations, Volume 9, 2013.

[233] Brown, Davis. Use of Force against Terrorism after September 11th: State Responsibility, Self-Defense and Other Responses. Cardozo Journal of International and Comparative Law, Vol. 11, Issue 1, 2003, lk 13.

omistamine riigivastutuse sätete alusel on jäänud seetõttu tagaplaanile.[234]

Kaudse vastutuse kohaldamiseks on esmajoones vaja tuvastada, millised on riigi rahvusvahelised kohustused rahvusvahelise õiguse alusel. Corfu Kanali kaasuses sõnastas Rahvusvaheline Kohus põhimõtte, mille kohaselt ei tohi riik teadlikult lubada oma territooriumi kasutada teiste riikide õiguste rikkumiseks.[235] 24. oktoobril 1970. aastal kiitis ÜRO Peaassamblee heaks deklaratsiooni sõbralike suhete ja koostöö kohta riikide vahel, mille kohaselt on igal riigil kohustus hoiduda tsiviilkonfliktide või terroriaktide organiseerimisest, alustamisest, abistamisest või neis osalemisest või vaikivalt nõustuda enda territooriumil organiseeritud tegevusega selliste tegude korraldamiseks kui see hõlmab endas jõu kasutamist või sellega ähvardamist.[236] Seda põhimõtet kinnitas ÜRO Julgeolekunõukogu ka oma resolutsioonis nr 1373, pärast 11. septembril 2001. aastal toimunud terrorirünnakut Ameerika Ühendriikides asunud Maailma Kaubanduskeskuse kaksiktornide vastu.[237] Kuigi kaksiktornide ründamine ei olnud Afganistanile omistatav, sest Afganistani tollane valitsus ei rakendanud al-Qaeda üle ei efektiivset ega üldist kontrolli ning ei kiitnud al-Qaeda rünnakuid ka tagantjärgi heaks, siis Afganistan vastutas selle eest, et ta ei täitnud oma rahvusvahelist kohustust hoiduda terroristidele nn. turvapaiga pakkumisest.[238]

Riikidel on aktiivne kohustus ka takistada oma territooriumil mitte-riiklikel rühmitustel teiste riikide vastu rünnakute toimepanemist ning selliste rünnakute tolereerimise korral rikub riik oma rahvusvahelist kohustust. Seda põhimõtet kajastab ka *Tallinn Manual*'i reegel 5, mis sätestab, et riik ei tohi teadlikult lubada küberinfrastruktuuri, mis asub selle riigi territooriumil või tema eksklusiivse kontrolli all, kasutada viisil, mis negatiivselt ja ebaseaduslikult mõjutab teisi riike.[239] See reegel ei ole piiratud jõu kasutamisega vaid laieneb igasugusele

[234] Proulx, Vincent-Joël. Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?, lk 638; Grosswald, Levi. Cyberattack Attribution Matters under Article 51 of the U.N. Charter. Brooklyn Journal of International Law, Volume 36, Issue 3, 2011, lk 1164.

[235] Corfu Channel case, Judgment of April 9th, lk 22. Seda seisukohta kinnitas Rahvusvaheline Kohus hiljem ka Tehrāni Pantvangide kaasuses.

[236] United Nations General Assembly. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. A/RES/25/2625. Arvutivõrgus: http://www.un-documents.net/a25r2625.htm (04.05.2015).

[237] United Nations Security Council. Resolution 1373 (2001). Adopted by the Security Council at its 4385th meeting, on 28 September 2001. S/RES/1373. Arvutivõrgus: http://www.un.org/Docs/journal/asp/ws.asp?m=S/RES/1373%282001%29 (04.05.2015).

[238] Proulx, Vincent-Joël. Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?, lk 638.

[239] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 26.

kübertegevusele, mis rikub teiste riikide õigusi ja millel on negatiivne mõju teiste riikide territooriumile. Lisaks ei nõua reegel 5, et küberinfrastruktuuri kasutamise tagajärjeks on asjade kahjustumine või inimestele vigastuste tekitamine.[240]

Ei ole siiski realistlik eeldada, et riigid suudaksid täielikult takistada mitte-riiklikke üksuste poolt küberrünnakute toimepanemist riigi territooriumilt. Igal konkreetsel juhul tuleb seega hinnata, kas riik täitis oma kohustust piisaval määral, ehk siis kas ta tegi kõik mõistliku selle ärahoidmiseks.[241] Selle hindamiseks tuleb esmalt aga välja selgitada, millised on need konkreetsed kohustused, mida riik täitma peab. Küberrünnakute puhul on välja pakutud, et riikidel on rahvusvahelise õiguse alusel kohustus küberrünnakute toimepanemist ennetada ja neid takistada.

Rünnakute ennetamine hõlmab endas kohustust: (1) kehtestada seadused, mille alusel oleks võimalik kriminaalvastutusele võtta isikud, kes küberrünnakuid toime panevad või organiseerivad; (2) viia läbi toimunud küberrünnakute sisuline ja detailne uurimine ja võtta vastutusele isikud, kes on rünnakutega seotud; (3) teha tihedat koostööd küberrünnaku ohvriks langenud riigi uurimisasutustega, et rünnaku organiseerijaid vastutusele võtta.[242] Kui riik on ükskõikne selle osas, et tema küberinfrastruktuuri kasutatakse pidevalt küberrünnakute toimepanemiseks teiste riikide vastu, ta ei võta vastu seaduseid küberrünnakute kriminaliseerimiseks, ei näita üles huvi alustada kriminaalmenetlust küberrünnakute uurimiseks ning ta keeldub koostööst küberrünnaku ohvriteks langenud riikidega, et hoida ära edasisi rünnakuid, siis vastutab kõnealune riik oma tegevusetuse eest.[243] Oma tegevusetusega on ta rikkunud rahvusvahelist kohustus küberrünnakuid ennetada.

Rünnakute takistamine hõlmab mõistlike sammude võtmist, et takistada või lõpetada küberrünnakud, mida pannakse toime kasutades küberinfrastruktuuri, mis asub selle riigi territooriumil.[244] Juhul kui rünnaku lõpetamiseks vajalikku tegevust saab läbi viia üksnes eraõiguslik juriidiline isik, näiteks internetiteenuse pakkuja, siis on riigil kohustus kasutada

[240] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 27.

[241] Sklerov, Matthew J. Solving The Dilemma Of State Responses To Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, lk 43.

[242] Graham, David E. Cyber Threats and the Law of War. Journal of National Security Law & Policy, Volume 4, 2010, lk 93-94. Vt ka: Sklerov, Matthew J. Solving The Dilemma Of State Responses To Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, lk 62 jj.

[243] Graham, David E. Cyber Threats and the Law of War, lk 94-95.

[244] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 27.

kõiki tema käsutuses olevaid võimalusi, et survestada seda eraõiguslikku juriidilist isikut vajalikke samme astuma küberrünnaku lõpetamiseks või tõkestamiseks.[245]

Juhul küberrünnakud on korduvad ning riik ei ole varasemalt midagi ette võtnud, et takistada küberrünnakute toimepanemist, siis võib tegemist olla nn. "varjupaigariigiga", mille vastu on küberrünnakute ohvriks sattunud riikidel õigus kasutada olenevalt küberrünnaku olemusest, kas aktiivseid kaitsemeetmeid, jõudu või muid vastumeetmeid.[246] Aktiivsed kaitsemeetmed on teatud tüüpi vastumeetmed, mille eesmärk on küberrünnak lõpetada. Nendeks võib olla küberrünnakule vastamine sarnase rünnakuga – see võib seisneda ründavate arvutisüsteemide vasturündamist, arvutisüsteemide väljalülitamist ning seeläbi rünnaku lõpetamist poole pealt. Olemas on ka programme, mis tuvastavad automaatselt pahatahtliku süsteemi sissetungija ja algatavad ründaja vastu hävitavaid viirusesarnaseid rünnakuid. Passiivsed kaitsemeetmed on traditsioonilised arvutiturvalisuse tagamise vahendid nagu näiteks arvutisüsteemidele ligipääsu piiramine, andmetele ligipääsu piiramine, turvalisuse tagamine ja süsteemi ülesehituse turvalisus.[247] Enne vastumeetmete kasutamist on riigil siiski kohustus sellest rünnaku lähteriiki siiski eelnevalt teavitada tulenevalt riigivastutuse artiklite eelnõu artikkel 52 lõige 1 punktist b.

Küberrünnakute toimepanijatel on väga mitmeid erinevaid võimalusi, kuidas varjata oma asukohta või võltsida andmeid nii, et jätta mulje, et küberrünnak tuleneb mingist kolmandast riigist. Nagu eelnevalt mainitud, üksnes asjaolu, et rünnak paistab pärinevat teatud riigist, ei anna alust väita, et riik või mõni riigiväline üksus oli selle rünnaku korraldaja. Seega võtab riik aktiivsete vastumeetmete kasutamisel riski, et juhul kui hiljem selgub, et küberrünnakus esialgu kahtlustatav riik selle taga siiski ei olnud ja riik, kes vastumeetmeid kasutas neid õigusvastaselt, siis kaasneb sellega rahvusvaheline vastutus.[248]

Otsese vastutuse kohaldamine on võimalik üksnes juhul kui riik teadis või pidi teadma, et tema territooriumi kasutatakse teiste riikide huvide vastasel viisil ajal, mil need teod toime pandi. Teiseks tuleb hinnata, kas riigil oli reaalne võimalus ohu ärahoidmiseks.[249] Riik on

[245] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 28.

[246] Sklerov, Matthew J. Solving The Dilemma Of State Responses To Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, lk 13.

[247] Jensen, Eric Talbot. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Stanford Journal Of International Law, Volume 38, 2002, lk 231.

[248] Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, lk 130.

[249] Crawford, James. State Responsibility, lk 159.

küberrünnakute toimepanemisest teadlik kui näiteks tema luureorganid on tuvastanud, et riigi rünnak tuleneb riigi territooriumilt või kui riik on muul moel saanud usutavat informatsiooni, et rünnak toimub.[250] Kuna riigil on kohustus ka rünnakuid ennetada juba toimunud rünnakute uurimise ning menetlemise kaudu, siis juhul kui riik seda kohustust korduvalt on rikkunud, hoolimata näiteks küberrünnaku ohvriks sattunud riigi palvetest, siis ei tohiks olla sellel riigil õigus tugineda mitteteadmisele ja seeläbi vastutusest vabaneda.

Riigi kaudne vastutus võib tuleneda ka küberterroristide või mitte-riiklike üksuste toetamisest. ÜRO Julgeolekunõukogu resolutsioonist nr 1373 tulenevalt on igal riigil keelatud pakkuda terroristlike aktidega seotud isikutele või üksustele toetust ükskõik millises vormis, nii aktiivselt kui ka passiivselt.[251] Kuna terrorismil puudub hetkel rahvusvahelises õiguses üldtunnustatud definitsioon, siis on keeruline öelda, millisel juhul on küberrünnakute näol tegemist terrorismiga ja millal mitte.

René Värk on defineerinud terrorismi alljägnevalt: terrorism on ebaseaduslik vägivalla kasutamine või sellega ähvardamine või relvastatud jõu kasutamine inimeste või vara vastu poliitiliste sihtide saavutamiseks ning eesmärgiga tekitada üldsuses hirmu või sundida valitsust, rahvusvahelist organisatsiooni või üksikisikut midagi tegema või millestki hoiduma.[252] Küberterrorism on terrorismiaktide toimepanemine kasutades infotehnoloogilisi vahendeid.[253] Juhul kui arvutisüsteeme kasutades pannakse toime rünnak mingi riigi, organisatsiooni või isiku arvutisüsteemide vastu ning see rünnak vastab jõu kasutamise või relvastatud rünnaku standardile ning see rünnak pandi toime poliitiliste eesmärkide saavutamiseks ning üldsuses hirmu tekitamiseks, siis võib selle näol olla tegemist küberterrorismiaktiga.

Rühmitus Guardians of Peace varastas pahavara kasutades Sony Pictures Entertainment'lt rohkem kui 100 terabaiti salastatud informatsiooni ning lekitas seda infot osade kaupa Internetti alates 24. novembrist 2014. Lisaks informatsiooni vargusele hävitas rünnakus kasutatud pahavara ka teatud informatsiooni, mis oli arvutitesse salvestatud. Info kustutamise tõttu ei olnud võimalik osasid arvuteid enam sisse lülitada. Rühmitus ähvardas terrorismiaktide toimepanemisega Ameerika Ühendriikides asuvate kinoteatrite vastu, juhul kui Sony näitab

[250] Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare, lk 28.

[251] United Nations Security Council. Resolution 1373 (2001), lk 2.

[252] Värk, René. Terrorism, State Responsibility and the Use of Armed Force. ENDC Proceedings, Number 14, Volume 2, 2001, lk 81.

[253] Brenner, Susan. "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare, lk 386.

kinodes komöödiafilmi "The Interview", kus kahele ameeriklasele antakse ülesanne tappa Põhja-Korea juht Kim Jong-un. Sony võttis ähvardusi tõsiselt ning otsustas 17. detsembril 2014. aastal filmi esilinastused ära jätta. Teoreetiliselt võiks väita et Guardians of Peace panid toime küberterrorismiakti, sest ähvardasid jõu kasutamisega, kasutasid pahavara teel saadud informatsiooni, et sundida rahvusvahelist firmat teatud tegevusest hoiduma ning aimatav oli ka teatud poliitiline eesmärk. Siiski ei olnud tegemist küberterrorismiga, sest rünnaku tagajärjed ei olnud sellised, et saaks öelda, et tegemist on jõu kasutamisega ÜRO harta artikkel 2 lõige 4 mõttes või relvastatud rünnakuga.[254]

Kui riik toetab teatud mitteriiklikke üksuseid ning need üksused panevad toime rahvusvahelise õiguse vastaseid tegusid, siis võib riigivastutus tekkida sellistele üksustele toetuse pakkumise tõttu. See tähendab, et juhul kui riik toetab teatud küberrünnakuüksust rahaliselt, pakub neile väljaõpet, valib neile sobilikud sihtmärgid, kuid jättes üksusele siiski teatava autonoomia, mistõttu ei saa öelda, et riik rakendaks üksuse üle efektiivset või üldist kontrolli, siis tuleks kontrollida, kas riik on sellise käitumisega rikkunud mõnda muud rikkumisega seonduvat rahvusvahelise õiguse primaarnormi, milleks võib olla näiteks jõu kasutamise keeld või teise riigi siseasjadesse mittesekkumise kohustus.

3.4. Vahekokkuvõte

Riik vastutab küberoperatsioonide eest, mis on talle omistatavad ja mis kujutab endast rahvusvahelise kohustuse rikkumist. Sellest tulenevalt on igasugune küberettevõtmine, mis on toime pandud riigi luureorganite, sõjaväe, sisejulgeoleku üksuste, tolli või mõne muu riigiorgani poolt, sellele riigile omistatav. Teatud juhtudel on riikidele omistatavad ka riigiväliste isikute poolt toimepandud teod. Mitte-riiklike rühmituste poolt toimepandud küberrünnakute omistamiseks riigile riigivastutuse artiklite artikkel 8 alusel on vaja, et küberrünnakud oleksid toime pandud riigi juhendamisel või riigi suunamise või kontrolli all. Kui mitte-riiklikud rühmitused on täielikult sõltuvad neid toetavast riigist, ning riigil on rühmituse üle täielik kontroll, siis on selle rühmituse näol tegemist *de facto* riigiorganiga. Kui rühmitus loetakse *de facto* riigiorganiks, siis on võimalik selle poolt toimepandud küberrünnakud omistada riigile samade põhimõtete alusel nagu ametlike organite poolt korraldatud rünnakuid.

Kui täielikku sõltuvust riigi ja küberrünnaku toimepannud mitte-riikliku rühmituse vahel ei esine või ei suudeta tõendada, siis lähtuvalt Rahvusvahelise Kohtu poolt Nicaragua lahendis

[254] Schmitt, Michael. International Law and Cyber Attacks: Sony v. North Korea. Just Security, 17. detsember 2014. Arvutivõrgus: http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (04.05.2015).

sõnastatud ja Bosnia Genotsiidi lahendis kinnitatud, efektiivse kontrolli standardis alusel oleksid küberrünnakud riigile omistatavad, kui riik konkreetselt juhendab või nõuab küberrünnakute toimepanemist, riik täielikult kavandab operatsiooni strateegia või taktika, kontrollib igat küberoperatsiooni ja kõiki konflikti faase. Efektiivse kontrolli standard on saanud õiguskirjanduses teatava kriitika osaliseks ning mõningate autorite arvates on efektiivse kontrolli standardi kohaldamine praktikas ebarealistlik ning ebaõiglane. Võttes arvesse kübermaailma eripärasid, siis on tõenäoline, et efektiivse kontrolli tõendamine osutub võimatuks.

Mitmete autorite silmis on küberrünnakute omistamiseks riigile sobilikum kasutada Endise Jugoslaavia Kriminaaltribunali poolt sõnastatud üldise kontrolli standardit. Endise Jugoslaavia Kriminaaltribunali apellatsioonikoda leidis, et riigile teatud tegevuse omistamiseks ei pea sellel riigil olema kontroll iga konkreetse operatsiooni üle, vaid piisab sellest, et riik kontrollib mitte-riikliku rühmituse sõjalist tegevust üldiselt. Üldise kontrolli standardit kohaldades oleks võimalik omistada riigile küberrünnakud juhul kui riik on pakkunud rünnaku toimepannud organiseeritud rühmitusele tehnilist või muud tuge ja kelle tegevust riik organiseeris, isegi kui riigi osalust konkreetses küberrünnaku etapis ei ole võimalik rahuldavalt tõendada. Üldise kontrolli mõnevõrra madalama standardi kohaldamine suurendaks tõenäosust küberrünnakute riigile omistamist ning vastutuse vältimise välistamise võimaluse vähendamist.

Nii üldise kui ka efektiivse standardi kohaldamine kübermaailmas toimunud rünnakutele on tehniliste puudujääkide tõttu raskendatud. Tasub kaalumist, et kas küberrünnakute eripärasid arvesse võttes oleks mõistlikum sätestada küberrünnakutele eriomased omistamise reeglid. Teisalt on võimalik seda probleemi ka ületada normide tõlgendamise teel, mille puhul võetakse arvesse küberrünnakute tehnilise omistamise probleeme.

See aga ei tähenda, et riikidele ei järgneks küberrünnakute toetamisel mingeid tagajärgi. Riigi kaudne vastutus võib tekkida ka mõne muu rikkumisega seonduva primaarnormi rikkumisest. Riikidele tuleneb rahvusvahelisest õigusest kohustus küberrünnakuid ennetada ja takistada. Ennetamine sisaldab endas kohustust kriminaliseerida küberrünnakud, viia läbi tõhus üürimismenetlus ning vajadusel teha koostööd küberrünnaku ohver-riigiga. Takistamise kohustus tähendab kohustust teha kõik mõistlikult võimalik, et juba toimuvaid küberrünnakuid takistada. Näiteks kui riik toetab olulisel määral teatud mitte-riiklikke rühmitusi ning need rühmitused panevad toime rahvusvahelise õiguse vastaseid küberrünnakuid, kuid neid küberrünnakuid riigile omistada ei ole võimalik, siis tuleb välja selgitada, kas riik võis rikkuda näiteks teise riigi siseasjadesse sekkumise keeldu, või riivata selle riigi suveräänsust.

Kokkuvõte

Riigivastutuse doktriin on üks rahvusvahelise õiguse aluspõhimõtetest. Eraldi õigusinstituudina hakati riigivastutust käsitlema 19. sajandi lõpul. Riigivastutuse kodifitseerimisega alustati 1920-datel aastatel Rahvasteliidu eestvedamisel. Esimesed kodifitseerimiskatsed keskendusid riigi vastutusele välismaalastele põhjustatud kahju eest. Pärast II maailmasõda loodud Rahvusvahelise Õiguse Komisjon tõstis riigivastutuse teema kodifitseerimise taaskord päevakorda. Ligikaudu pool sajandit hiljem said riigivastutuse artiklid valmis ning need kiideti 2001. aastal ÜRO Peaassamblee poolt heaks.

Riigivastutuse artiklite kohaselt iga riigi poolt toime pandud rahvusvahelise õiguse vastane tegu sisaldab ka vastutust selle eest. Rahvusvahelise õiguse vastane tegu koosneb kahest elemendist, milleks on teo omistatavus riigile ning selle teoga mingi riigi rahvusvahelise kohustuse rikkumine. Kuna riigid ei ole võimelised iseseisvalt käituma, siis tuleb hinnata, kas mingi inimese või inimeste rühma teod on riigile omistatavad. Omistamine on õiguslik protseduur, mille käigus selgitatakse välja, kas teo tegeliku toimepanija ning riigi vahel eksisteerib selline seos, mis lubab öelda, et see isik on riigi esindaja või agent ning pani teo toime riigi eest ja nimel.

Riik vastutab üldjuhul üksnes enda ametlike organite tegude eest. Teatud puhkudel vastutab riik ka mitte-riiklike rühmituste poolt toime pandud tegude eest. Seda juhul kui riik on rühmitust volitanud riigivõimu teostama, ta andis rühmitusele juhiseid või rühmitus käitus riigi suunistel ning kontrolli all, või kiitis riik mitte-riikliku rühmituse või eraisikute käitumise heaks *ex post facto* ja tunnustas käitumist kui iseenda oma.

Riigiorganite tegude omistamisel on vaja tuvastada, kas teo toimepanija oli ametlikult riigiorgan või selle osa. Seejuures ei ole tähtsust kas tegu pandi toime riigiorgani pädevuse raames või ületades seda. Riik vastutab kõigi riigivõimu harude eest ning võimude lahususe printsiip rolli ei mängi.

Riik vastutab ka küberrünnakute eest, mille on läbi viinud tema organid või riigi poolt volitatud üksused. Termini "küberrünnak" all mõeldakse igasugust kübermaailmas toimepandud rünnakut, millega püütakse õõnestada vastase arvutivõrgu toimimist poliitilistel või rahvusliku julgeoleku eesmärkidel. See definitsioon hõlmab endas nii rünnakuid, mida võib pidada relvastatud rünnakuks kui ka madala intensiivsusega rünnakuid. Samas jääb definitsiooni alt välja rünnakud mida panevad toime mitteriiklikud kuritegelikud rühmitused oma erahuvides või riikide küberspionaaž.

Seega on igasugune küberettevõtmine, mis on toime pandud riigi luureorganite, sõjaväe, sisejulgeoleku üksuste, tolli või mõne muu riigiorgani poolt, sellele riigile omistatav. Mitmetel riikidel on olemas spetsialiseerunud sõjaväelised küberüksused, mille poolt toimepandud rahvusvahelise õiguse vastased tegusid on võimalik vastavatele riikidele riigivastutuse artiklite alusel omistada.

Kui küberrünnakut alustati või see pärineb mingi riigi riiklikust küberinfrastruktuurist ei tähenda see siiski automaatselt, et rünnakut oleks võimalik sellele riigile omistada, see asjaolu üksnes viitab sellele, et riik võib rünnakuga seotud olla. Kui traditsiooniliste rünnakute puhul, mille toimepanemiseks kasutatakse riiklikke vahendeid, eelkõige riigi sõjaväelist varustust, ei teki enamjaolt küsimustki, kas rünnakuid on võimalik omistada sellele riigile, kuid kübermaailm erineb selles osas märkimisväärselt reaalsest maailmast, ning tõenäosus, et riiklikku küberinfrastruktuuri kasutatakse hoopis mitte-riiklike rühmituste poolt kasvab oluliselt. Seetõttu ei ole võimalik omistada riigile automaatselt kõiki tegusid, mis pannakse toime riigi küberinfrastruktuuri kasutades. Kas riigi osalust rünnakus võib tuletada ka asjaolust, et riik ei võta mõistlikke meetmeid juba toimuva rünnaku takistamiseks, on veel lahtine. Siiski ei leiab autor, et riigi poolt üles näidatud igasugune apaatia küberrünnaku takistamiseks võib olla oluline indikaator, et riik on rünnaku osaline, kuid see ei ole siiski piisav alus näitamaks sidet toimuva küberrünnaku ning riigi vahel. Kui küberrünnak üksnes suunatakse läbi mingi riigi küberinfrastruktuuri, siis see asjaolu ei ole piisavaks aluseks omistamaks küberrünnakut sellele riigile.

Juhul kui riik volitab mingit riigivõimu elementi teostama mitte-riikliku rühmituse, siis vastutab riik ka selle mitte-riikliku rühmituse poolt toimepandud rahvusvahelise õiguse rikkumiste eest, kuid üksnes selles ulatuses, milles rikkumised on seotud neile antud volituse sisuga. Riigile on omistatavad ka selle riigi poolt kübereesmärkide saavutamiseks palgatud erafirmade tegevus. Riiklik funktsioon mida need täita võivad on näiteks riigi küberjulgeoleku tagamine, kübervõimekuse arendamine, küberruumis luureinfo kogumine, sorteerimine ja salvestamine.

Juhul kui riik on küberrünnakud toimepandud rühmitustele andud juhised või rühmitus on teod toime pannud riigi juhendamisel või riigi suunamise või kontrolli all, siis on küberrünnakut võimalik riigile omistada. Riigi poolt teostatava kontrolli hindamiseks on loodud kaks erinevat standardit – efektiivse ja üldise kontrolli standard. Efektiivse kontrolli standardi alusel on küberrünnakud riigile omistatavad, kui riik konkreetselt juhendab või nõuab küberrünnakute toimepanemist, riik täielikult kavandab operatsiooni strateegia või taktika, kontrollib igat küberoperatsiooni ja kõiki konflikti faase, s.t. efektiivse kontrolli standardi kohaldamisel peab

esinema efektiivne kontroll terve konflikti jooksul ning kõigi toimepandud küberoperatsioonide üle. Efektiivse kontrolli standard on sellest tulenevalt väga kõrge. Mitmete autorite silmis on efektiivse kontrolli standard praktikas ebarealistlik ning ebaõiglane. On välja pakutud, et küberrünnakute omistamiseks riigile on sobilikum kasutada Endise Jugoslaavia Kriminaaltribunali poolt sõnastatud üldise kontrolli standardit.

Üldise kontrolli standardi kohaldamiseks ei pea sellel riigil olema kontroll iga konkreetse operatsiooni üle, mille käigus rahvusvahelise õiguse vastased teod toime pandi, vaid piisab sellest, et riik kontrollib rühmituse sõjalist tegevust üldiselt. Riik peab lisaks rühmituse rahastamisele, treenimisele, varustamisele ja muule operatiivse toetuse pakkumisele ka üldiselt organiseerima, koordineerima või planeerima rühmituse sõjalist tegevust. Üldise kontrolli standard on mõnevõrra madalam, sest tõendada ei ole vaja riigi seotust iga konkreetse küberrünnakuga, piisab kui riigil on kontroll organiseerunud rühmituse poolt toimepandud küberoperatsiooni üle.

Madalama kontrollistandardi kohaldamine võib olla õigustatud kübermaailma "tehnilise omistamise probleemi" tõttu. Internet ei ole üles ehitatud nii, et küberrünnakute toimepanijate tuvastamine ja nende identifitseerimine oleks võimalikult lihtne. Üheks olulisemaks takistuseks küberrünnaku tehnilise omistamise jaoks on üsnagi suur anonüümsus, mis võimaldab ründajal oma tegelikku identiteeti varjata. Anonüümsust saab tagada nii IP aadresside võltsimise kui ka anonümiseerimisprogrammide kasutamise teel. Mõned autorid leiavad, et üksnes tehniliste indikaatorite ja informatsiooni põhjal isiku, keda saab pidada küberrünnaku eest vastutavaks, tuvastamine ei ole võimalik ning mitte keegi ei ole sellele lähedalegi jõudnud. Teised jällegi leiavad, et omistamise probleem on ülehinnatud. Üldiselt võib öelda, et kuigi tehnilisi võimalusi rünnakute algallikate tuvastamiseks uuritakse ning arendatakse pidevalt, siis tõsikindlate tõendite kogumine kübermaailmas on siiski keeruline, sest digitaalsed tõendid on oma olemuselt kaduvad ja kergesti manipuleeritavad. Digitaalsete tõendite muutmine on niivõrd lihtne, et see võib juhtuda ka kogemata. Digitaalsete tõendite muutmist keerulisem tuvastada kui füüsiliste tõendite puhul, mis võimaldab alati tõendi tõesuses kahelda. Kolmandaks on tekib digitaalset infot arvutites ning võrkudes meeletus koguses. Kogu selle informatsiooni läbitöötamine on võrreldav elektroonilisest heinakuhjast nõela otsimisega. Võrgupõhised tõendid on veelgi problemaatilisemad, sest need on püsimatud, lühikese elueaga ning tihtipeale asuvad teistes riikides.

Tehnilise omistamise probleemi ning riigivastutuse kohaldamise ülikõrge tõendamisstandardi tõttu on küberrünnakute otsene omistamine riikidele üsnagi problemaatiline. See ei tähenda,

aga küberrünnakute eest vastutuse kohaldamine oleks välistatud. Kaudne vastutus tähendab, et kuigi riigile ei ole võimalik omistada mingi konkreetset tegu või tegevusetust, siis riik võib vastutada mõne teise primaarnormi rikkumise eest. Näiteks on riikidel on aktiivne kohustus takistada oma territooriumil mitte-riiklikel rühmitustel teiste riikide vastu rünnakute toimepanemist ning selliste rünnakute tolereerimise korral rikub riik oma rahvusvahelist kohustust.

Ei ole siiski realistlik eeldada, et riigid suudaksid täielikult takistada mitte-riiklikke üksuste poolt küberrünnakute toimepanemist riigi territooriumilt. Igal konkreetsel juhul tuleb seega hinnata, kas riik täitis oma kohustust piisaval määral, ehk siis kas ta tegi kõik mõistliku selle ärahoidmiseks. Küberrünnakute puhul on välja pakutud, et riikidel on rahvusvahelise õiguse alusel kohustus küberrünnakute toimepanemist ennetada ja neid takistada. Juhul kui küberrünnaku lähteriik ei ole valmis astuma samme küberrünnakute ennetamiseks või tegema koostööd küberrünnakute takistamiseks, siis on küberrünnakute ohvriks sattunud riikidel õigus kasutada olenevalt küberrünnaku olemusest, kas aktiivseid kaitsemeetmeid, jõudu või muid vastumeetmeid. Enne vastumeetmete kasutamist on riigil siiski kohustus sellest rünnaku lähteriiki siiski eelnevalt teavitada tulenevalt riigivastutuse artiklite eelnõu artikkel 52 lõige 1 punktist b.

Küberrünnakud ei leia aset reaalses füüsilises maailmas, mistõttu oma olemuselt on need suuresti erinevad traditsioonilistest rünnakutest. Tehnilised väljakutsed küberrünnakute toimepanijate tuvastamiseks ning digitaalsete tõendite iseloomulikud probleemid tähendavad, et üksnes traditsioonilistele omistamisreeglitele tuginemine on keeruline. Ka mitte-riiklike rühmituste üle teostatava kontrollistandardite kasutamine on suure tõenäosusega praktikas äärmiselt raskendatud. Kuigi esmapilgul tundub, et riigivastutuse artiklites sisalduvaid omistamise norme on võimalik lihtsasti kohandada vastavalt küberrünnakute kontekstile, siis nii see kahjuks ei ole. Kindlasti tuleks tulevikus analüüsida, kas ja millised oleksid võimalused riigivastutuse artiklite täiendamiseks küberrünnakute kontekstis. Teisalt ei pruugi omistamise probleem osutuda praktikas väga oluliseks, sest riigid võivad vastutada rünnakute eest ka kaudselt. Seega ei pruugi olla oluline siduda rünnak konkreetse riigiga, kui riigivastutust on võimalik kohaldada seeläbi, et tuvastatakse riigi suutmatus takistada oma küberinfrastruktuuri kasutamist teiste riikide huvide vastaselt.

Summary

The doctrine of state responsibility is one of the main principles of International law even though it is relatively young branch of International law. Only in the late 19th century and early 20th century did state responsibility rise to the forefront in the minds of legal scholars. League of Nations started the codification of the state responsibility doctrine in the mid 1920's. First attempts at codification were mainly concerned with the international responsibility of States for injuries on their territory to the person or property of foreigners. Even though countries mainly agreed on the topic of state responsibility, major disagreements arouse over the topic of treatment of the foreigners. Thus the attempt at codifying of international state responsibility did not bear fruit.

After the Second World War and after legal and political situation within the international community had found its equilibrium, the International Law Commission decided in 1950's that it shall start with the codification of the state responsibility. After almost half a century worth of effort to codify the law of international responsibility of the states, the UN General Assembly approved the draft articles on state responsibility on 2001.

Articles on state responsibility Article 1 stipulates that every internationally wrongful act of a State entails the international responsibility of that State. According to article 2, there is an internationally wrongful act of a State when conduct consisting of an action or omission is attributable to the State under international law and constitutes a breach of an international obligation of the State. Because the states are not able to act on their own but only through representatives or agents, it must be evaluated whether act of these persons is attributable to the state. Attribution is legal procedure whereby it is decided whether there exists real and significant bond between the actor and the state.

The guiding principle of the attribution is that the conduct of any State organ shall be considered an act of that State under international law. On certain occasions the state is also responsible for the actions of non-governmental actors. Attribution of non-state actors is attributable to the state if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct or if and to the extent that the State acknowledges and adopts the conduct of the non-state actors in question as its own.

The state may also bear responsibility for the cyberattacks that are carried out by its organs or by the non-state actors the state has empowered by the law to exercise elements of the governmental authority.

As a clarification the author points out that within the framework of this thesis, the author uses the term cyber-attack in a meaning that „a cyber-attack consists of any action taken to undermine the function of a computer network for a political or national security purpose." This definition is used in order to include attacks that may not be considered armed attacks o ruse of force Under UN Charter. But on the other hand, this definition excludes attacks that are carried out by non-state actors for purposes of personal gain.

As it was said, states bear responsibility for cyber-attacks committed by its own agents. This means that any cyber operation which is carried out by the intelligence organs, military, enforcement agents or custom is attributable to the state. Many countries have developed special military cyber units, e.g. Joint Forces Cyber Group of Great Britain. The actions of these cyber units are attributable to the state.

The differences between cyber-attacks and traditional attacks is the fact that it is very difficult to ascertain from where the attack originates and who is behind it. In case of traditional attacks it is fairly certain to assume that if an attack launches from the territory of that state and the launchers are members of the military or customs of that state, then it is fairly easy to presume that that state is also behind the attacks in some way. This is not the case for cyber-attacks. Because gaining control over foreign state cyberinfrastructure can be easier than gaining that same control over some other military infrastructure in traditional sense, it is not possible to make any real presumptions. But this fact may serve as an indication of state participation. It is arguable if the presumption may arise in the case where the attacks from the governmental infrastructure are launched periodically and the origin state does not show any willingness to combat that problem. The author contends that periodically launched attacks from governmental infrastructure certainly should give more strength to the argument that the government is connected to the attacks but is not enough to attribute cyber-attacks to that government.

If the state empowers a person or an entity to exercise any elements of the governmental authority, then state shall bear the responsibility of the actions of that person or entity, but only to the extent that the person or entity acted in that particular capacity. Thus, if the government empowers an entity to fulfil certain official cyber objectives of the state, then the actions of these entities is attributable to a state. The elements of governmental authority may be cyber security, improving the cyber capacity of that state, collecting intelligence in cyber world, etc.

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or

under the direction or control of that State in carrying out the conduct. To decide if the non-state actors acted under control of the state two diverging approaches have emerged.

First is the effective control standard put forth by International Court of Justice in the Military and Paramilitary Activities in and against Nicaragua case. The status of effective control as principle of customary law was also mentioned in the Application of the Convention on the Prevention and Punishment of the Crime of Genocide case.

Under effective control standard the actions of non- state actors are attributable to the state if the state directed or enforced the perpetration of the acts that breached the international obligations of that state. Effective control means that the state must issue specific directions to carry out specific operations or enforcing the non-state actors to carry out specific task. This means that the state must be involved in every act during the entirety of the operation in order for that cyber-attack to be attributable to a state. This is very exacting standard and has been considered by some as unrealistic and unfair.

It is stated that the overall control standard may be more appropriate in the context of cyber attacks. Overall control standard was stated by the International Criminal Tribunal for the former Yugoslavia. Under overall control standard it is enough if the state has control over hierarchically organised group of non-state actors and it is not necessary to prove that the state used its control over every single action the group carried out. Thus the standard of overall control is slightly lower than effective control. For this reason it can be used in the context of cyber-attacks – if the state has overall control over non-state group of hackers then it is fair to assume that it also had control over every specific stage in preparation of the attacks and during it.

Lower standard of control might be especially useful to attribute cyber-attacks because of the problems relating to technical attribution. Technical attribution means attributing an attack to a specific person who carried out the attacks. Technical attribution problem exists for several reasons. Firstly, the Internet was not built attribution in mind. It is fairly easy for experienced user to hide its identity in cyber space.

Some authors believe that technical attribution is impossible, because the technology has not developed far enough and it will not possible in the foreseeable future. Others on the other hand have stated that technical attribution problem is overrated and there are only few dozens of actors who are able to carry out cyber-attacks. The truth is probably in the middle. While technologies to trace the cyber-attacks back to the point of origin being constantly improved

and new technologies constantly researched and developed, the attackers also improve and develop their capacity to cause damage and hide their identities. Secondly there is obstacles in acquiring evidence in cyberspace. Digital evidence is more easily manipulated than physical evidence and the manipulation does not bear often any hints of it. Moreover, the information in cyberspace amasses in faster pace than it does in physical world, which means that the amount of data to be processed by the forensics investigators is often very time consuming. Finally digital evidence is ephemeral, which means that any delay in collecting digital evidence may mean that it is going to be "overwritten" or lost. Thus it might be said that relying only on technical attribution would not be possible, but using intelligence sources and other secondary means can build a convincing case to attribute cyber attack to a state.

But building a convincing case may not be enough for cyber-attack attribution because the standard of proof in international tribunals and courts is higher than that – mostly facts must be proven beyond reasonable doubt. To achieve that high threshold of proof may prove to be impossible for states. Therefore the author of this thesis is on the opinion that current attribution standards stipulated in articles on state responsibility do not serve particularly well the needs of cyber world. Direct responsibility is under these rules are fairly easy to avoid, especially if the cyber-attacks have been carried out by non-state actors under the control of the state. Some authors have pointed out that after the 9/11 attacks against the Twin Towers, the international law of responsibility has shifted to favour indirect responsibility.

Indirect responsibility means that state is not held accountable for the fact that it carried out a cyber-attack, but that it breached its international obligation of due diligence because it failed to fulfil certain obligation – e.g. not let knowingly use its territory for acts contrary to the interest of other states. The states have international obligation to prevent and stop the cyberattacks emanating from their territory.

The duty of prevention mainly concerns with adopting internal legislation to criminalise the launching of cyber attacks, carrying out substantial and detailed investigations when cyber-attacks have happened and co-operating with the victim state's investigations. The duty to stop cyber-attacks consists taking every reasonable measure to stop the attack whilst underway from their territory. This obligation can take various forms depending on the cyber capacity of that state. If the state wherefrom the attacks originate fail to take necessary measures or show complete apathy in doing so, then victim state has the right to use countermeasures. In cyber world countermeasures can include shutting down all the connections coming from one state, using technologies to hack back etc. Before resorting to countermeasures the victim state must

first officially notify the attacking-state of its plan and give that state reasonable time to take some action.

Because cyber-attacks do not take place in tangible world, they differ significantly from traditional operations. Problems with technical attribution and digital evidence mean that relying on traditional bases of attribution may prove to be difficult. It is difficult also to prove the level of control the state may exercise over the non-state actors it uses to further its goals. It is easy to hide your identity in cyberspace and it has been said that "electrons do not wear uniforms" meaning that it is especially hard to distinguish in cyberspace between official organs of the state and regular members of the public who are hacking for their private gain. More research is necessary into whether the world needs new cyber-treaty with its own specific attribution rules or if it is enough to allow some leeway when it secondary rules of attribution are used in context of cyberattacks.

It is fair to assume that because of the difficulties related to using the attribution standards drom articles on state responsibility will increase the importance of the indirect responsibility doctrine. According to indirect responsibility doctrine the responsibility may be imputed because the state has failed to fulfil its international obligation indirectly – e.g. letting malicious non-state actors to use its cyber infrastructure for cyber attacks or supporting the terrorists via various means. This means that even if victim state can not prove the link between the actor and the state, it can prove that the state was negligent in protecting the interests of other states within its territory.

Kasutatud allikad

Kasutatud õigusaktid

1. 2. augusti 1949 Genfi konventsioonide 8. juuni 1977 (II) lisaprotokoll siseriiklike relvakonfliktide ohvrite kaitse kohta. Arvutivõrgus: https://www.riigiteataja.ee/akt/79271.

2. Rahvusvahelise Kriminaalkohtu Rooma statuut, vastu võetud 17.07.1998. Arvutivõrgus: https://www.riigiteataja.ee/akt/78574 (04.05.2015).

3. Rules of Procedure and Evidence of the International Criminal Tribunal for the former Yugoslavia (as amended 22 May 2013), 11 February 1994. Arvutivõrgus: http://www.icty.org/x/file/Legal%20Library/Rules_procedure_evidence/IT032Rev49_en.pdf (04.05.2014)

4. Rules of Procedure and Evidence of the International Tribunal for Rwanda (as amended 10 April 2013), 29 June 1995. Arvutivõrgus: http://www.unictr.org/sites/unictr.org/files/legal-library/130410_rpe_en_fr.pdf (04.05.2015).

5. Statute of the International Criminal Tribunal for the Former Yugoslavia (as amended on 7 July 2009), 25 May 1993. Arvutivõrgus: http://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf (04.05.2015).

6. ÜRO Julgeolekunõukogu. Resolution 1373 (2001). Adopted by the Security Council at its 4385th meeting, on 28 September 2001. S/RES/1373. Arvutivõrgus: http://www.un.org/Docs/journal/asp/ws.asp?m=S/RES/1373%282001%29 (04.05.2015).

7. ÜRO Peaassamblee. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. A/RES/25/2625. Arvutivõrgus: http://www.un-documents.net/a25r2625.htm (04.05.2015).

Kasutatud lahendid

Rahvusvaheline Kohus

8. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43. Arvutivõrgus: http://www.icj-cij.org/docket/files/91/13685.pdf (04.05.2015).

9. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 168. Arvutivõrgus: http://www.icj-cij.org/docket/files/116/10455.pdf (04.05.2015).

10. Avena and Other Mexican Nationals (Mexico v. United States of America), Judgment, I.C.J. Reports 2004, p. 12. Arvutivõrgus: http://www.icj-cij.org/docket/files/128/8188.pdf (04.05.2015).

11. Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, p. 4. Arvutivõrgus: http://www.icj-cij.org/docket/files/1/1645.pdf (04.05.2015).

12. Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion, I.C.J. Reports 1999. Arvutivõrgus: http://www.icj-cij.org/docket/files/100/7619.pdf (04.05.2015).

13. Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, I.C.J. Reports 1997, p. 7. Arvutivõrgus: http://www.icj-cij.org/docket/files/92/7375.pdf.

14. Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea intervening), Judgment, I.C.J. Reports 2002, p. 30. Arvutivõrgus: http://www.icj-cij.org/docket/files/94/7453.pdf (04.05.2015).

15. Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua intervening), Judgement, I.C.J. Reports 1992, p. 506. Arvutivõrgus: http://www.icj-cij.org/docket/files/75/6671.pdf (04.05.2015).

16. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment. I.C.J. Reports 1986, p. 14. Arvutivõrgus: http://www.icj-cij.org/docket/files/70/6503.pdf (04.05.2015).

17. North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3. Arvutivõrgus: http://www.icj-cij.org/docket/files/52/5561.pdf (04.05.2015).

18. Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, p. 161, lk 189, para. 57. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9715.pdf (04.05.2015).

19. United States Diplomatic and Consular Staff in Tehran, Judgment, I.C.J. Reports 1980, p. 3. Arvutivõrgus: http://www.icj-cij.org/docket/files/64/6291.pdf (04.05.2015).

20. Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia), Judgment, I.C.J. Reports 2002. Arvutivõrgus: http://www.icj-cij.org/docket/files/102/7714.pdf (04.05.2015).

Rahvusvahelise Kohtu kohtunike eriarvamused

21. Case concerning Right of Passage over Indian Territory (Merits), Judgrnent of 12 April 1960: I.C.J. Reports 1960, p. 6, Dissenting Opinion of Judge Moreno Quintana. Arvutivõrgus: http://www.icj-cij.org/docket/files/32/4541.pdf (04.05.2015).

22. Case of Certain Norwegian Loans, Judgment of July 6th, 1957: I.C. J. Reports 1957, p. 9, Separate Opinion of Judge Sir Hersch Lauterpacht. Arvutivõrgus: http://www.icj-cij.org/docket/files/29/4781.pdf (04.05.2015).

23. Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea intervening), Judgment, I.C.J. Reports 2002, p. 30, Dissenting Opinion of Judge Ajibola. Arvutivõrgus: http://www.icj-cij.org/docket/files/94/7471.pdf (04.05.2015);

24. Land, Island and Maritime Frontier Dispute (El Salvador/Honduras: Nicaragua intervening), Separate opinion of Judge Torres-Bernárdez. Arvutivõrgus: http://www.icj-cij.org/docket/files/75/6679.pdf (04.05.2015).

25. Maritime Delimitation and Territorial Questions between Qatar and Bahrain, Merits, Judgment, I.C.J. Reports 2001, p. 40, Separate Opinion of Judge Torres Bernárdez. Arvutivõrgus: http://www.icj-cij.org/docket/files/87/7047.pdf (04.05.2015).

26. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Dissenting opinion of Judge Sir Robert Jennings, lk 533. Arvutivõrgus: http://www.icj-cij.org/docket/files/70/6525.pdf (04.05.2015).

27. Nottebohm Case (second phase), Judgement of April 6th, 1955: I.C.J. Reports 1955, p. 4, Dissenting Opinion by Judge Read. Arvutivõrgus: http://www.icj-cij.org/docket/files/18/2680.pdf (04.05.2015).

28. Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, p. 161, Separate Opinion of Judge Owada. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9733.pdf (04.05.2015).

29. Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Kooijmans. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9725.pdf. (04.05.2015)

30. Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Buergenthal. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9729.pdf (04.05.2015).

31. Oil Platforms (Islamic Republic of Iran v. United States of America), Separate Opinion of Judge Higgins. Arvutivõrgus: http://www.icj-cij.org/docket/files/90/9721.pdf (04.05.2015).

32. Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14, Separate Opinion of Judge Keith. Arvutivõrgus: http://www.icj-cij.org/docket/files/135/15881.pdf (04.05.2015).

33. South West Africa Cases (Ethiopia v. South Africa; Liberia v. South Africa), Preliminary Objections, Judgment of 21 December 1962: I.C.J. Report; 1962, p. 319, Joint Dissenting Opinion of Sir Percy Spender and Sir Gerald Fitzmaurice. Arvutivõrgus: http://www.icj-cij.org/docket/files/47/4925.pdf (04.05.2015).

34. Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia), Judgment, I.C.J. Reports 2002, p. 625, Declaration of Judge Oda. Arvutivõrgus: http://www.icj-cij.org/docket/files/102/7716.pdf (04.05.2015).

Muude rahvusvaheliste kohtute ja tribunalide otsused

35. Aguilar-Amory and Royal Bank of Canada claims (Great Britain v. Costa Rica). Reports of International Arbitral Awards, Volume I, 18 October 1923. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_I/369-399.pdf (04.05.2015).

36. German Settlers in Poland, (1923) P.C.I.J., Series B, Advisory Opinion No. 6. On 3 February 1923.

37. Home Frontier and Foreign Missionary Society of the United Brethren in Christ (United States v. Great Britain). Reports of International Arbitral Awards, Volume VI, 18 December 1920. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_VI/42-44_Brethren.pdf (04.05.2015).

38. Phosphates in Morocco Case, (1938) P.C.I.J., Ser. A/B, No. 74.

39. Prisoners of War, Eritrea's Claim 17. Eritrea Ethiopia Claims Commission, Partial Award of 1 July 2003. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_XXVI/23-72.pdf (04.05.2015).

40. Prosecutor v. Duško Tadic, Judgement, Case No. IT-94-1-A, ICTY Appeals Chamber, 15 July 1999. Arvutivõrgus: http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf (04.05.2015).

41. Prosecutor v. Duško Tadic, Judgment, Case No. IT-94-1-T, ICTY Trial Chamber, 7 May 1997. Arvutivõrgus: http://www.icty.org/x/cases/tadic/tjug/en/tad-tsj70507JT2-e.pdf (04.05.2014).

42. Sambiaggio Case (of a general nature). Reports of International Arbitral Awards, Volume X, 1903. Arvutivõrgus: http://legal.un.org/riaa/cases/vol_X/499-525.pdf (04.05.2015).

43. The Mavrommatis Jerusalem Concessions, (1925) P.C.I.J., Ser A. No. 5. On 26 March 1925. Arvutivõrgus: http://www.icj-cij.org/pcij/serie_A/A_05/15_Mavrommatis_a_Jerusalem_ Arret_19250326.pdf (04.05.2015).

44. Velasquez Rodriguez Case, Judgment of July 29, 1988, Inter-American Court of Human Rights (Ser. C) No. 4 (1988). Arvutivõrgus: http://www1.umn.edu/humanrts/iachr/b_11_12d.htm (04.05.2015).

Kasutatud kirjandus

45. Abass, Ademola. Proving State Responsibility for Genocide: The ICJ in Bosnia v. Serbia and the International Commission of Inquiry for Darfur. - Fordham International Law Journal, Volume 31, Issue 4, 2007.

46. Ago, Roberto. First report on State responsibility by Mr. Roberto Ago, Special Rapporteur - Review of previous work on codification of the topic of the international responsibility of States. - Yearbook of the International Law Commission, 1969, Volume 2, United Nations: New York, 1970. Arvutivõrgus: http://legal.un.org/ilc/documentation/english/a_cn4_217.pdf. (04.05.2015)

47. Ago, Roberto. Fourth report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The internationally wrongful act of the State, source of international responsibility. - Yearbook of the International Law Commission, 1972, Volume 2, United Nations: New York, 1974. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1972_v2_e.pdf (04.05.2015).

48. Ago, Roberto. Second report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The origin of international responsibility. - Yearbook of International Law Commission, 1970, Volume 2, United Nations: New York, 1972. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1970_v2_e.pdf (04.05.2015).

49. Ago, Roberto. Third report on State responsibility, by Mr. Roberto Ago, Special Rapporteur—The internationally wrongful act of the State, source of international responsibility. - Yearbook of the International Law Commission, 1971, Volume 2, Part one. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes %28e%29/ILC_1971_v2_p1_e.pdf (04.05.2015).

50. Ahmed, Dawood I. Defending Weak States against the Unwilling or Unable Doctrine of Self-Defense. - Journal of International Law and International Relations, Volume 9, 2013.

51. Antolin-Jenkins, Vida M. Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places? - Naval Law Review, Vol 51, 2005. Arvutivõrgus: http://www.jag.navy.mil/documents/navylawreview/nlrvolume51.pdf (04.05.2015).

52. Del Mar, Katherine. The International Court of Justice and Standards of Proof. Artikkel raamatus: Bannelier, Karine (toim.). The ICJ and the Evolution of International Law: the

Enduring Impact of the Corfu Channel Case. London; New York: Routledge, 2012, 2013.

53. Barkham, Jason. Information Warfare and International Law on the Use of Force. - New York University Journal of International Law and Politics, Volume 34, Issue 1, 2001.

54. Berman Russell. The U.S. Government Is Under (Cyber) Attack. - The Atlantic. 17. november 2014. Arvutivõrgus: http://www.theatlantic.com/politics/archive/2014/11/the-government-is-under-cyber-attack/382859/ (04.05.2015).

55. Bodansky, Daniel; Crook, John R. Symposium: The ILC's State Responsibility Articles. Introduction and Overview. - American Journal of International Law, 96 (2002).

56. Boebert, W. Earl. A Survey of Challenges in Attribution. - Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press, 2010.

57. Brenner, Susan. "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare. - The Journal of Criminal Law & Criminology, Volume 97, Issue 2, 2007.

58. Broad, William J.; Markoff, John; Sanger, David E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. - The New York Times, 15. jaanuar 2011. Arvutivõrgus: http://www.nytimes.com/2011/ 01/16/world/middleeast/16stuxnet.html?_r=0. (04.05.2015)

59. Bronk, Christopher; Tikk-Ringas, Eneken. The Cyber Attack on Saudi Aramco. - Survival: Global Politics and Strategy, Vol 55, Issue 2, 2013.

60. Brown, Davis. Use of Force against Terrorism after September 11th: State Responsibility, Self-Defense and Other Responses. - Cardozo Journal of International and Comparative Law, Vol. 11, Issue 1, 2003.

61. Burma Hit by Massive Net Attack Ahead of Election. - BBC News, 4.11.2010. Arvutivõrgus: http://www.bbc.co.uk/news/technology-11693214 (04.05.2015).

62. Cartwright, James E. Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories on Joint Terminology for Cyberspace Operations. 2011. Arvutivõrgus: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Opera tions.pdf (04.05.2014).

63. Cassese, Antonio. The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. - The European Journal of International Law, Volume 18, Issue 4.

64. Chaikin, David. Network Investigations of Cyber Attacks: the Limits of Digital Evidence. - Crime, Law and Social Change, Volume 46, Issue 4-5, December 2006.

65. Clark, David D.; Landau, Susan. Untangling Attribution. - Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press, 2010.

66. Clarke, Richard A.; Knake, Robert K. Cyber War: The Next Threat to National Security and What To Do About It. New York: Ecco, 2010.

67. Commentary to the Articles on the Responsibility of States for Internationally Wrongful

Acts. - Yearbook of International Law Commission, 2001, Volume 2, Part 2, United Nations: New York and Geneva, 2007. Arvutivõrgus: http://legal.un.org/ilc/texts/instruments /english/commentaries/9_6_2001.pdf (04.05.2015).

68. Crawford, James; Pellet, Alain; Olleson, Simon; Parlett, Kate (toim). The Law of International Responsibility. Oxford [etc.]: Oxford University Press, 2010.

69. Crawford, James. First report on State responsibility, by Mr. James Crawford, Special Rapporteur. *sine loco.* Arvutivõrgus: http://legal.un.org/ilc/documentation/ english/a_cn4_490.pdf (04.05.2015).

70. Crawford, James. State Responsibility. The General Part. New York; Cambridge: Cambridge University Press, 2013, 2014.

71. David E. Sanger, Obama Order Sped Up Wave of Cyberatacks Against Iran. - The New York Times, 1. juuni 2012. Arvutivõrgus: http://www.nytimes.com/2012/06/01/world/middleeast/ obama-ordered-wave-of-cyberattacks-against-iran.html (04.05.2015).

72. Dumberry, Patrick. New State Responsibility for Internationally Wrongful Acts by an Insurrectional Movement. - The European Journal of International Law, Volume 17, Issue 3, 2006.

73. Dupuy, Pierre-Marie. Dionisio Anzilotti and the Law of International Responsibility of States. - The European Journal of International Law, Vol. 3, Issue 1, 1992.

74. Economist. War in the Fifth Domain. - The Economist, 1. juuli 2010. Arvutivõrgus: http://www.economist.com/node/16478792 (04.05.2015).

75. Fleck, Dieter. Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual. - Journal of Conflict & Security Law, Volume 18, Issue 2, 2013.

76. Frates, Chris; Devine, Curt. Government Hacks and Security Breaches Skyrocket. - Cable News Network, 19. detsember. 2014. Arvutivõrgus: http://edition.cnn.com/2014/12/19/politics/government-hacks-and-security-breaches-skyrocket/ (04.05.2015).

77. Gaetano Arangio-Ruiz. Second report on State responsibility, by Mr.Gaetano Arangio-Ruiz, Special Rapporteur. - Yearbook of the International Law Commission, 1989, Volume II (Part I), United Nations: New York, 1992. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1989_v2_p1_e.pdf (04.05.2015).

78. García-Amador, Francisco V. International responsibility: Sixth report by F. V. Garcia Amador, Special Rapporteur. - Yearbook of International Law Commission 1961, Volume 2, United Nations: New York, 1962. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_1961_v2_e.pdf.

79. Georgiades, Eugenia; Caelli, William J.; Christensen, Sharon; Duncan, W.D. Crisis On Impact: Responding to Cyber Attacks on Critical Information Infrastructures. - Journal of Information, Technology & Privacy Law, Volume 30, 2013;

80. Gervais, Michael. Cyber Attacks and the Laws of War. Berkeley Journal of International Law, Vol 30, Issue 2, 2012.

81. Glennon, Michael J. The Road Ahead: Gaps, Leaks and Drips. - International Law Studies, Volume 89, 2013.

82. Gourgourinis, Anastasios. General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System. - The European Journal of International Law, Volume 22, Issue 4, 2011.

83. Graham, David E. Cyber Threats and the Law of War. - Journal of National Security Law & Policy, Volume 4, 2010.

84. Griebel, Jörn; Plücken, Milan. New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia. - Leiden Journal of International Law, Volume 21, Issue 03, September 2008.

85. Grosswald, Levi. Cyberattack Attribution Matters under Article 51 of the U.N. Charter. - Brooklyn Journal of International Law, Volume 36, Issue 3, 2011.

86. Hathaway, Oona A.; Crootof, Rebecca; Levitz, Philip; Nix, Haley; Nowlan, Aileen; Perdue, William; Spiegel, Julia. The Law of Cyber-Attack. - California Law Review, Vol 100, 2012.

87. Headen Pfitzer, James; Sabune, Sheila. Burden of Proof in WTO Dispute Settlement: Contemplating Preponderance of the Evidence. - ICTSD Dispute Settlement and Legal Aspects of International Trade, April 2009, Issue Paper No. 9. Arvutivõrgus: http://www.ictsd.org/downloads/2012/02/burden-of-proof-in-wto-dispute-settlement.pdf (04.05.2015).

88. Hoffman, David E. The New Virology. From Stuxnet to biobombs, the future of war by other means. - Foreign Policy, 21. veebruar 2011. Arvutivõrgus: http://foreignpolicy.com/2011/02/21/the-new-virology/ (04.05.2015).

89. Hoisington, Matthew. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. - Boston College International and Comparative Law Review, Volume 32, Issue 2, 2009.

90. Hollis, Duncan B. An e-SOS for Cyberspace. - Harvard International Law Journal, Vol 52, Issue 2, 2011.

91. Jensen, Eric Talbot. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. - Stanford Journal of International Law, Volume 38, Issue 2, 2002.

92. Kantzer, Kenneth Han-Wei. Cyber Attack Attribution: An Asymmetrical Risk to U.S. National Security. Bakalaureusetöö. Princeton: Princeton University 2011.

93. Kelly, Brian B. Investing In a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform. - Boston University Law Review, Vol 92, 2012.

94. Knake, Robert K. Internet Governance in an Age of Cyber Insecurity. - Council Special Report, No. 56, September 2010. Arvutivõrgus: http://www.cfr.org/internet-policy/internet-governance-age-cyber-insecurity/p22832 (04.05.2015).

95. Lin, Herbert S. Offensive Cyber Operations and the Use of Force. - Journal of National Security Law and Policy, Vol 4, 2010.

96. Lipson, Howard F. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global

Policy Issues. - Carnegie Mellon University, 2002.

97. Margulies, Peter. Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. - Melbourne Journal of International Law, Vol 14, 2013.

98. McGhee, James E. Hack, Attack or Whack; The Politics of Imprecision in Cyber Law. - Journal of Law & Cyber Warfare, Vol. 4, Issue 1, 2014.

99. Milanović, Marko. State Responsibility for Acts of Non-state Actors: A Comment on Griebel and Plücken. - Leiden Journal of International Law, Volume 22, Issue 02, June 2009.

100. Nazario, Jose. Politically Motivated Denial of Service Attacks. - The Virtual Battlefield: Perspectives on Cyber Warfare. IOS Press: Amsterdam, 2009.

101. Nguyen, Reese. Navigating Jus Ad Bellum in the Age of Cyber Warfare. - California Law Review, Vol 101, 2013.

102. Owens, William A.; Dam, Kenneth W.; Lin, Herbert S. (toim). Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. The National Academies Press: Washington, DC, 2009, lk 41.

103. Panetta, Leon E. Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York 11.10.2012. Transkriptsioon arvutivõrgus: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (04.05.2015).

104. Pihelgas, Mauno. Back-Tracing and Anonymity in Cyberspace. Artikkel raamatus: Ziolkowski, Katharina (toim). Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy. NATO CCD COE Publication: Tallinn, 2013.

105. Proulx, Vincent-Joël. Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks? Berkeley Journal of International Law, Volume 23, Issue 3, 2005, lk 623.

106. Rahvusvahelise Õiguse Komisjon. Draft Articles on State Responsibility with Commentaries thereto Adopted by the International Law Commission on First Reading. Arvutivõrgus: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf.

107. Rahvusvahelise Õiguse Komisjon. Report of the Commission to the General Assembly. Report of the International Law Commission on the work of its twenty-first session, 2 June-8 August 1969. Yearbook of the International Law Commission 1969, Volume 2, United Nations: New York. Arvutivõrgus: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes(e)/ILC_1969_v2_e.pdf.

108. Rajković, Nikolas. On 'Bad Law' and 'Good Politics': The Politics of the ICJ Genocide Case and Its Interpretation. - Leiden Journal of International Law, Volume 21, Issue 04, December 2008.

109. Richardson, John. Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. - Journal of Computer & Information Law, Vol 29, 2011-2012.

110. Robertson, Jordan; Riley, Michael A. Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar. - Bloomberg, 10. detsember 2014. Arvutivõrgus: http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-

blast-opened-new-cyberwar. (04.05.2015)

111. Rogers, Michael. Hearing of the House (Select) Intelligence Committee on the subject of “Cybersecurity Threats: The Way Forward". - Federal News Service: Washington D.C, 2014. Arvutivõrgus: https://www.nsa.gov/public_info/_files/speeches_testimonies /ADM.ROGER S.Hill.20.Nov.pdf (04.05.2015).

112. Roscini, Marco. World Wide Warfare: Jus ad bellum and the Use of Cyber Force. - Max Planck Yearbook of United Nations Law, Volume 14, 2010;

113. Ryan, Daniel J.; Dion, Maeve; Tikk, Eneken; Ryan, Julie J. C. H. International Cyberlaw: A Normative Approach. - Georgetown Journal of International Law, Vol. 42, Issue 4, 2011.

114. Sang-Hun, Choe; Markoff, John. Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea. - The New York Times, 8.07.2009. Arvutivõrgus: http://www.nytimes.com/2009/07/09/technology/09cyber.html (04.05.2015).

115. Sanger, David E.; Barboza, David; Perlroth, Nicole. Chinese Army Unit Is Seen as Tied to Hacking Against U.S., - The New York Times, 18. veebruar 2013. Arvutivõrgus: http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

116. Schmitt, Michael N. (toim.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge; New York: Cambridge University Press, 2013. Arvutivõrgus: https://issuu.com/nato_ccd_coe/docs/tallinnmanual/1?e=0/1803379 (05.04.2015).

117. Schmitt, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. - Columbia Journal of Transnational Law, Volume 37, Issue 3, 1999.

118. Schmitt, Michael N. Cyber Operations and the Jus Ad Bellum Revisited. - Villanova Law Review, Volume 56, Issue 3, 2011.

119. Schmitt, Michael. International Law and Cyber Attacks: Sony v. North Korea. - Just Security, 17. detsember 2014. Arvutivõrgus: http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (04.05.2015).

120. Schreier, Fred. On Cyberwarfare. - DCAF Horizon 2015 Working Paper No. 7, 2015.

121. Shackelford, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. - Berkeley Journal of International Law, Volume 27, Issue 1, 2009.

122. Shackelford, Scott J.; Andres, Richard B. State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. - Georgetown Journal of International Law, Vol 42, 2001.

123. Shackelford, Scott. Holding States Accountable for the Ultimate Human Right Abuse: A Review of the International Court of Justice’s Bosnian Genocide Case. - Human Rights Brief, Volume 14, Issue 3, March 2007.

124. Shaw, Malcolm N. International Law, 6th edition. Cambridge [etc.]: Cambridge University Press, c2008, 2011.

125. Sklerov, Matthew J. Solving The Dilemma Of State Responses To Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to

Prevent. - Military Law Review, Volume 201, Fall 2009, lk 8.

126. Zimmermann, Andreas; Tomuschat, Christian; Oellers-Frahm, Karin (toim). The Statute of the International Court of Justice: A Commentary. Oxford: Oxford University Press, 2006.

127. Thienel, Tobias. The Burden and Standard of Proof in the European Court of Human Rights. German Yearbook of International Law. Berlin: Duncker & Humblot.

128. Tikk-Ringas, Eneken. Küberjulgeoleku õiguslik raamistik. - Juridica IV/2012, lk 277.

129. Tikk, Eneken, Kaska, Kadri, and Vihul, Liis. International Cyber Incidents - Legal Considerations, 2010, lk 74. Arvutivõrgus: https://ccdcoe.org/publications/books/legalconsiderations.pdf (04.05.2015).

130. Tsagourias, Nicholas. Cyber-attacks, Self-defence and the Problem of Attribution. Journal of Conflict and Security Law, Volume 17, Issue 2, 2012.

131. United Nations. Materials on the Responsibility of States for Internationally Wrongful Acts. New York: United Nations, 2012.

132. Waxman, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). - Yale Journal of International Law, Volume 36, Issue 2, 2011.

133. Wheeler, David A.; Larsen, Gregory N. Techniques for Cyber Attack Attribution. - Institute for Defense Analyses, IDA Paper P-3792, October 2003.

134. World Trade Organization. Legal issues arising in WTO dispute settlement proceedings: Burden of proof. Arvutivõrgus: https://www.wto.org/english/tratop_e/dispu_e/disp_settlement_cbt_e/c10s6p1_e.htm (04.05.2015).

135. Värk, René. Riigi vastutus mitteriiklike terroristlike rühmituste eest. - Juridica, (2012), 20(2).

136. Värk, René. Terrorism, State Responsibility and the Use of Armed Force. - ENDC Proceedings, Number 14, Volume 2, 2001.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Sille Rästas,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Küberrünnakute omistamine riigile rahvusvahelises õiguses", mille juhendajad on Erki Kodar ja Mario Rosentau,

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, **04.05.2015**