TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Õiguse instituut

Andres Vaet

MITTESÕJALISTE KÜBERRÜNNETEGA TEKITATUD KAHJUDE HINDAMINE MITTESEKKUMISE PRINTSIIBIST LÄHTUVALT

Magistritöö
Õppekava Eesti avalik ja eraõigus

Juhendaja: Eneken Tikk, PhD
Kaasjuhendaja: Agnes Kasper, PhD

Tallinn 2018

Deklareerin, et olen koostanud töö iseseisvalt ja
olen viidanud kõikidele töö koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on 17564 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Andres Vaet ……
(allkiri, kuupäev)
Üliõpilase kood: 162705HAJM
Üliõpilase e-posti aadress: andresvaet@gmail.com

Juhendaja: Eneken Tikk, PhD:
Töö vastab kehtivatele nõuetele

……
(allkiri, kuupäev)

Kaasjuhendaja Agnes Kasper, PhD:
Töö vastab kehtivatele nõuetele

……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees: /lisatakse ainult lõputöö puhul/
Lubatud kaitsmisele

……
(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Antud töö eesmärk on välja selgitada kuidas hinnata küberrünnaku poolt tekitatud kahju. Töö keskendub poliitiliselt motiveeritud küberrünnetele. Töö eesmärk on ka analüüsida, kas küberründe tagajärjel võib tekkida hüvitamisele kuuluvat kahju. Töö uurimismetoodika sisaldab analüüsi, kus hinnatakse kas on võimalik lahendada tänapäeva maailmas tekkivaid uusi õiguslike probleeme juba eksisteeriva rahvusvahelise õiguse põhimõtetega või nende edasi arendamisega.

Töö uurimisprotsess kujutab endast rahvusvaheliste lepingute tõlgendamist, rahvusvahelise õiguse põhimõtete uurimist, mõistete defineerimist, kohtulahendite analüüsi ning õigusteaduslike tekstide uurimist. Töös on kasutatud valdavalt inglise keelseid allikaid. Töö esimeses pooles avatakse riigi vastutuse printsiip, mis on kahju hüvitamise teooria aluseks. Teises peatükis tutvustab autor kahju hüvitamise teooriat riigivastutuse õigusest lähtuvalt. Viimases peatükis avab autor küberrünnaku mõiste ning tutvustab olulisemaid küberrünnakute liike. Seejärel annab autor ülevaate kahjudest, mis võivad tekkida küberrünnaku tagajärjel. Viimane peatükk lõppeb kahjude hindamise metoodika tutvustamisega ning selle kohaldatavuse kontrollimisega riigivastastele küberrünnakutele.

Töö otsib vastust küsimusele kas riigil on võimalik nõuda küberrünnakuga tekitatud kahju hüvitamist, kui küberrünnak kujutab endas mittesekkumise printsiibi rikkumist. Analüüsides rahvusvahelisi kohtulahendeid tõdeb autor, et riigil on võimalik nõuda kahju hüvitamist.

Võtmesõnad: küberrünnak, riigivastutus, kahju hüvitamine

SISSEJUHATUS

Info- ja kommunikatsioonitehnoloogiate (edaspidi IKT) jätkuv kiire areng ja üleilmastumine omavad mõju nii inimeste igapäevaelule kui riigi majandusele ja üldisele toimimisele. Selle tulemusel on tekkinud uued võimalused ja vajadused majandusliku heaolu kasvatamiseks ja julgeoleku tagamiseks. IKT kiire areng on toonud kaasa teenuste parema kättesaadavuse ja kasutusmugavuse, parandanud riigi toimimise läbipaistvust ning vähendanud avaliku- kui erasektori kulutusi. Samuti on suurenenud nii inimeste omavaheline seotus kui ka riigi inimese vastastikune seotus ja sõltuvus. Teisest küljest on tehnoloogia osatähtsus ühiskonnas kasvatanud majanduse ja riigi sõltuvust e-lahendustest ning loonud ootuse e-teenuste tõrgeteta toimisele.[1] Koos IKT arenguga on kasvanud ka pahatahtlike küberinsidentide arvukus ja ulatus. 2017. aastal registreeriti Eestis esmakordselt üle 10 000 küberjuhtumi, millest veerandi moodustasid juhtumid, millega kaasnes otsene mõju teabe või süsteemide konfidentsiaalsusele, kättesaadavusele ning terviklikkusele. Küberinsidentide maht kasvab ka terves maailmas. Lunavarainsidentide hulk kasvas võrreldes 2017. aastaga 36% võrra ning teenustõkestusrünnete arv tõusis 7,5 miljonini. Samuti kasvasid kasutajainfo lekked ning pahavara rünnakute arv.[2]

Küberkuritegevus ei kujuta endas ohtu aga ainult maailma majandusele. Riigid on hakanud üha vilunumalt kasutama digitaalset keskkonda mõjutustegevuseks ja geopoliiitlise positsiooni tugevdamiseks. Üha rohkem ja rohkem esineb maailmas poliitilistel põhjustel tekitatud võrguhäireid ning samuti on tihenenud katsed, kus püütakse mõne teise riigi või organisatsiooni võrkude üle kontrolli saada. 2015 aastal rünnati vahetult enne jõule Ukraina elektrijaama, mille tulemusel jäid inimesed tundideks elektrita, juhtumis kahtlustati Vene Föderatsiooni.[3] 2017. aastal raputas maailma ka kaks suurt pahavarakampaaniat WannaCry ja Petya/NotPetya. Wannacry nakkatas umbes 400 000 seadet ning hinnanguliseks kahjuks loetakse 4 miljardit dollarit. Küberrünnak mõjutas ainuüksi Ühendkuningriigis rohkem kui 600 tervishoiuasutust[4], küberrünnaku taga arvatakse olevat Põhja-Korea. Petya/NotPetya nakatas kuni 20 000 erinevat seadet ning tekitas hinnanguliselt 1,2 miljardit dollarit kahju. Selle aasta veebruaris omistas Ameerika Ühendriikide valitsus vastutuse Venemaa valitsusele ja sõjaväele. USA avalduse

[1] Majandus- ja kommunikatsiooniministeerium. (2014). Küberjulgeoleku strateegia 2014-2017, 4. Kättesaadav: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf 14.05.2018.
[2] Riigi Infosüsteemide Amet. (2018). Küberturvalisus 2018, 5. Kättesaadav: https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf 14.05.2018.
[3] Zetter, K. (2016). Inside the cunning, unprecedented hack of ukraine's power grid – Wired, 3. Märts.
[4] National Audit Office. (2017). Investigation: WannaCry cyber attack and the NHS. – 27. Oktoober.

kohaselt oli NotPetya näol tegemist maailma kulukaima küberründega, tekitades mitme miljardi ulatuses kahju.[5] Olulisemateks demokraatlike protsesside vastasteks rünnakuteks saab pidada 2016. aastal Ameerika Ühendriikides ja 2017. aastal Prantsusmaal toimunud presidendi valimistega seotud küberrünnakuid. Mõlemaid küberünnakuid iseloomustab ründe eesmärk, mis oli avalikkuse meelsusega manipuleerimine ning avalikkus usalduse kahjustamine valimisprotsessi vastu.[6]

Arvutiturbefirma McAfee ja Strateegiliste ja Rahvusvaheliste Uuringute Keskus (CSIS) poolt läbi viidud uuringu kohaselt on küberkuritegevuse majanduslik mõju kasvanud vahemikus 2013-2017 viis korda.[7] 2017. aastal läbi viidud uuringu kohaselt ulatub küberkuritegevuse kahju 600 miljardi dollarini aastas.[8] Seega võib järeldada, et küberrünnakutel ei ole oluline mõju ainult majandusele, vaid ka demokraatlikele protsessidele. Lähtudes riigivastutuse õigusest, uurib autor millised vahendid on poliitiliselt motiveeritud küberrünnakute ohvriks langenud riigil enda õiguste kaitsmiseks ning mis on nende vahendite rakendamise eeldused. Töö võtab aluseks poliitiliselt motiveeritud küberrünnakute uurimise, kahjude hüvitamise võtmes. Töö eesmärk on ka välja selgitada, kuidas hinnata poliitilist laadi küberrünnakutega tekitatud kahju, ning analüüsida, kas hüvitamisele kuuluvat kahju tekib. Töö uurimisküsimuseks on kas riigil on võimalik nõuda küberrünnakuga tekitatud kahju hüvitamist mittesekkumise põhimõtte rikkumise korral?

Antud töö on nii teoreetiline kui ka rakenduslik uurimistöö. Töö uurimismetoodika sisaldab analüüsi, kus hinnatakse kas on võimalik lahendada tänapäeva maailmas tekkivaid uusi õiguslike probleeme juba eksisteeriva rahvusvahelise õiguse põhimõtetega või nende edasi arendamisega. Tegemist on kvalitatiivse uuringuga, kus uurimisprotsess kujutab endast rahvusvaheliste lepingute tõlgendamist, rahvusvahelise õiguse põhimõtete uurimist, mõistete defineerimist, kohtulahendite analüüsi ning õigusteaduslike tekstide uurimist.

[5] Greenberg, A. (2018). The White House blames Russia for notpetya, the 'most costly cyberattack in history'. – Wired, 15. Veebruar.
[6] Majandus- ja kommunikatsiooniministeerium (2014), supra nota (1), lk 35.
[7] McAfee & Centre for Strategic and International Studies. (2014). Net losses: Estimating the Global Cost of Cybercrime. Kättesaadav: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf 14.05.2018.
[8] Center for Strategic and International Studies & McAfee. (2018). Economic impact of Cybercrime – No slowing down. Report. Kättesaadav: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70- 13.05.2018.

Käesolev magistritöö koosneb kolmest peatükis, millest esimene peatükk avab riigivastutuse mõiste ja selgitab printsiibi kujunemislugu rahvusvahelises õiguses. Teises peatükis analüüsib autor kahjude sissenõudmise teooriat ja kohtupraktikat ning kolmas peatükk sisaldab endas kahjude hindamise analüüsi.

Esimeses peatükis analüüsib autor, tuginedes riigivastutuse artiklitele ja kohtu lahenditele, millistel alustel riikidele vastutust omistatakse. Esmalt käsitletakse riigivastutuse õiguse ja omistamisreeglite ajaloolist kujunemist ja sisu. Seejärel analüüsitakse omistamisreegleid üldiselt. Reeglid, mis puudutavad riigi vastutus tulenevad rahvusvahelisest tavaõigusest, kohtulahenditest ja eraldi lepingutest ning on kogutud riigivastutuse eelnõusse. Autor kasutab riigivastutuse printsiibi lahti mõtestamisel Riigivastutuse artiklite kommentaare ja kohtulahendeid, et selgitada, millised on nõutud eeldused riigivastututuse omistamiseks.

Teises peatükis keskendub autor kahjude sissenõudmise teooria analüüsimisele. Selles peatükis avatakse kõigepealt kahju hüvitamise teooria kohaselt olulised mõisted ning seejärel analüüsitakse erinevaid kahju hüvitamise vorme. Lisaks riigivastutuse reeglite analüüsimisele kasutab autor ka kohtulahendite analüüsi.

Kolmandas peatükis keskendub autor küberrünnakute kahjude analüüsimisele. Autor käsitleb nelja erinevat küberrünnakut, mis on Välisasjade nõukogu statistika kohaselt toime pandud riigi vastu. Autor tutvustab, millist liiki kahju võib tekkida iga erineva küberrünnaku lõikes. Lisaks sisaldab peatükk küberrünnakute kahjuga seotud analüüsi, võttes aluseks küberkuritegevuse kahjude hindamise metoodika ja statistika.

1. RIIGI VASTUTUSE PRINTSIIP

1.1. Riigivastutuse printsiibi areng rahvusvahelises õiguses

Rahvusvaheliste suhete puhul, nagu ka kõikide teiste sotsiaalsete suhete korral, toob õigussubjekti õiguste rikkumine kaasa rikkuja poolse vastutuse, kus vastutuse sisu määrab kindlaks õigussüsteem. Rahvusvahelise vastutuse puhul on õigussubjektideks tavapäraselt riigid, kuid vastutus on oma olemuselt laiem küsimus, mis puudutab kõiki õigussubjekte. Riigivastutuse küsimus on õigusteadlaste seas olnud enim vasturääkivusi põhjustanud teema. Juba keskajal sisaldasid rahvusvahelised lepingud endas konkreetseid sanktsioneerivaid ja kohustavaid norme, mis rakendusid lepingu rikkumise korral. Rahvusvahelise Kohtu praktika, koosmõjus eraviisiliste sunnimeetmete kasutamise tülikusega on kaasa aidanud vastutustundlikuma riigi vastutuse printsiibi väljatöötamisele. Õigusvastaste tegudega võitlemisel olid reparatsiooni ja kahju hüvitamise institutsioonid Euroopas kasutusel juba sajandeid ning ka klassikalised kirjanikud, sh Hugo Grotius, osutasid tihti hüvitise ja reparatsioonide õigusele seoses ebaõiglase sõjapidamisega.[9]

Rahvusvaheline vastutus ei olnud kuni 19. sajandi lõpuni õigusteadusliku uurimise aluseks. Varasemad õigusteadlased nagu Francisco de Vitoria, Francisco Suarez ja Jean Bodin ei näinud vastutust kui eraldi õiguseteadusliku valdkonda, vaid lähenesid vastutusele teoloogilisest vaatevinklist, mille kohaselt on suverään vastutav ainult jumala ees.[10]

Ehkki Hugo Grotius ei määratlenud rahvusvahelist vastutust kui eraldiseisvat õiguslikku valdkonda, oli tema esimene, kes käsitles vastutust süstemaatiliselt. Grotius uuris juhtide vastutust ja nende karistamist seoses sõjapidamisega, ning ei teinud selget vahet individuaalse- ja riigi vastutuse vahel. Põhjus, miks ükski varajastest kirjanikest ei määratlenud vastutust eraldi õigusvaldkonnana oli selles, et rahvusvahelisel tasandil puudusid institutsioonid, mis oleksid nõudnud riigi vastutuse selget eristamist seal elavate kodanike vastutusest või oleksid keskendunud reparatsioonide maksmise kohustusele. Pärast Grotiust muutus rahvusvaheliste lepingute rikkumisega kaasnevate kohustuste mõiste järk-järgult õigusliku uurimise aluseks, kuid see protsess oli aeglane ja ebaühtlane. Alles Christian Wolffiga kaasnes arusaam riigi vastutusest

[9] Brownlee, I. (2003). Principles of Public International law. Fifth Edition. New York: Oxford University Press, 435.
[10] Crawford, J. (2013). State Responsibility: The General Part. New York; Cambridge: Cambridge University Press, 3.

kui kohustusest maksta teisele suveräänile tekitatud kahju eest reparatsioone. Wolff sõnastas tänapäevase kontseptsiooni sekundaarsest kohustusest, mille kohaselt tekib lepingut rikkunud riigil kohustus maksta reparatsioone. Emerich de Vattel, tuginedes Wolffile leidis, et rahvusvaheline vastutus sisaldab endas kohustust mitte kahjustada teisi riike. Lisaks leidis Vattel, et kodanike vastu suunatud tegusid võib lugeda toimepanduks ka riigi vastu üldiselt.[11]

Heinrich Triepili ja Dionisio Anzilottit võib pidada esimesteks autoriteks, kes käsitlesid riigi vastutust kui iseseisvat õigusvaldkonda. Anzilotti tegeles peamiselt riigi vastutusega välismaalastele põhjustatud kahju eest, kuid tema käsitlust riigi vastutuse omistamise kriteeriumitest võib pidada tänapäevase riigi vastutuse printsiibi aluseks. Anzilotti leidis, et riigi vastutuse eelduseks on rahvusvahelisest õigusest tuleneva kohustuse rikkumine ning selle omistatavus riigile. [12]

Riigi vastutust reguleerivaid sätteid on eelmise sajandi jooksul järk-järgult arendatud, kuid riigi vastutuse kontseptsioon, kindlalt määratletud tuumaga on hiljutine nähtus.[13] Tänapäevase käsitluse järgi saab riigi vastutuse printsiipi pidada rahvusvahelise õiguse aluspõhimõtteks, mis on tekkinud rahvusvahelise õigussüsteemi olemusest ning riikide suveräänsuse ja võrdsuse doktriinidest.[14] Rahvusvahelisel tasandil võetud kohustuse rikkumise suhtes, olenemata, kas kohustus tuleneb tavaõigusest või lepingust, kohalduvad alati riigi vastutuse reeglid.[15] Riigi rahvusvahelisel vastutusel on kõige lähedasem seos rahvusvahelise õiguse tuuma, teleoloogiaga ning ka rahvusvahelise õiguskorra loomisega. Riigi vastutuse printsiipi võib vaadelda üldiselt kui globaalset süsteemi, mis kehtestab funktsionaalsed reeglid, kuidas rahvusvahelise õiguse subjektid omavahel suhtlevad. Rahvusvahelise vastutuse kontseptsiooni võib tõlgendada ka kui vaheetappi, mis jääb ühelt poolt siseriikliku õiguse ja riigi suveräänsuse vahelise seose ning teiselt poolt rahvusvahelise õiguse printsiipide reaalse rakendamise vahele.[16]

Esimene katse kodifitseerida riigi vastutuse õigust toimus 1930. aastal Haagis I rahvusvahelise õiguse kodifitseerimise konverentsil. Riigivastutuse komisjon võttis eesmärgiks luua ühtne

[11] *Ibid.*, lk 18.
[12] *Ibid.*, lk 22.
[13] Dimitrovska, M. (2015). The concept of International responsibility of state in the International public law system. *Journal of Liberty and International Affairs* Vol. 1, No. 2, 2.
[14] Shaw, M.N. (1997*). International Law. Fourth edition*, Cambridge (UK). Cambridge University Press, 541.
[15] Crawford, J. (2010). The system of International responsibility. *Oxford commentaries on International law*. New York: Oxford University Press. 20-21.
[16] Dimitrovska, M. (2015), *supra nota* 5, lk 2-3.

raamistik seoses riigi vastutusega välismaalaste ja nende varale põhjustatud kahjuga, võttes aluseks 1927. aastal Rahvusvahelise Õiguse Instituudi ja Harvardi Ülikooli koostatud eelnõud. Riigivastutuse komisjoni ettepanekud leidsid tulist vastuseisu ning ajapuuduse tõttu ei jõutud püstitatud eesmärgini.[17]

Töö riigivastutuse printsiibi väljatöötamisega jätkus 1956. aastal, kui Rahvusvahelise Õiguse Komisjonis määras riigi vastutuse valdkonna arendamise eest vastutavaks eriraportööri Garcia Amadori. Eriraportör G. Amadori varajane töö keskendus sarnaselt Haagi Konverentsil riigi vastutusele seoses välismaalaste ja nende varale põhjustatud kahjuga. Kuigi G. Amador esitas aastatel 1956-1961 kuus aruannet, leidsid need vähe kõlapinda ning 1957. aasta arutelu näitas, et riikide seas puudus ühtne arusaam, millises suunas riigi vastutuse printsiibi arendamisega edasi minna. 1962. aastal tehti ettepanek muuta esialgset uurimise teemat ning keskenduti riigi rahvusvahelise vastutuse üldreeglite määratlemisele. Uus suund ei tähendanud mitte sisuliste eeskirjade väljatöötamist ega nendest tulenevate riikide konkreetsete kohustuste väljatöötamist, vaid keskendus vastutuseeskirjade raamistikule, määratlemaks kas riik on toime pannud rikkumise ning millised on selle tagajärjed. Rahvusvahelise Õiguse Komisjon kiitis teema ümberkodifitseerimise heaks ning määras 1963. aastal uueks eriraportööriks Robert Ago.[18] Eriraportöör R. Ago oli vastutav projekti põhistruktuuri ja suuna kehtestamise eest. Ajavahemikul 1969-1980 koostas ta kaheksa aruannet ning Rahvusvahelise Õiguse Komisjon võttis ajutiselt vastu kokku 35 artiklit, mis moodustasid riigivastutuse artiklite esimese osa (riigi vastutuse tekkimise alused). Oma esimeses aruandes leidis Ago, et riigi vastutus ei tohiks taanduda ainult tagajärgedele, eriti kohustusele hüvitada tekitatud kahju. Antud põhimõtet väljendas ta eelnõu esimeses artiklis: „Iga rahvusvahelise õiguse vastane tegu toob kaasa rikkujariigi vastutuse“. Tegemist oli riigivastutuse kontseptsiooni revolutsioonilise muutusega, kus „kahju“ ei olnud enam vastutuse tekkimise eelduseks. Ago lähenemine leidis õigusteadlaste seas palju toetust, mida kinnitab ka asjaolu, et esimese artikli sõnastus jäi muutmata kujul eelnõusse aastani 2001.[19] Teise olulise muutusena liigitas Ago riigivastutuse artiklid teisejärgulisteks rahvusvahelise õiguse

[17] Bories, C. (2010), The Hague conference of 1930. *The law of International responsibility. Oxford commentaries on International law*. New York: Oxford university press, 61-67.
[18] Crawford, J. (2012). State Responsibility. *Max Planc Encoclopedia of Public International Law*. Volume IX, 517-533.
[19] Pellet, A. (2010). The ICL articles on state responsibility for internationally wrongful acts and related texts. *The law of International responsibility. Oxford commentaries on International law*. New York: Oxford university press, 75-94.

normideks, kuna need puudutavad esmaste õigusnormide alusel kehtestatud kohustuste rikkumise tagajärgede kindlaksmääramist.[20]

1971. aastal määrati eriraportööriks Willem Riphagen. Aastatel 1980-1986 esitas ta seitse aruannet, mis sisaldasid riigivastutuse artiklite teist (rahvusvahelise vastutuse sisu, vormid ja astmed) ja kolmandat (vaidluste lahendamine) osa. Teiste teemade eelistuste tõttu võeti ajutiselt vastu ainult viis artiklit teisest osast. 1987. aastal määrati eriraportööriks Gaetano Arangio, kes esitas aastatel 1988 kuni 1995 samuti seitse aruannet, mis võimaldasid 1996. aastal Rahvusvahelise Õiguse Komisjonil läbi viia eelnõu esimene lugemine. 1997. aastal määrati eriraportööriks James Crawford ning 2001. aastal võeti vastu Rahvusvahelise Õiguse Komisjoni poolt välja töötatud riikide vastutuse eelnõu artiklid.[21]

Riigivastutuse eelnõu artiklite ülesanne ei ole täpsustada rahvusvahelise õiguse subjekti kohustava õigusnormi sisu ega nende tõlgendamist. Samuti ei käsitleta artiklites küsimust, kas ja kui pikalt antud kohustav õigusnorm kehtib õigussubjektile. Kas riik on kehtiva lepingu osaline, kas leping kehtib selle riigi suhtes ja milliste sätete osas ja kuidas lepingut tõlgendatakse, tuleb otsustada primaarseid kohustusi loova lepingute õigusest lähtuvalt. Eelnõu artiklid pakuvad raamistiku selleks, et otsustada, kas riik on lepinguga võetud kohustust rikkunud ning millised õiguslikud tagajärjed sellele rikkumisele järgnevad. Eelnõu artiklid käsitlevad tagajärgi, mis tulenevad rahvusvahelise õiguse vastaste tegude toime panemisest. Rahvusvaheline vastutus tuleneb üksnes rahvusvahelise õigusega vastuolus olevast õigusvastasest tegevusest. Ühelt poolt puudutavad eelnõu artiklid ainult riikide vastutust rahvusvaheliselt süülise käitumise eest, jättes kohaldamisalast välja rahvusvahelised organisatsioonid või muud valitsusvälised üksused. Teiselt poolt on käesolevad artiklid seotud kogu riigi vastutuse valdkonnaga. Seega ei piirdu nad ainult kahepoolsete kohustuste rikkumisega, nt riikide kahepoolsete lepingute alusel, vaid on kohaldatavad kogu rahvusvaheliste kohustuste valdkonna suhtes, olenemata sellest, kas kohustus on võlgu ühele või mitmele riigile, üksikisikule, grupile või rahvusvahelisele üldsusele tervikuna. Sellegipoolest on riigid vabad sõlmima kokkuleppeid, millega määratakse kindlaks konkreetsed tagajärjed lepingu rikkumisel, jättes välja üldised riigi vastutuse eeskirjad. [22]

[20] Wood, M., Pronto, A. (2010). *The international law commission 1999-2009. Volume IV: Treaties, final draft articles and ohter meterials*. New York: Oxford University Press,128.
[21] Crawford (2012), *supra nota* 11, lk 517-533.
[22] United Nations (2008), *supra nota* 9, lk 31.

1.2 Riigi vastutuse printsiip

Klassikalise riigivastutuse teooria kohaselt koosnes riigi vastutus kolmest sambast, milleks olid rahvusvahelise õiguse vastane tegu, selle läbi tekitatud kahju ning selle teo omistatavus riigile.[23] Hugo Grotius määratles vastutust kui loomupärast kohustust hüvitada tekitatud kahju, mis sai traditsioonilise riigi vastutuse printsiibi aluspõhimõtteks. Traditsioonilist teooriat riigi vastutusest on kõige paremini väljendanud Dionisio Anzilotti, kelle sõnade kohaselt kujutab riigivastutus endas õigussuhet, kus õigusvastase teo toimepanijal on kohustus hüvitada tekitatud kahju ning õigustatud riigil on õigus reparatsioonideks.[24] Seda arusaama riigi vastutuse printsiibist kajastatakse ka kohtuasjas *Chorzow Factory*, kus Alaline Rahvusvaheline kohus leidis, et kohustuse rikkumise tulemusel tekitatud kahju hüvitamine on rahvusvahelise õiguse printsiip.[25] Charlez de Visscher kirjeldas riigi vastutust kui õiguse aluspõhimõtet, mis taandub kahju tekitanud riigi kohustusele maksta reparatsioone. Seega traditsioonilise käsitluse järgi ei olnud kahju hüvitamine mitte ainult riigi vastutuse tagajärjeks, vaid kohustus kahju hüvitada tähendaski riigivastutust kui printsiipi. [26]

Tänapäevast riigivastutuse käsitlust iseloomustab kõige paremini riigivastutuse eelnõu artikkel 1, mis ütleb, et iga rahvusvahelise õiguse vastane tegu toob endaga kaasa riigi vastutuse. Eelnõu esimene artikkel sätestab riigi vastutuse printsiibi aluspõhimõtte, mille kohaselt tekib vastutus iga rahvusvahelise õiguse vastase teo toimepanemisel. Artikkel 1 ei sätesta täpseid eeldusi vastutuse tekkimiseks, nagu teo toimepanija süü või kannatanud riigi kahju. Samuti ei täpsustata artikli sõnastuses, kas õigusnorm kohaldub ühele riigile, riikidele või rahvusvahelistele organisatsioonidele. Mõiste "rahvusvaheline õigusvastane tegu" on ette nähtud igasuguse riigi õigusvastase käitumise katmiseks, olenemata sellest, kas see tuleneb ühest või mitmest eraldiseisvast teost või tegevusetusest või nende kombinatsioonist. Iga riik vastutab oma eksimuse eest, mis ei piira võimalust, et teine riik võib olla vastutav sama õigusvastase käitumise eest, kui see on toimunud viimase riigi kontrolli all või tema volituste kohaselt.[27]

[23] Stern, B. (2010). The elements of an internationally wrongful act. *The Law of International Responsibility. Oxford commentaries on International law*. New York: Oxford university Press,194-220.
[24] Pellet, A. „The definiton of responsibility in International law“ *The law of International responsibility. Oxford commentaries on International law*. New York: Oxford university press 2010, 5.
[25] Kohtuotsus, PCIJ. 26.07.1927, Factory at Chorzow, (Saksamaa v Poola). (ser. A), No. 9.
[26] Stern, B. (2010), *supra nota* 16, lk 194.
[27] Crawford (2012), supra nota 2, lk 517-533.

Alaline Rahvusvaheline Kohus on artikkel 1 sätestatud printsiipi rakendanud mitmetes kohtulahendites. *Phosphates in Morocco* kohtulahendis leidis kohus, et kui üks riik paneb toime rahvusvahelise õigusvastase teo teise riigi suhtes, rakendub koheselt riigivastutuse printsiip.[28] Kohtuasjas *Corfu Channel* leidis kohus, et Albaania riik on vastutav kahju eest, mis tekkis meremiinide asetamisest enda territoriaalvetesse, kuna jättis teatamata meremiinidest tulenevast ohust. Kohus leidis, et taoline tegevusetus hõlmab Albaania rahvusvahelist vastutust ning Albaania on kohustatud hüvitama plahvatuste tagajärjel tekkinud kahju.[29] Alaline Rahvusvaheline Kohus kohtuasjas *Gabcikovo-Nagymaros*[30] ja Rahvusvaheline Arbitraaži Kohus kohtuasjas *Rainbow Warrior* [31] leidis, et kui riik on rikkunud rahvusvahelist lepingulist kohustust, rakenduvad riigivastutuse printsiibist ja Viini Konventsioonist tulenevad kaitsemeetmed paralleelselt. Kuid need kaks täidavad erinevaid funktsioone. Lepinguõiguse normid määravad kindlaks, millal lepingulised kohustused on riigi jaoks kehtivad ja kuidas neid kohustusi tõlgendada. Riigivastutuse printsiip aga sätestab lepingulise kohustuse rikkumise õiguslikud tagajärjed. Riik, kelle lepingust tulenevaid õigusi on rikutud, võib peatada või lõpetada lepingu vastavalt kohalduvatele lepingueeskirjade sätetele, kuid selline tegevus ei takista tal nõude esitamist reparatsioonide tasumiseks riigivastutuse sätete alusel.[32] Rahvusvaheline Arbitraaži Kohus on riigi vastutuse printsiipi rakendanud sarnaselt mitmetes kohtuasjades, nagu *Dickson Car Wheel Company*[33], *International Fisheries Company*[34], *the British Claims in the Spanish Zone of Morocco*[35] *ja Armstrong Cork Company case.*[36]

Riigi vastutuse eelnõu artikkel 2 täpsustab nõutavaid tingimusi tuvastamaks rahvusvahelise õiguse vastase teo olemasolu:

[28] Kohtuotsus, PCIJ. 14.07.1938, Phosphates in Morocco, (Itaalia v Prantsusmaa), A/B No 74.
[29] Kohtuotsus, ICJ. 1949. Corfu Channel (Suurbritannia v. Albaania), GL No 1, ICJ Rep 4, ICGJ 199.
[30] Kohtuotsus, ICJ. 1997.Gabcikovo-Nagymaros Project (Ungari v Slovakkia) I.C.J. 7.
[31] Kohtuotsus, Prantsuse-Uus-Meremaa Arbitraaži Tribunal. 30.04.1990, Rainbow warrior (Uus-Meremaa vs Prantsusmaa), 82 I.L.R. 500.
[32] Crawford (2013), supra nota 2, lk 52.
[33] Kohtuotsus, R.I.A.A. 1931. Dickson Car Wheel Company (Ameerika Ühendriigid v. Mehhiko), No.669.
[34] Kohtuotsus, R.I.A.A. 1931. International Fisheries Company (Ameerika Ühendriigid v. Mehhiko), No. 691.
[35] Kohtuotsus, R.I.A.A. 1924. British Claims in the Spanish Zone of Morocco (Suurbritannia vs Hispaania), No. 615.
[36] Kohtuotsus, R.I.A.A. 1953. Armstrong Cork Company (Ameerika Ühendriigid vs Itaalia), No. 159.

1) Õigusvastane tegu peab olema rahvusvahelise õiguse alusel omistatav riigile, kus tegu hõlmab nii tegevust kui tegevusetust.
2) Riik peab rikkuma rahvusvahelisest õigusest tulenevat kohustust.

Nagu öeldud, võib riigile omistatav käitumine seisneda nii tegevuses kui tegevusetuses. Kohtuasjas *Corfu Channel* leidis kohus, et riigivastutuse printsiibi rakendamiseks oli piisav alus, kuna Albaania riik teadis, või pidi teadma, et tema territoriaalvetesse on asetatud meremiine ning jättis sellest teisi riike teavitamata.[37] Kohtuasjas *United States Diplomatic and Consular Staff in Tehran* leidis kohus, et Iraani Islamivabariigi vastutus on tingitud tema asutuste tegevusetusest, kes ei võtnud asjakohaseid meetmeid olukorras, kus sellised sammud olid vajalikud.[38]

Rahvusvahelise õigusvastase teo olemasolu teine tingimus on see, et riigile omistatav käitumine peab rikkuma selle riigi rahvusvahelisel tasandil võetud kohustust. Rahvusvahelise kohustuse rikkumise terminoloogiat kasutatakse nii lepinguliste kui ka lepinguväliste kohustuste täitmisel. Kohtuasjas *Rainbow Warrior* määratles kohus rahvusvahelise õiguse vastast tegu kui mistahes riigi poolt võetud rahvusvahelise kohustuse rikkumist.[39] Kohtupraktikas kasutatakse lisaks termineid "rahvusvaheliste kohustuste täitmata jätmine", "rahvusvaheliste kohustustega kokkusobimatud toimingud", "rahvusvahelise kohustuse rikkumine" või "töösuhte rikkumine".[40]

Riigivastutuse eelnõu artikkel 3 sätestab, et tegevuse kvalifitseerimisel rahvusvahelise õiguse vastaseks teoks, tuleb lähtuda rahvusvahelisest õigusest, olenemata, et tegu võib olla siseriikliku õiguse alusel õiguspärane. Alaline Rahvusvaheline Kohus on kohtuasjas *Greco-Bulgarian*[41] öelnud, et on rahvusvaheliselt üldtunnustatud põhimõte, et siseriiklikud õigusaktid ei saa olla ülimuslikud riikidevaheliste lepinguliste sätete üle. [42]

[37] Kohtuotsus, ICJ. 1949. Corfu Channel (Suurbritannia v. Albaania), GL No 1, ICJ Rep 4, ICGJ 199.
[38] Kohtuotsus, PCIJ. 1980. United States Diplomatic and Consular Staff in Tehran (Ameerika Ühendriigid vs Iraan), No.64.
[39] Rainbow Warrior (1990), supra nota 23.
[40] United Nations (2008), *supra nota* 9, lk 36.
[41] Kohtuotsus, PCIJ. 1930.Greco-Bulgarian "Communities". Advisory Opinion. Series B, No. 17.
[42] United Nations (2008), *supra nota* 9, lk 37.

1.3 Riigiorganite tegevuse omistamine

Montevideo Konventsioonis riikide Õiguste ja Kohustuste kohta sätestatakse, et riik kui rahvusvahelise õiguse subjekt, peab vastama neljale kriteeriumile: [43]

1. alaline rahvastik,
2. piiritletud territoorium,
3. valitsusasutused,
4. võimekus astuda suhetesse teiste riikidega.

Kuid riik kui poliitiline abstraktsioon, ei saa tegutseda iseenesest, vaid ainult oma esindajate ja agentide kaudu. Et teatud käitumist liigitada rahvusvahelise õiguse vastaseks teoks, peab see esmajärjekorras olema riigile omistatav. Omistamine on protsess, mille läbi on rahvusvahelises õiguses võimalik tuvastada, kas isiku või mõne muu üksuse poolt toime pandud tegu saab omistada riigile ja seeläbi tuvastada riigivastutust. Omistamist peetakse seetõttu rahvusvahelises õiguses riigivastutusest rääkidest nn. baaskontseptsiooniks ja oluliseimaks tingimuseks vastutuse omistamisel.[44]

Riigi vastutse printsiip baseerub esinduse kontseptsioonil. Seega, on põhimõttelise tähtsusega küsimus, millised isikuid saab pidada riigi esindajaks ehk kelle käitumist saab omistada riigile.[45] On rahvusvaheliselt tunnustatud põhimõte, et riik on vastutav enda organite tegevuse eest. Riigiorganid koosnevad erinevatest juriidilistest isikutest, kellele kohalduvad erinevad õigused ja kohustused. Rahvusvahelise õiguse tähenduses käsitletakse riiki kui ühtset juriidilist isikut, seega on oluline, et konkreetne sündmus oleks seotud riigi tegevuse või tegevusetusega. Riigi vastutuse eelnõu artiklid 4-7 moodustavad omistamise doktriini tuuma, käsitledes riigile tema organite ja agentide tegude omistamist. [46]

[43] Montevideo Convention on the Rights and Duties of States, 26.12.1933, Montevideo.
[44] Crawford, J. (2013). *State Responsibility: The General Part (Cambridge Studies in International and Comparative Law*). Cambridge: Cambridge University Press, 115-140.
[45] Värk, J. (2012). Riigi vastutus mitteriiklike terroristlike rühmituste eest. Tallinn: Juridica. Juridica II/2012, 102.
[46] United Nations (2008), *supra nota* 9, lk 39.

1.3.1 Riigi ametlikud organid

Riigivastutuse artikkel 4 sätestab üldreegli, et rahvusvahelise õiguse kohaselt on riik vastutav kõigi oma organite tegevuse eest, olenemata sellest, kas tegemist on täidesaatva-, seadusandliku- või kohtuvõimu esindaja teoga. Artikkel 4 lõige 2 täpsustab, et termin "riigiorgan" hõlmab iga isikut või üksust, kellel on siseriikliku õiguse alusel vastav staatus.[47]

Kohtuasjas *Salvador Commercial Company* leidis kohus, et kui tegu on toime pandud ametlikult, on riik vastutav võimul olijate tegevuse eest, olenemata, kas nad kuuluvad seadusandlikku, täidesaatvasse või kohtuorganisse.[48] Riigiorgani mõiste ei piirdu ainult keskvalitsuse organite, kõrgemate ametnike või isikutega, kes on vastutavad riigi välissuhete eest, vaid laieneb kõikidele isikutele ja organitele, mis täidavad riigi või kohaliku võimu ülesandeid.[49] Kohtulahendis *United States Diplomatic and Consular Staff in Tehran* märkis Rahvusvaheline Kohus, et rahvusvahelise õigusvastase teo toimepanemisel ei ole vahet, mis tasandi riigiorganiga on tegemist. Riigivastutus rakendub kõigi riigiorganite käitumise eest, olenemata nende haldustasandist.[50] Seega tuleb mõistet „riigiorgan" mõista kõige laiemas tähenduses, hõlmates kõiki riigi valitsemisega seotud struktuuriüksuseid, sh kohalike eristaatusega organeid, mis on loodud siseriikliku õiguse alusel.

Riigiorganite tegude omistamiseks riigile ei oma tähtsust ka võimude lahususe printsiip. Võimude lahususe printsiibi rakendamine on eelkõige riigi sisepoliitiline otsus, seega ei ole võimude lahususe printsiibil tähtsust riigi organite vastutuse omistamisel. Ka Anzilotti on märkinud, et on kahtlemata viga eitada, et riiki ei saa pidada vastutaks kohtute kohtuotsuste eest pelgalt kohtuorgani iseseisvuse eest, mis ei välista täidesaatva võimu sekkumist õiguse mõistmisesse.[51] Kõige paremini ilmestavad riigivastutuse omistamist relvakonfliktid, kuna riiklike relvavägede tegevuste puhul on üldjuhul osapooled teada ja tegevuste riigile omistamine ei osutu keeruliseks. Rahvusvahelises õiguses on mõningaid arvamusi seoses automaatse omistamisega relvavägede tegevuse korral, mille korral rakenduks *ratione materiae* reegel, ehk relvavägede tegevused oleks automaatselt omistatavad riigile ka sellises olukorras, kus sõjajõud ei ole enam riigi otsese kontrolli all, nt. olukorras, kus sõjajõud on sattunud olukorda, kus nad peavad keerulistes

[47] United Nations (2008), *supra nota* 9, lk 40.
[48] Kohtuotsus, R.I.A.A. Claim of the Salvador Commercial Company ("El Triunfo Company") (El Salvador vs Ameerika Ühendriigid) No.15.
[49] United Nations (2008), *supra nota* 9, lk 41.
[50] Shaw (2008), *supra nota* 41, 788-789.
[51] Momtaz, D. (2010). Attributin of conduct to the state: state organs and entities empowered to exercise elements of govermental authority. *The law of International responsibility. Oxford commentaries on International law*. New York: Oxford University Press. 237-246.

olukordades iseseisvalt otsuseid vastu võtma. Pelk fakt, et sõdur on eksinud ja kaotanud kontakti oma vägedega ei võta temalt riigi organi staatust ja *prima facie* iga tegu mis sõdur toime paneb, ajal kui ta ei ole oma vägedega kontaktne, on omistatav riigile, isegi kui need teod on toime pandud isiklikust huvist ja enda hüvanguks. Seevastu sõjaväelaste tegevuse üle, kes puhukuse ajal panevad toime õigusrikkumisi, ei tekitaks riigivastutuse küsimust. Kõige paremini illustreerib eelmainitut *Youmansi* kohtuasi, kus Mehhiko väed ebaõnnestusid neile valitsuse poolt antud ülesandes tõrjuda rahvamassi rünnakut kolme Ameerika kodaniku suunas. [52] Lisaks rahvamassi laiali ajamise läbikukkumises, osalesid väed ka ise rahutuses. Rahutuste tulemusel sai surma 3 ameerika kodaniku. Tulenevalt asjaolust, et sõdurid olid saanud käsu kõrgemalt ohvitserilt, võeti Mehiko kolme Ameerika kodaniku surmas vastutusele. Kui Mehhiko väeüksuse liikmed oleks olnud erariietuses ning osalenud rahutuses tsiviilisikutena, ei oleks Mehhikot tõenäoliselt vastutusele võetud.[53]

Läbi seaduste, määruste ja muude õigusaktide loomise teostab riigivõimu ka seadusandja. Seadusandliku võimu poolt vastu võetud siseriiklik õigusakt, mis on vastuolus riigi rahvusvahelise kohustusega, toob kaasa riigi vastutuse. Samuti tekib riigi vastutus, kui seadusandliku võimu poolt vastu võetud siseriiklik õigusakt on vastuolus rahvusvahelisel tasandil võetud kohustusega.[54] Kohtuasjas *German Interest in Polish Upper Silesia* leidis Alaline Rahvusvaheline kohus, et rahvusvahelise õiguse seisukohast on siseriiklikud õigusaktid faktid, mis väljendavad riigi tahet ja kujutavad endas riigi tegevust, samalaadselt nagu haldusmeetmed või kohtuotsused.

Siseriikliku õigussüsteemi doktriinid nagu parlamentaarne demokraatia ei vähenda selle järelduse jõudu. Kohus võttis *Avena Interpretation* kohtuasjas seisukoha, et siseriiklik õigus, mis on takistanud riigil oma rahvusvaheliste kohustuste täitmisest, ei saa vabastada riiki võetud kohustuste täitmisest. Ameerika Ühendriikidel lubati oma kohustuste täitmiseks valida sobiv meede ja kui valitud vahendid ei saavuta mõistliku aja jooksul edu, peab ta kiiresti pöörduma alternatiivsete ja tõhusamate vahendite poole vajaliku tulemuse saavutamiseks.[55] Võimude lahususe printsiip, sarnaselt parlamentaarse suveräänsusega, on ainult riigisisese mõjuga, olenemata kui lahus üks riigiorgan on riigijuhtimisest.

[52] Kohtuotsus, R.I.A.A. 1926. Youmans (Ameerika Ühendriigid vs Mehhiko), 4 R.I.A.A. 110.
[53] Crawford (2013), *supra nota* 36, lk 123.
[54] Värk, R. 2005 Sissejuhatus rahvusvahelisse õigusesse. Tartu Ülikooli kirjastus, 112.
[55] Request fo interpretation of the judgment of 31 March 2004 in the case concerning Avena and other Mexican Nationals. ICJ rep 2009 p.3, 18.

Täpsemalt märgib WTO apellatsioonikogu, et USA, nagu ka kõik teised WTO liikmed ja üldine kogukond, kannab vastutust kõigi valitsuse osakondade, sealhulgas kohtusüsteemi tegude eest. Üks iseloomulik viis, kuidas kohtumenetlus hõlmab riigi rahvusvahelist vastutust, on välismaalaste suhtes õigusemõistmise eitamine ning teine on rahvusvaheliste lepingute väär tõlgendamine või valesti kohaldamine. *LaGranda* ja *Avenda* asjas mõisteti Ameerikas surma välisriigi kodanikud ilma, et oleks arvesse võetud nende konsulaarsuhete Viini konventsioonist tulenevaid õigusi. Rahvusvaheline Kohus nõudis täitmise peatamist, märkides, et riigi rahvusvaheline vastutus on seotud selles riigis tegutsevate pädevate organite ja asutustega, olenemata nende võimalustest. Pärast USA Riigikohtu ettekirjutuste tagasilükkamist põhiseaduslikutel põhjustel teostati Arizona osariigis hukkamised. Seejärel leidis Rahvusvaheline Kohus, et Ameerika Ühendriigid rikkusid siseriiklikele õigusaktidele tuginedes oma rahvusvahelisi kohustusi. Kohtuasjas *Alabama Arbitration* peeti Suurbritanniat vastutavaks, kuna valitsus ei takistanud kommertslaevaks maskeeritud sõjalaeva CSS Alabama ehitust, mis oli Ameerika Ühendriikide ja Suurbritannia vahelise lepingu põhimõtetega vastuolus.[56] Laeva ehituseks andis loa Suurbritannia mereväe ohvitser, kelle tegevuse eest vastutas Suurbritannia.

1.3.2 Riigivõimu teostamiseks volitatud organid

Riigivastutuse eelnõu artikkel 5 kohaselt on riik vastutav ka selliste füüsiliste ja juriidiliste isikute käitumise eest, kes ei kuulu riigiorgani töötajate hulka või ei ole ise riigiorgan, kuid kes on seaduse alusel volitatud teostama avaliku võimu funktsioone. Artikkel 5 olulisus on kasvanud, kuna nüüdisaegne riik annab üha rohkem valitusele pandud avalike ülesandeid edasi eraõiguslikele isikutele, mille tulemuseks on riigi osalusega üksuste märgatav kasv.[57] Sellest lähtuvalt on ka artikli eesmärk takistada olukorda, kus riikidel on võimalik vabaneda vastutusest läbi avalikke ülesannete delegeerimise. Lisaks on artikkel 5 eesmärk käsitleda erastatud korporatsioonide olukorda, mis säilitavad teatavad avalikud või reguleerivad funktsioonid nagu eraõiguslikud turvateenistust pakkuvad ettevõtted, kes on volitatud tegutsema vangivalvuritena või kus eraõiguslikud või riigi omandis olevad lennuettevõtjad teostavad teatavat sisserände kontrolli.[58]

Milline tegevus kvalifitseerub „riigivõimu“ elemendiks, sõltub konkreetse ühiskonna korraldusest, selle ajaloost ning traditsioonidest. Lisaks tuleb uurida, kas konkreetse tegevuse näol on tegemist

[56] Kohtuotsus, R.I.A.A 08.05.1872. Alabama arbitration (Suurbritannia v Ameerika Ühendriigid). Reports of International Arbitral awards. Volume XXIX.
[57] Crawford (2013), *supra nota* 36, lk 127.
[58] M.N. Shaw (2008) *International law. Sixth Edition.* Cambridge: Cambridge Univesity Press. 787-788.

riigi poolt antud volituste teostamisega või saab seda tegevust teha igaüks, ilma riikliku volituseta. Sellegipoolest võib tuvastada mõne keskse juhtumi riigivõimu teostamisest, kus eraettevõtteid on volitatud täitma avalikke ülesandeid. Nende hulka kuuluvad volitused isikuid kinni pidada ning määrata distsiplinaarkaristusi ning volitused sisserände kontrollimiseks ja vara arestimiseks. Artikli 5 seotud küsimused võivad tekkida ka juhul, kui riigi organ või agent antakse muu rahvusvahelises õiguses eksisteeriva juriidilise üksuse käsutusse olukorras, kus nii loovutav riik kui muu üksus teostavad asjassepuutuva organi või agendi suhtes kontrollielemente. Antud olukorda ilmestab kõige selgemalt, kui rahuvalvemissiooni läbiviimiseks antakse ÜRO käsutusse teise riigi sõjaväeüksus. Eelmainitud juhul rakendub üksusele nii loovutava riigi kui ka ÜRO jurisdiktsioon. Sarnane olukord leidis aset kohtuasjas *Behrami v France*[59], kus kohus seisis silmitsi küsimusega, kas NATO liikmesriigi sõjaväeükssused, mis moodustasid osa KFOR-ist (Kosovo Force) ja tegutsesid vastavalt ÜRO resolutsioon 1244 järgi, langevad Euroopa Kohtu jurisdiktsiooni alasse. Juhul kui üksuste eest vastutab ÜRO, ei kuulu KFOR Euroopa Kohtu jurisdiktsiooni alasse. Kohtu leidis, et eelneva küsimuse lahendamiseks tuleb analüüsida, kas ÜRO julgeolekunõukogu omas kontrolli KFOR'i üle ning kas rünnaku käsk tulenes resolutsiooni 1244 alusel ÜRO Julgeolekunõukogult. Viimasel ajal on rahvusvahelise kogukonna tähelepanu keskendunud erasektori militaarettevõtele ja turvafirmadele nagu Blackwater ning DynCorp, kelle teenuseid Ameerika Ühendriigid on korduvalt kasutanud nii Afganistanis kui ka Iraagis. Täiendavaid näiteid saab tuua ka pangandussektorist, kus keskpangad, olles paljudel juhtude riigi valitsusest ja majanduspoliitikast eraldiseisvad, teostavad reguleerivat võimu.[60]

1.3.3 Teise riigi käsutusse antud riigiorganid

Riigivastutuse eelnõu artikkel 6 käsitleb riigiorganeid, mis on antud teise riigi käsutusse. Artikkel 6 kohaselt, kui üks riik annab organid teise riigi käsutusse, siis vastutab organi saanud riik ka tema käitumise eest. Sellele lisandub eeldus, mille kohaselt peavad nimetatud organid täitma kasusaaja riigi avaliku võimu funktsioone. Termin „käsutusse andmine" väljendab endas olulisi tingimusi, mis peavad olema täidetud, et organi käitumine oleks omistatav vastuvõtvale riigile. Esiteks peab riigiorgani käsutusse andmine toimuma vastuvõtva riigi nõusolekul. Teiseks peab riigiorganit loovutav riik andma täielikult üle kontrolli teostamise ja korralduste andmise õiguse.[61]

[59] Behrami and Behrami v. France and Saramati v. France, Germany and Norway. ECHR 02.05 2017, lk 4-5.
[60] Crawford (2013), *supra nota* 36, lk 128
[61] Crawford (2013), *supra nota* 45, lk 113.

Kohtuasi *Chevrau* puudutas Suurbritannia aukonsulit Iraanis, kes, tegutsedes ajutise diplomaadina Prantsuse aukonsulaadis Teheranis, kaotas talle usaldatud dokumendid. Kohtunik Beichmann leidis, et Suurbritannia valitsust ei saa pidada vastutavaks oma konsuli hooletuses, kuna kokkulepitud tingimused, mille alusel Briti aukonsul tegutses, ei sisaldanud ühtegi sätet selle kohta, et tema teo eest vastutaks Suurbritannia.[62] Kohtuasjas *X and Y v Switzerland* leidis Euroopa Inimõiguste Kohus, et Liechtensteinis tegutsenud Šveitsi politseinikute eest vastutab Šveits, olenemata Liechtensteini valitsuse heakskiidust, kuna politseinikud teostasid ja tegutsesid Šveitsi seaduste alusel.[63] Aritkli 6 kohaldamiseks on lisaks kaks täiendavat nõuet. Esiteks peab käsutusse andev üksus vastama artiklis 4 toodud riigiorgani definitsioonile ning teisena peab kõnealune üksus teostama kasusaaja riigi riigivõimu.

1.3.4 Võimuvolitusi ületav või juhistele mittevastav käitumine

Siseriiklikus õiguses on pikka aega leidnud kinnitust tõdemus, et riigiorgani *ultra vires* tegevus ei välista selle organi vastutust. Rahvusvaheline kohtupraktika ja enamus õigusteadlasi on seisukohal, et riigil tekib vastutus enda organite tegevuse eest, kes ületavad neile antud kompetentsi (*ulra vires*).[64] Tavaõiguse kohaselt tekib riigivastuts ka juhul, kui riigiorganiks on teise riigi poolt laenatud üksus. Antud põhimõte on kodifitseeritud riigivastutuse eelnõu artiklisse 7.[65]

Riigivastutuse eelnõu artikkel 7 kohaselt vastutab riik riigiorganite ning avaliku võimu täitvate isikute käitumise eest ka siis, kui viimased ületavad oma võimupiire või lähevad vastuollu nendele antud juhistega. Riigi vastutus enda organite tegude eest on piiramatu, senimaani kuni organ käitus asjaomases olukorras ametlikus rollis. Seega ainuüksi volituste ületamine ei vabasta riiki vastutusest. Samuti ei välista riigi vastutust riigi poolne korraldus järgida asjakohaseid reegleid või õigusakte.[66]

Samas ei vastuta riik iga isiku käitumise eest, vaid ainult nendel juhtudel, kus isik tegutseb riigi nimel või annab seda mõista. Artikkel 7 kontekstis seisneb raskus riigi organi tegevuse, ehkki *ultra vires*, teo eristamine puhtalt eraviisilisest teost. Kõige paremini aitab antud asjas selgust luua

[62] Kohtuotsus. R.I.I.A 1931. Chevreau (Prantsusmaa v Suurbritannia), 2 RIIA 1113.
[63] X and Y v Switzerland. 20 ECHR 1977, p. 402, 402-6.
[64] Brownlee, I. (2003). *Principles of Public International Law. Sixth Edition*. New York: Oxford University Press, 435.
[65] Land, K. (2002). Rahvusvaheline vastutus. Rahvusvaheline õigus. Tallinn: Juura, 184.
[66] Värk (2005), *supra nota* 45, lk 113.

Prantsusmaa-Mehhiko komisjoni otsus kohtuasjas *Caire*. Caire, kes oli prantsuse kodanik, pidas Põhja-Mehhikos pansionaati. Pansionaadi üheks kliendiks oli linna okupeerinud sõjaväe ohvitser. Ohvitser, koos kahe sõduriga ähvardasid Caire ära tappa, kui viimane ei anna neile raha. Caire keeldumise järel viidi ta sõjaväe linnakusse, kus ta lasti maha. Komisjon leidis, et hoolimata sellest, et sõjaväe ohvitserid tegutsesid eraviisilistest motiividest lähtuvalt ning ületasid sellega neile antud volituse piire, on Mehhiko riik vastutav, kuna ohvitserid tegutsesid ametlikus rollis ning kasutasid selle staatuse tõttu neile käsutuses olevaid vahendeid.[67] Mehhiko riigivastutuse tekkimise oluliseks tingimuseks olid asjaolud, et ohvitserid kandsid sõjaväe vormiriietust ning viisid hukkamise läbi sõjaväe kasarmutes, välistades sellega puhtalt eraviisilise tegutsemise. [68]

1.3.5 Riigiväliste organite tegevuse omistamine

Riigivastutuse printsiibi üldpõhimõtte kohaselt ei omistata eraisikute ja eraõiguslike juriidiliste isikute poolt toime pandud tegusid riigile. Kuid teatud olukordades on võimalik riigi vastutust rakendada ka riigi väliste organite tegevuse korral. Riigi vastutuse eelnõu artikli 8 kohaselt tekib riigil vastutus ka eraisikute või eraisikute grupi poolt toimepandud tegude suhtes, kui need teod on toime pandud riigilt juhiseid või suuniseid saades või riigi kontrolli all. Eraisikuid või eraisikute gruppe saab seeläbi mõista kui riigi käepikendust, mille abil soovituid tulemusi ellu viiakse.[69]

Artikkel 8 rakendusala on võimalik jagada kaheks. Esimene tegeleb olukorraga, kus eraisikud tegutsevad riigi poolt antud juhiste alusel ning teine üldisema olukorraga, kus eraisikud alluvad riigi kontrollile või suunistele. Vastutuse tekkimiseks piisab, kui esineb üks eelmainitud olukoradest. Oluline on aga silmas pidada, et mõlemal juhul tuleb võtta arvesse tegeliku seose olemasolu teo toime pannud isiku ja riigi vahel. Kõige sagedamini tekivad sellised juhtumid olukorras, kus riik palkab või õhutab eraisikuid või eraisikute gruppe osalema tegevuses, mis teenib riigi huve, jättes nad riigi ametlikust struktuurist välja. Näiteks võib riik anda vabatahtlikele isikutele konkreetsed juhised tegutsemiseks väljaspool riigi piire, kuid saadetud üksused ei kuulu ametlikult politsei või relvajõudude hulka. Keerulisem on olukord, kus eraisikute tegevus toimus riigi suunitlustel või kontrolli all. Riigi vastutus saab sellisel juhul tekkida ainult siis, kui riik juhtis või kontrollis konkreetset tegevust, mis oli õigusvastase teo oluline eeldus.

[67] Kohtuotsus, R.I.A.A. 1929. Jean-Baptiste Caire Claim (Prantsusmaa v Mehhiko). 5 R.I.A.A 516.
[68] Crawford (2013), *supra nota* 36, lk 137.
[69] United Nations (2008), *supra nota* 9, lk 47.

Riigivastutuse eelõnu artikkel 8 sätestab millal tekib riigi vastutus, kuid jätab täpsustamata, millise tegevuse korral on riik rakendanud üksuse üle piisavalt kontrolli või andnud juhiseid, et tegevus oleks riigile omistatav. Rahvusvaheline kohus on loonud läbi kohtupraktika kaks kontrollistandardit, mis on abiks vastutuse omistamisel ja mida autor tutvustab järgmises alapeatükis.

1.3.6 Efektiivne kontroll

Efektiivse kontrolli testi kasutati kohtu poolt esmakordselt kohtuasjas *Nicaragua vs Usa*, mis on olnud juhtivaks lahendiks eraisikute või isikute grupi poolt toime pandud tegevuse omistamisel riigile. *Nicaragua vs USA*[70] kohtuasja eellugu on seotud Ameerika Ühendriikide ja Nicaraguas tegutsenud paramilitaarse rühmituse – contrate, omavahelise seosega. Nimelt oli kohtuasja keskseks küsimuseks, kas Ameerika Ühendriikidel lasub vastutus contrate poolt toime pandud rahvusvahelise humanitaarõiguse rikkumise eest. 1986. aastal käsitles rahvusvaheline kohus just selle kohtuasja kestel esimest korda efektiivse kontrolli printsiipi. Nimetatud kaasust on läbi rahvusvahelise õiguse ajaloo kasutatud korduvalt olukordades, kus keskseks küsimuseks on riigivastutuse omistamine, seda just seetõttu, et lahend on andnud vastuseid paljudele rahvusvahelises õiguses esile kerkinud probleemidele.[71]

Tulles tagasi lahendi sisulise osa juurde, leidis kohus, et kõik ajavahemikus 1981 kuni september 1984 aset leidnud sündmused, mis olid toime pandud contrate poolt Nicaraguas ja Nicaragua vastu (nii militaarsed kui ka paramilitaarsed), olid saanud rahastuse Ameerika Ühendriikide poolt. Ent hoolimata asjaolust, et Ameerika Ühendriigid olid contrate tegevust nii rahastanud, kui ka organiseerinud rühmituse tegevust, treenimist ja panustanud olulisel määral contrate relvastusse, ei olnud kohtul piisavalt tõendusmaterjale vastutuse omistamiseks. Eelnimetatu põhjal saaks justkui põhjendada USA poolset ilmselget contratega tegevuste juhtimist, kuid samas ei saa väita, et contrad ei oleks suutnud iseseisvalt nimetatud rahvusvahelise humanitaarõiguse vastaseid tegusid toime panna. Selleks, et omistada vastutus contrate poolt toime pandud kuritegude eest USA-le oleks kohtul olnud vaja tõestada, et USA-le oli contrate tegevuse üle efektiivne kontroll. Kohus selgitas lahendis, et pelk asjaolu, et USA toetas contrate tegevust ülalmainitud viisil, ei tähenda, seda, et USA-l oli täielik kontroll kõikide tegevuste üle, mis contrad toime panid. Kohtu

[70] Kohtuotsus, ICJ. 27.06.1986. the case concerning Military and Paramilitary Activities in and against Nicaragua brought by Nicaragua against the United States of America, I.C.J. 39.
[71] Hoss,C., Villalpando, V., Sivakumaran, S. (2012). Nicaragua: 25 years Later. *Leiden Journal of International Law*, 132-133.

seisukohalt tuleks eelmainitust aru saada selliselt, et contrad ei vabane vastutusest seoses toime pandud tegudega ja USA on vastutav iseenda käitumise eest Nicaraguas seoses contrate tegevusega. See, mida kohus pidi uurima, oli otsene seotus Ameerika Ühendriikide ja contrate poolt toime pandud tegude vahel.[72] Lahendis on välja toodud, et USA poolne contrate rahaline toetus on otseselt seotud USA finantsaasta lõppemisega ja rahaülejäägi suunamisega humanitaarprojektidesse. Kuigi kohus võttis seisukoha, et humanitaarabi andmine on kooskõlas rahvusvahelise õigusega, peavad humanitaarabi andmisel kohalduma Punase Risti põhimõtted (vähendada inimeste kannatamist ja kaitsta inimelu, olenemata isikutele omistavatest tunnustest religiooni, rassi jm alusel). Kohus võttis seisukoha, et antud kohtuasjas on viidatud humanitaarabi andmisele vaid eesmärgiga hoiduda kõrvale Nicaragua siseasjadesse sekkumisega seotud võimalikust hukkamõistmisest. [73] Lisaks ülalmainitud contrate juhendamisele ja miinide asetamisega Nicaragua vetesse, kirjeldavad kohtule esitatud materjalid, et 1983. aastal said contrad CIA poolt partisanisõja käsiraamatu, milles kutsuti üles toime panema rahvusvahelise õiguse vastaseid tegusid (tapmised, ametnike neutraliseerimised, vägistamised jne). Kuigi USA väitis, et tegu ei olnud tahtlikult suunatud Nicaraguas toime pandud tegude õhutamiseks, ei olnud kohus sellega nõus, selgitades, et raamatu avaldajad pidid olemas teadlikud Nicaraguas toimuvast, ja luges käsiraamatu rahvusvahelistes lepingutes sätestatud humanitaarõiguse põhimõtetega vastuolus olevaks. [74] Kohus võttis lahendis kokku, et eelmainitud käsiraamatu levitamisega ja Nicaragua vetesse miinide asetamisega on USA läinud vastuollu rahvusvahelise õigusega, kuid sellest hoolimata ei saa USA-le omistada contrate poolt toime pandud tegevuste osas vastutust, kuna tõendamist ei leidnud otseste juhiste andmine konkreetsete tegude toimepanemiseks ehk USA ei omanud iga contrate poolt toime pandud teo üle efektiivset kontrolli. [75]

[72] Kohtuotsus, ICJ. 27.06.1986. the case concerning Military and Paramilitary Activities in and against Nicaragua brought by Nicaragua against the United States of America, I.C.J. 39.
[73] *Ibid.,* p 242, 243, 254.
[74] *Ibid.,* p 117, 122.
[75] *Ibid.,* p 115.

1.3.7 Üleüldine kontroll

1999. aastal pandi eelmainitud efektiivse kontrolli test küsimärgi alla, kui Jugoslaavia rahvusvahelise kriminaaltribunali ette tuli lahendamiseks Dusko Tadići kohtuasi. Kohtualusele Tadićile pandi süüks nii sõjakuriteo kui ka inimsusevastase kuriteo toimepanemine, kuna Tadić osales inteneerimislaagri valvurina 14 000 inimese hukkamisel.

Kuigi Jugoslaavia rahvusvahelise kriminaaltribunali tuvastamispädevusse ei kuulu tegude omistatavus riikidele, tuli siiski välja selgitada, kas Tadići teod on omistatavad Serbiale, ehk kas teod, milles Tadićit süüdistati, olid toime pandud rahvusvahelise või mitte rahvusvahelise relvakonflikti raames. Antud kohtuasja raames vaatas kohus uuesti üle Nicaragua asjas välja töötatud efektiivse kontrolli testi ja tegi vajalikud muudatused, mille tulemusena kujunes välja „üleüledise kontrolli“ printsiip. Enam ei arvanud kohus, et riigil ei pea olema rühmituse või isiku tegude üle efektiivset kontrolli, ehk riik ei pea andma konkreetseid juhiseid, et omada kontrolli isiku üle, vaid piisab nn üleüldisest kontrollist. [76]

Kohus laiendas efektiivse kontrolli testi, võttes seisukoha, et riigile saab omistada vastutust, ka sellisel juhul, kui riik tunnustab rikkumist avalikult. Kahe nimetatud testi erinevus seisneb kontrolli ulatuses, mida riik omab toime pandud teo üle. Heaks näiteks üleüldise kontrolli rakendumiseks on nt. mitte-organiseeritud grupeeringud, millel on üldjuhul hierarhiline struktuur ja mille osas eeldatakse üleüldise kontrolli printsiipi kasutades, et kui riigil on kontroll selle organisatsiooni nn. juhi üle, on riigil hierarhilisest struktuurist tulenevalt automaatselt kontroll ka terve organisatsiooni üle. Sellega lükkas kohus kõrvale range kriteeriumi, mis toob endaga kaasa suure tõendamiskoormuse konkreetsete juhiste andmiseks. Teoreetikud on arvamusel, et „üleüldise kontrolli“ test ei ole sobilik, et tuvastada riigivastutust, vaid selleks on ja jääb efektiivse kontrolli test. [77]

[76] Kohtuotsus. ICTY Appeals Chamber, 15.07.1999, Prosecutor v. Duško Tadic. No. IT-94-1-A.
[77] Tonkin, H. 2011. State Control over Private Military and Security Companies in Armed Conflict. New York, Cambridge University Press, 118.

2. KAHJU HÜVITAMISE TEOORIA

Juba varajases ajaloos maksid sõja kaotanud pool võitjatele hüvitist. Aja jooksul muutus taoline käitumine tavaks, mille kohaselt oli sõja kaotanud pool kohustatud võitja riigile hüvitama sõjapidamise kulud.[78] Teise maailmasõja järel kujunenud reparatsioonide režiim on teravaks kontrastiks pärast I maailmasõda loodud reparatsioonidele.[79] Reparatsioon vahetas mõistena välja I Maailmasõja järgselt kasutatud mõiste „sõjakahju", mis kujutas lüüa saanud riikide kohustust maksta kogu kahju, mis konflikti tulemusel oli tekkinud. Viimaste sõjaliste konfliktidega on „sõjakahju" mõiste asendunud reparatsioonidega rahvusvahelise õigusvastase teo eest. Iraagi-Kuveidi sõja ajal võttis ÜRO Julgeolekunõukogu vastu mitmeid resolutsioone Kuweidi okupeerimise kohta, keskendudes Iraagi sissetungi ja okupatsiooni ebaseaduslikkusele. Resolutsioonis 687 kinnitas ÜRO Julgeolekunõukogu, et Iraak oli rahvusvahelise õiguse kohaselt vastutav igasuguse otsese kahju eest, sealhulgas keskkonnakahjude ja loodusvarade kahanemise eest ning välisriikide valitsuste, kodanike ja ettevõttetele tekitatud kahju eest, mis tulnenes tema ebaseaduslikust käitumisest.[80]

Rahvusvahelise tavaõiguse kohaselt tekib rahvusvahelise õigusvastase teo toimepanemisel kohustus tekitatud kahju hüvitada. Antud põhimõte on sätestatud riigivastutuse eelnõu artiklis 31, sätestades üldreegli, mille kohaselt on vastutav riik õiguslikult ja automaatselt kohustatud hüvitama kahju, mis on tekkinud õigusvastase teo toimepanemisel. Põhimõtet mille kohaselt tekib riigil primaarse kohustuse rikkumisel sekundaarne kohustus tasuda reparatsioone tekkinud kahju eest, kinnitas Alaline Rahvusvaheline Kohus selgelt varasemalt mainitud kohtuasjas *Factory at Chazow*. *Factory at Chazow* kohtuasi hõlmas Poola riigi valduse kehtestamist tehasele, mis Saksamaa-Poola vahelise lepingu kohaselt pidi jääma Saksamaa valdusesse. Kohus märkis, et kahju hüvitamine primaarse kohustuse rikkumisega tekitatud kahju eest on rahvusvahelise õiguse printsiip. Kohus kasutas terminit „reparatsioonid" kõige üldisemas tähenduses. Kohus lükkas tagasi Poola argumendi, mille kohaselt puudub kohtul pädevus otsustamaks reparatsioonide vormi ja suuruse üle.[81] Sama kohtuasja hilisemas faasis jätkas kohus üksikasjalikumalt kahju hüvitamise

[78] Shelton, D. (2009). Reparations. *Max Planck Encyclopedia of Public International Law, Volume VIII. Max Planck Insitute for Comparative Public Law and International Law*. New York: Oxford University Press, 883-892.
[79] P.Argent. 2009. Reparations after World War II. *The Max Planck Encyclopedia of Public International Law, Volume VIII. Max Planc Institute for Comparative Public Law and International Law*. New York: Oxford University Press, 893-901.
[80] Shelton (2009), *supra nota,* lk 884.
[81] Kohtuotsus, PCIJ. 26.07.1927, Factory at Chorzow, (Saksamaa v Poola). (ser. A), No. 9

kohustuse sisu täpsustamisega. Kohus kirjeldas, et võttes aluseks rahvusvaheliste tribunalide otsused ja kehtiva rahvusvahelise õiguse praktika, peavad reparatsioonid võimaluse korral kõrvaldama kõik õigusvastase teo tagajärjed ja taastama olukorra, mis oleks tõenäoliselt eksisteerinud, kui rahvusvahelist õigusvastast tegu ei oleks toime pandud.[82] Kahju hüvitamise kohustust taastada *status quo ante* on leidnud kinnitust mitmetes rahvusvahelistes kohtutes ja tribunalides.[83] Kahju hüvitamise eesmärk on esmajärjekorras olukorra taastamine, mis oleks valitsenud, kui ei oleks toimunud rahvusvahelise kohustuse rikkumist. Seega on kahju hüvitamine suunatud primaarsete kohustuste täieliku täitmise tagamisele ja rikkumise tagajärjel tekkinud kahju kompenseerimiseks. Kahju hüvitamise teooria kohaselt peaks võimaluse korral alustama kõige leebemast vahendist, millest piisaks olukorra taastamiseks.[84]

Kahju hüvitamise kohustus on primaarsest kohustusest eraldiseisev ning ei oma tähtsust kas primaarse kohustuse allikas tuleneb lepingust või rahvusvahelisest tavaõigusest. Antud põhimõtet selgitas Alaline Rahvusvaheline kohus kohtuasjas *Gabcikoco-Nagymaros*.[85] Kohus selgitas, et poolte vaheline leping jäi jõusse olenemata mõlema poole jätkuvast rikkumisest. Kuigi riigid võivad nõustuda, et mõned lepingud lõppevad lepingusätete rikkumise korral, on see küsimus reguleeritud asjakohase primaarse kohustusega, millele riigivastutuse sätted ei kohaldu.[86]

2.1 Mõiste „kahju“

Riigivastutuse eelnõu artikkel 31 sätestab üldreegli, mille kohaselt on vastutav riik õiguslikult ja automaatselt kohustatud hüvitama kahju, sealhulgas mis tahes materiaalse või moraalse kahju, mille on põhjustanud õigusvastane tegu. Mõiste „kahju“ tähendab igasugust kahju, mille on põhjustanud õigusvastane tegu, hõlmates mis tahes tekkinud materiaalset või moraalset kahju, kuid välistades igasuguse abstraktse kahju, millel ei ole kindlat alust.[87]

Materiaalse kahju all mõeldakse kahju riigi või tema kodanike varale või muudele hüvedele, mis on rahaliselt hinnatav. Moraalne kahju hõlmab endas individuaalseid valu ja kannatusi, lähedaste

[82] Stern. (2010). The obligation to make reparation. *The law of International responsibility. Oxford commentaries on International law*. New York: Oxford university press, 564-571.
[83] Crawford (2013), *supra nota* 36, lk 481.
[84] *Ibid.*, lk 886.
[85] Kohtuotsus, PCIJ. 1930.Greco-Bulgarian “Communities“. Advisory Opinion. Series B, No. 17.
[86] D.Shelton (2009), *supra nota,* lk 885.
[87] United Nations (2008), supra nota 9, lk 91.

surma või isiklike rünnakuid, mis on seotud eraelu- ja kodu puutumatusega. Asjaolu, et reaalne kahju ei ole vajalik vastutuse tekkimiseks on autor analüüsinud eelnevates peatükkides. Artikkel 31 kohaselt puudub üldine nõue, mis sätestaks, et riik peab kandma olulist kahju, enne kui ta võib taotleda reparatsioone. Seega saab kahjuks lugeda ka nö „õigusliku kahju", mis tekib pelgalt rahvusvahelise kohustuse rikkumisest. Tegeliku kahju olemasolu, kas materiaalse või moraalse kahjuna, on oluline reparatsioonide vormi ja ulatuse valimisel. Kohtuasjas *Rainbow Warrior*[88] märkis kohus, et õigusvastane käitumine mittemateriaalsete huvide vastu, nagu riigi au, väärikuse ja prestiiši mõjutavad tegevused, annavad ohverriigile õiguse nõuda reparatsioone, isegi kui need tegevused ei ole toonud kaasa rahaliselt mõõdetavad kahju.[89] Seega puudub üldine nõue kahju esinemiseks. Mõistet „kahju" tuleb analüüsida eelkõige primaarsest kohustusest lähtuvalt. Arvestades primaarset kohustust võib „kahju" esineda reaalses materiaalses kahjus teisele riigile, kuid mõnel juhul tekib riigivastutus riigi poolse tegevusetusega, olenemata, et reaalset materiaalset või moraalset kahju ei teki. Seega määravad primaarsed kohustused kindlaks selle eelduse, mis on oluline vastutuse tekkimiseks.[90]

2.2 Põhjuslik seos

Riigivastutuse eelnõu artikkel 31 teises lõigus käsitletakse põhjuslikku seose küsimust rahvusvahelise õigusvastase teo ja kahju vahel. Nimelt sätestab artikkel, et riigilt saab kahju hüvitamist nõuda ainult teo eest, mis on õigusvastane ja põhjuslikkuses seoses tekkinud kahjuga, välistades muude tekkinud kahjude hüvitamise kohustust.[91] Põhjusliku seose nõue ei ole aga alati rahvusvahelise kohustuse rikkumise korral ühesugune.

Põhjusliku seose analüüsimisel ei piisa ainult teo faktiliste asjaolude uurimisest, vaid arvesse tuleb võtta, kas kahju tekkimine oli vahetu ning kas kannatajariigil oli võimalus võtta meetmeid kahju ära hoidmiseks või kahju vähendamiseks. Kuigi riigivastutuse eelnõu redaktsioonikomitee selgitas, et põhjusliku seose tingimused on sätestatud primaarseid kohustusi loovas rahvusvahelises lepingus, oli põhjusliku seose täpsustamata jätmise põhjuseks eelkõige asjaolu, et komisjon ei suutnud luua ühtset reeglistiku, mida saaks rakendada kõikidele võimalikele

[88] Rainbow Warrior (1990), supra nota 23.
[89] United Nations (2008), *supra nota* 9, lk 91.
[90] *Ibid*, lk 92.
[91] *Ibid*, lk 92.

rikkumistele. Redaktsioonikomitee tõdes, et oli kaalunud mitmeid soovitusi kõnealuse põhjusliku seose tingimuste kvalifitseerimiseks, kuid loobus sellest põhjusel, et igat rikkumist tuleb analüüsida eraldi ning üldiste normide kohaldamine raskendaks asja lahendamist.[92] Seega leiab kohtupraktikast mitmeid erinevaid termineid mille kaudu on kohus hinnanud põhjusliku seose olemasolu. Ka põhjusliku seose tuvastamine ei ole alati piisav tingimus kahju hüvitamiseks ning uurimise all võib olla ka küsimus kas teo tagajärjed olid liiga „kauged" et õigustada reparatsioone. Kohtud on siinkohal kasutanud termineid „otsesus", „prognoositavus" ning „vahetu".[93] Samuti tuleb arvesse võtta teisi tegureid, näiteks kas riigiasutused on tekitanud tahtlikult kahju või kas tekitatud kahju oli piisav.[94]

Kohtuasjas *Adminitrative Decision No.II* leidis Portugali-Saksamaa vahekohus, et põhjusliku seose hindamisel on kahju „otsesusest" olulisem kahju ettenähtavus või tema vahetu mõju seoses õigusvastase teoga. Kohus märkis, et vahetu põhjus kahju esinemiseks pidi olema Saksamaa kohustuse rikkumine ning selle rikkumise vahetu tagajärg peab olema kahju, mille hüvitamist nõutakse. Kohus jätkas, et ei ole oluline, kas kahju on tekkinud otseselt või kaudselt, kuniks esineb selge ja katkematu sündmuste ahel Saksamaa õigusvastase teo ja kahju vahel. Samuti ei ole oluline, kui palju erinevaid elemente sündmusteahelas on, vaid oluline on, et sündmusteahelas ei esineks pause ning kahju saab selgelt, eksimatult ja kindlalt omistada rikkujale.[95]

Kohtuasjas *Ethiopia's Damages Claim* võttis kohus eesmärgiks anda konkreetsemad tingimused, tuvastamaks põhjusliku seost. Kohus märkis, et põhjuslikku seost saab kõige paremini analüüsida läbi tema „vahetu" omaduse. Hinnates, kas antud tegu oli vahetu või mitte, ning kas teo ja tagajärje vahel on piisavalt tugev põhjuslik seos, kaalus komisjon lisaks, kas konkreetne kahju oleks pidanud olema mõistlikult ettenähtav rahvusvahelise õigusvastase teo toime pannud riigile. Kahju prognoositavus võimaldab hinnata paremini, kas tekkinud kahju oli vahetu või mitte. Sellest tulenevalt omab kahju tekkimise vahetus olulist mõju hindamaks, kas kahju kuulub hüvitamisele.[96]

[92] Crawford (2013), *supra nota* 36, lk 493.
[93] Kohtuotsus. R.I.I.A. 31.07.1928. Portuguese Colonies case (Naulilaa incident), 2 RIIA 1011.p.1025–1026.
[94] Kohtuotsus. Iraan-Ameriika Ühendriikide Arbitraaži Tribunal. 28.12.1998 in The Islamic Republic of Iran v. The United States of America cases A15 (IV) and A24. No. 590–A15 (IV)/A24–FT.
[95] Cheng, B. (1993). General Principles of law as applied by International Courts and Tribunals. New York: Cambridge University Press, 241-253.
[96] Kohtuotsus, R.I.A.A. 2009. Ethiopia's Damages Claim (Eritrea vs Etioopia). No. 2001-02.

Vahetu mõju printsiipi põhjusliku seose leidmisel on kohtud nimetanud ka terminiga „tavapärane kahju“. Kohtuasjas *Antippa* märkis kohus, et vastavalt rahvusvahelises õiguses tunnustatud põhimõtetele kuulub makstava hüvitise hulka kogu kahju, mida võib pidada kahju põhjustanud tegevuse tavapäraseks tagajärjeks.[97] Lisaks taolisele objektiivsele tingimusele saab kahju hüvitamisel hinnata ka poolte subjektiivseid asjaolusid, nagu kahju ettenägevus ning kavatsus. Ettenägevuse hindamisel saab arvestada ainult asjaolusid mida rikkuja oleks pidanud ja oleks saanud ettenäha.[98]

Veel üks reparatsioonide ulatust mõjutav element on kahju leevendamise küsimus. Õigusvastase teo ohvrilt eeldatakse kahju tekkimisel mõistliku käitumist. Kuigi tihtipeale väljendatakse antud tegevust kui kohustust leevendada kahju, ei ole tegemist juriidilise kohustusega, mille rikkumine omakorda tekitaks vastutuse. Riigivastutuse eelnõu kommentaarid selgitavad, et kahju mis oli kannataja riigil võimalik ära hoida, ei kuulu reparatsioonide korras tagasinõudmisele. Antud seisukohta on kohus kinnitanud ka kohtuasjas *Gabcikovo-Nagymaros.*[99] Seega kahju, mis tekib kannatajariigi endapoolse kohustuse rikkumise puhul ei ole põhjustatud rikkuja riigi poolsest ebaõigest käitumisest.[100]

Riigivastutuse eelnõu artikkel 34 näeb ette kolm kahju hüvitamise vormi: ennistamine, varalise ning mittevaralise kahju hüvitamine. Kahju hüvitamise eesmärk on täielikult kõrvaldada õigusvastase teo tagajärjel tekkinud kahju, kas ühe või mitme kahju hüvitamise vormi koosmõjus. Nii traditsiooniline käsitlus riigivastutusest kui ka tänapäevane lähenemisviis näevad õigusvastase tegevuse peatamist, kui üht reparatsiooni viisi. Riigi vastutuse eelnõu ei käsitle primaarse kohustuse rikkumist kahju hüvitamise vormina vaid riigi sisemise kohustusena. Antud küsimus on lahendatud riigivastutuse eelnõu artikkel 29-ga, mis sätestab, et rahvusvahelise õiguse vastasest teost tingitud tagajärgedest hoolimata on vastutaval riigil jätkuv kohustus primaarsest kohustusest kinni pidada. Artikkel 30 täiendab eelmainitud ning lisab, et kui õigusvastane tegu jätkub, peab vastutav riik selle lõpetama ja kui asjaolud seda nõuavad, pakkuma asjakohaseid tagatisi ja garantiisi rikkumise ärahoidmiseks.[101] Seega esimene nõu, mis lasub rahvusvahelise õigusevastase teo toime pannud riigil, on rikkumise lõpetamine, olenemata kas kannatajariik seda ise taotleb.[102]

[97] Kohtuotsus. Kreeka-Saksamaa Arbitraaži Kohus. 1926. Antippa (The Spyros). No. 285.
[98] Cheng (1993), *supra nota* 86, lk 241-253.
[99] Kohtuotsus, ICJ. 1997.Gabcikovo-Nagymaros Project (Ungari v Slovakkia) I.C.J. 7.
[100] Crawford (2013), *supra nota* 36, lk 494.
[101] United Nations (2008), supra nota 9, lk 97.
[102] *Ibid*.

2.3 Õigusliku seisundi ennistamine

Kuigi kannatajariigil on õigus otsustada, millist kahju hüvitamise vormi ta eelistab, loetakse ennistamist esmaseks kahju hüvitamise vormiks, välja arvatud juhul, kui see on materiaalselt võimatu ning kui muude vormide kasutamine oleks vähem koormav.[103] Riigivastutuse eelnõu artikkel 35 sätestab, et rahvusvahelise õigusvastase teo eest vastutav riik on kohustatud ennistama õigusliku seisundi, st taastama olukord, mis oli olemas enne õigusvastase teo toimepanemist, tingimusel ja selles ulatuses, et ennistamine:

- ei ole materiaalselt võimatu;
- ei ole ebaproportsionaalne hüvitatava kahju ja soovitava tulemuse saavutamiseks.[104]

Artikli sõnastuse kohaselt tähendab ennistamine *status quo ante* olukorra taastamist, st olukorda, mis oli enne õigusvastase teo toimepanemist. Artiklis 35 on sätestatud ennistamise kitsam määratlus, mis seisneb faktiliste asjaolude hindamisel, jättes kõrvale hüpoteetilise uurimisie selle kohta, milline oleks olukord olnud, kui ei oleks toimunud õigusvastast tegu.[105] Tihti võib esineda olukordi, kus ennistamine ei ole võimalik või selle väärtus on nii vähene, et otsustatakse muude reparatsiooni vormide kasuks. Näiteks on ennistamine praktiliselt välistatud, kui rikkumise aluseks olev vara on praktiliselt hävinud või oluliselt muutunud. Olukorra ennistamine võib toimuda läbi territooriumi, isikute või vara tagastamise, samuti mõne juriidilise akti tühistamise või nende kombinatsioonide abil. Ennistamise näited hõlmavad kinnipeetavate vabastamist, arreteeritud isikute üleandmist, laevade tagastamist ning muu vara ja dokumentide tagastamist, sh kunstiteosed ja aktsiad. Kohtuasjas *Temple of Preah Vihear Case* nõudis Alaline Rahvusvaheline Kohus, et Tai Kuningriik tagastaks Preah Viheari templist õigusvastaselt võetud religioossed esemed Kambodžale.[106] Mõistet „õiguslik ennistamine“ kasutatakse ka siis, kui ennistamine hõlmab õigusliku olukorra muutmist vastutava riigi õigussüsteemis või selle õiguslikes suhetes kannatanud riigiga. Selliste juhtumite hulka kuuluvad näiteks olukorrad, kus siseriiklikul tasandil jõustunud õigusaktid on vastuolus rahvusvahelise lepinguga, välismaalase või tema vara suhtes ebaseaduslikud haldus- või kohtumeetmete rakendamisel või teatavate sammude võtmine rahvusvahelise lepingu lõpetamiseks. Seega artiklis 35 sätestatud ennistamisel on laiaulatuslik tähendus, hõlmates kõiki meetmeid, mida vastutav riik peab astuma rahvusvahelisest

[103] Crawford (2013), *supra nota* 36, lk 496.
[104] United Nations (2008), supra nota 9, lk 98.
[105] Crawford (2013), *supra nota* 36, lk 496.
[106] Kohtuotsus. ICJ. 1962. Temple of Preah Vihear Case (Kamboodža v Tai), ICGJ 160.

õigusvastasest tegevusest tuleneva olukorra taastamiseks. Mida kannatajariik ennistamisega taotleb sõltub suuresti primaarsest kohustusest ehk kohustava normi iseloomust. Ennistamine, mis on kahju hüvitamise vormidest esimene, on eriti oluline olukorras, kus kohustuse rikkumine on kestev ning rikutakse rahvusvahelise õiguse imperatiivset normi. Tuues näiteks riigi annekteerimise siis okupeerivate vägede tagasitõmbamine võib kujutada endas pigem rikkumise lõpetamist riigivastutuse artikkel 30 alusel, kui olukorra ennistamist artikkel 35 alusel.[107] Ka siis on kõrvalmeetmetena sissetungi käigus kinnipetud isikute ja vara tagastamine seotud olukorra ennistamisega artikkel 35 alusel.[108]

2.4 Varalise kahju hüvitamine

Nagu eelpool mainitult, võib ennistamine osutuda kahju hüvitamisel ebapiisavaks vormiks, et kõrvaldada täielikult tekkinud kahju. Kõige sagedamini kasutatav kahju hüvitamise vorm on varaline kahju hüvitamine. Riigivastutuse eelnõu artikkel 36 sätestab, et vastutaval riigil lasub kohustus maksta kahjutasu tekitatud kahjude eest, mida ei ole võimalik kõrvaldada ennistamisega. Kahjutasu hõlmab mis tahes rahaliselt hinnatavaid kahjusid, sealhulgas saamata jäänud kasumit.[109]

Varalise kahju hüvitamise eesmärk ei ole õigusvastase teo toimepannud riigi karistamine ega näitlikustamine, vaid tema eesmärgiks on rahvusvahelise süülise tegevuse tulemusena tekkinud tegelike kahjude kõrvaldamine. Varaline kahju hüvitamine vastab kannatanud riigi või selle kodanike rahalisele hinnangule, seega koosnedes üldiselt rahalisest maksetest. Erandina võivad pooled kokku leppida ka muus vääringus. Materiaalse kahju ulatus on piiratud väljendiga „mis tahes rahaliselt hinnatav kahju“. Rahaliselt hinnatav kahju hõlmab nii riigi enda (riigivarale või ametnikele tekitatud kahjustused) kui ka kodanikele tekitatud kahju, sealhulgas ettevõtetele tekitatud kahju mis kuuluvad riigi diplomaatilise kaitse alasse. Kahju hüvitamine ja selle ulatus sõltub rikutud kohustuse sisust, osapoolte käitumise hindamisest ning eesmärgist saavutada õiglane ja vastuvõetav tulemus. Riigile tekitatud kahju võib iseenesest tuleneda temale kuuluva õhusõiduki alla tulistamisest või laevade uputamisest, diplomaatiliste hoonete ja seal töötavate inimeste rünnakust, avaliku vara lõhkumisest, reostuskahjust või ettenägematutest kahjudest, mis tulenevad näiteks vajadusest maksta pensioni või tasuda ravikulusid, mis on tekkinud vigastades tööülesandeid täitnud ametnike.

[107] Kohtuotsus. P.C.I.J. 1933. Legal Status of Eastern Greenland case (Norra v Taani). Series A/B, No. 53.
[108] United Nations (2008), *supra nota* 9, lk 98.
[109] Kaczorowska, A. (2010) *Public International Law. The fourth editition*. London: Routledge, 483.

Kohtuasjas *Corfu Channel* taotles Suurbritannia kompensatsiooni Albaanialt kolme kulukomponendi eest: Kuningliku mereväe S-klassi hävitaja „Saumarez“ hävimisest, kahjustuste eest hävitajal „Volage“ ning personalile tekkinud vigastuste eest. Kohus tugines kahju suuruse kindlaks tegemisel ekspertarvamustele ning leidis, et seoses hävitaja „Saumarez“ hävinguga, on "tegelik hüvitise suurus" võrdeline hävitaja asendamise maksumusega selle kaotamise aja seisuga ja leidis, et Suurbritannia valitsuse poolt nõutud hüvitise suurus (700 087 naelsterlingit) oli põhjendatud. Alusele „Volage“ tekitatud kahju hindasid eksperdid mõnevõrra väiksemale summale kui 93 tuhat naelsterlingit, mida Suurbritannia nõudis, võttes suuruse hindamisel aluseks tööde ja seadmete maksumuse. Lisaks hävitajatele tekitatud kahjule, rahuldas kohus ka Suubritannia taotluse 50 508 naelsterlingi osas, mis oli seotud kulutustega, mis tulenesid viga saanud laeva meeskonna pensionide, halduskulude ja ravikulude tõttu.[110] Paljudel juhtudel, kus õigusvastase teo tagajärjel on tekkinud ulatusliku kahju laevale või lennukile ja selle meeskonnale, on riigid pidanud kompensatsiooni suuruse üle läbirääkimisi otse. Heaks näiteks taolise praktika koha võib pidada *Aerial Incident of 3 July 1988,* kus Ameerika Ühendriikide tegevuse tulemusel hävis Iraani reisilennuk koos 290 pardal olnud reisjaga.[111]

Järgmine olukord, kus riigil võib tekkida õigus varalise kahju hüvitamiseks on keskkonnareostus ja selle tagajärjel tekkinud kahju. 1978 jaanuaris kukkus Nõukogude Liidu sateliit nr 954 orbiidilt Kanada riigi territooriumile. Kanada taotles tekkinud kulutuste hüvitamist, mis olid seotud sateliidi asukoha kindlakstegemisega, selle eemaldamisega ning asukoha koristamisega radioaktiivsetest jäätmetest. Pooled jõudsid kokkuleppele, mille kohaselt maksis Nõukogude Liit Kanadale kahjutasu 3 miljoni dollari ulatuses.[112] Juhtudel, kus õigusvastase teo tagajärjel on tekkinud keskkonnakahju, on varalise kahju hüvitamist taotletud reostuse vältimise, kõrvaldamise ning keskkonna kahju vähendamise kulutuste hüvitamiseks. Samuti rikutud maa ja vara hüvitamiseks. Keskkonnaväärtuste nagu bioloogiline mitmekesisus kahjustamine on kompenseeritav samalaadselt kui iga muu vara puhul, olenemata võimalikest raskustest selle mõõtmisel.[113]

Artikkel 36 lõike 2 kohaselt kuulub hüvitamisele ka saamata jäänud tulu. Artikkel 36 eristab kolme erinevat tulu: tulu, mille laekumist sai eeldada enne kohtuotsust, seejärel tulu, mille laekumist saab

[110] Kohtuotsus, ICJ. 1949. Corfu Channel (Suurbritannia v. Albaania), GL No 1, ICJ Rep 4, ICGJ 199.
[111] Kohtuotsus. ICJ . 1996. Aerial Incident of 3 July 1988 (Iraan v. Ameerika Ühendriigid), No. 674.
[112] Cosmos 954 Soviet nuclear-powered satellite over its territory in 1978, ILM, vol. 18 (1979), p. 907.
[113] United Nations (2008), *supra nota* 9, lk 101.

eeldada kohtuotsuse järgselt ja viimasena tulu, mis jäi saamata vara takistamisest, olenemata kas takistus oli ajutine.[114] Artikkel 36 kohaselt on võimalik saamata jäänud tulu hüvitada üksnes juhul, kui kahju on tuvastatud. Rahvusvaheliste vahekohtute praktika kohaselt on kohtud suhtunud saamata jäänud tulu kompenseerimisse vastumeelselt, kui tulu baseerub ainult spekulatiivsetele elementidele. Põhivaraga võrreldes on ettevõtte tulud haavatavad kaubanduslikele ja poliitilistele riskidele. Kohtuasjas *Asian Agricultural Products case* lükati kompensatsiooni nõue saamata jäänud tulu eest tagasi kindlaksmääratud tulude ja tõendite puudumise tõttu. Kohus leidis, kompensatsiooni määramiseks on vajalik, et saamata jäänud tulu oleks tõenäoline ning seda oleks võimalik mõistlikult prognoosida.[115] Mitte ainult ei pea saamata jäänud tulu olema tõestatud, peab see olema ka kooskõlas riigivastutuse eelnõu artikliga 31, ehk tulu on saamata jäänud rahvusvahelise õigusvastase teo tõttu.[116]

2.5 Mittevaralise kahju hüvitamine

Riigivastutuse eelnõu artiklis 37 sätestatud mittevaraline kahju hüvitamine on kolmandaks kahju hüvitamise vormiks, mida saab vastutavalt riigilt nõuda.[117] Artikkel sätestab, et rahvusvahelise õigusvastase teo eest vastutav riik on kohustatud hüvitama tekkinud kahju niivõrd, kuivõrd seda ei ole võimalik kõrvaldada ennistamise või varalise kahju hüvitamise teel. Tegemist on pigem erandliku kahju hüvitamise vormiga ja selle seos täieliku hüvituse põhimõttega on rõhutatud fraasiga „niivõrd, kui kahju ei ole võimalik kõrvaldada ennistamise või varalise kahju hüvitamise teel“. Seega saab mittevaralise kahju hüvitamisele toetuda, kui eelnevad kahju hüvitamise vormid ei võimalda täielikult tekkinud kahju kõrvaldada.

Vastavalt riigivastutuse eelnõu artikli 31 lõikele 2 on kahju, mille eest vastutav riik on kohustatud täies ulatuses hüvitama, "mis tahes riigi rahvusvaheliselt õigusvastase teo tagajärjel tekkinud nii materiaalne kui moraalne kahju“. Rahvusvaheliselt õigusvastasest teost tulenevad materiaalsed ja moraalsed kahjud on tavaliselt finantsiliselt hinnatavad ning seega kaetakse muude kahju hüvitamise vormidega. Mittevaraliste nõuete hüvitamise eelduseks on õigusvastased teod, mille tagajärgedel tekkinud kahju ei ole võimalik rahaliselt hinnata. Seega kuuluvad antud peatüki alla

[114] *Ibid*., lk 104.
[115] Otsus. ICSID. 1990. Asian Agricultural Products v Sri Lanka. No. ARB/87/3.
[116] United Nations (2008), *supra nota* 9 lk 105.
[117] *Ibid*., lk 105.

rikkumised mis on oma olemuselt sümboolsed, olenemata ohverriigile tekkinud materiaalsetest kahjustustest.[118] Mittevaralise kahju esinemist ja selle kuulumist hüvitamisele on mitmed rahvusvahelised kohtud ja tribunalid korduvalt tunnustanud. See puudutab eriti moraalset või õiguslikku kahju, mis on õigusvastase teoga riigile tekkinud.[119] Näidetena saab tuua juhtumeid, kus on solvatud riigi sümboleid, rikutud riigi suveräänsust ja territoriaalset terviklikust, väärkoheldud riigi diplomaatilisi esindajaid või valitsusjuhte ning rikutud saatkondade või konsulaatide puutumatust.[120]

Artikkel 37 lõige 2 sätestab, et miitevaralise kahju hüvitamise võib seisneda õigusvastase teo tunnustamises, kahetsuse avalduses, ametlikus vabanduses või muus sobivas vormis, jättes nimekirja võimalikest vormides avatuks. Kahetsuse väljendus oli mittemateriaalse kahju hüvitamise nõudena leidis aset kohtuasjades *I'm Alone*[121] ning *Rainbow Warrior,*[122] *Consular Relations*[123] ning *LaGrand* .[124] Kahetsuse väljendused on sagedased nähtused diplomaatilistes suhetes. Mittevaralise kahju hüvitamine võib hõlmata ka garantiisi õigusvastase teo lõpetamiseks ja nendest hoidumiseks. Artikli kolmas lõige kirjeldab heastamise nõude piire, sätestades kaks tingimust: esiteks peab olema heastamise nõue olema proportsionaalne tekkinud kahjuga ning teiseks ei tohi nõue olla vastutavale riigile alandav. Riigivastutuse eelnõu kommentaarid tõdevad, et mõiste „alandav" on ebatäpne, kuid selliseid juhtumeid on ajaloo vältel juhtunud.[125]

Nagu antud peatükis selgitati on kahju hüvitamise eesmärk kõrvaldada täielikult õigusvastase teo tagajärjel tekkinud kahju. Täielikult kahju kõrvaldamine eeldab tekitatud kahju suuruse ja ulatuse täpset tuvastamist. Kahju hindamine õigusvastase teo puhul, mille tagajärjel tekib ainult materiaalne kahju ei valmista probleeme, kuna mõju avaldub üldjuhul ainult füüsilises keskkonnas. Küberrünnaku kahjud võivad ulatuda aga füüsilisest keskkonnast kaugemale, mõjutades nii füüsilist keskkonda, seadmetes sisalduvaid andmeid ja informatsiooni kui ka üldist elukeskkonda. Küberründed demokraatlike protsesse võimaldava tehnoloogia vastu võivad kahju tekitada aga kõikides eelnimetatud valdkonnas, muutes nendest tekkinud kahju hindamise keeruliseks.

---

[118] United Nations (2008), supra nota 9, lk 105.
[119] Rainbow Warrior (1990), supra nota 23.
[120] United Nations (2008), supra nota 9, lk 106.
[121] Kohtuotsus. U.N.R.I.I.A. 05.01.1935. I'm Alone (Kanada v Ameerika Ühendriigid). vol. III (Sales No. 1949.V.2).
[122] Rainbow Warrior (1990), supra nota 23.
[123] Kohtuotsus. ICJ. 1998. Vienna Convention on Consular Relations (Paraguai v. Ameerika Ühendriigid), Order of 9 April 1998.
[124] Kohtuotsus. ICJ. 2001. LaGrand (Saksamaa v. Ameerika Ühendriigid). 2001 I.C.J. 466.
[125] *Ibid*., lk 107.

3. KÜBERRÜNNAKU KAHJU HINDAMINE

Enamasti toetutakse küberrünnakute õiguslikul hindamisel ÜRO põhikirja artiklile 2 (4), mille kohaselt on jõu kasutamine rahvusvahelistes suhetes keelatud. Artikkel 2 (4) sätestatud jõu kasutamise keeldu peetakse rahvusvahelise õiguse imperatiivnormiks, mille rahvusvaheline riikide ühendus on omaks võtnud ja tunnustab tervikuna kui normi, millest kõrvalekaldumine on lubamatu ja mida võib muuta ainult järgneva samasuguse iseloomuga üldise rahvusvahelise õiguse normiga. Termin „jõud" tähendab ÜRO põhikirja kontekstis relvajõudu. Terminit „relvajõud" omakorda sisustakse kui konventsionaalse jõu kasutamist riigi sõjaväe või paramilitaarsete rühmituste poolt. Õigusteadlased on võtnud seisukoha, et küberrünnakut saaks liigitada jõua kasutamise alla, peab küberrünnakul esinema kineetilise-, bioloogilise- või keemiarelvaga sarnane mõju.[126] Antud seisukohta kinnitavad ka ÜRO Peaassamblee resolutsioonid, mis ei näe poliitilist ja majandusliku sunni rakendamist kui „jõu" kasutamist.[127] Riigi poliitiline ja majanduslik sfäär on kaitstud mittesekkumise printsiibiga, mida loetakse sarnaselt jõu kasutamise keeluga rahvusvaheliseks imperatiivnormiks. Õigusteadlased on mõtestanud interventsiooni kui sekkumist teiste riikide sise- või välisasjadesse.[128] Alaline Rahvusvaheline Kohus on mittesekkumise printsiipi avanud kohtuasjas Nicaragua, märkides, et suveräänsuse põhimõtte kohaselt, on riik vaba valima oma poliitilise, majandusliku, sotsiaalse ja kultuurilise süsteemi ja otsustama oma välispoliitika üle. Sekkumist loetakse õigusvastaseks juhul, kui kasutatakse sunnimeetmeid valikute puhul, mis peavad jääma vabaks.[129] Võttes arvesse, et jõu kasutamise keeldu on võimalik rikkuda küberründega[130], on selge, et küberründega on võimalik rikkuda ka mittesekkumise printsiipi.

Mittesekkumise printsiibi rikkumine võimaldab riigil tugineda riigivastutuse printsiibist tulenevale kahju hüvitamise õigusele. Järgnevalt analüüsib autor riikide vastu toimepandud küberrünnakuid, tutvustades millist liiki kahju võib tekkida iga erineva küberrünnaku lõikes. Seejärel analüüsib autor küberkuritegevuse metoodika asjakohasust riigivastaste küberrünnakute tagajärjel tekkinud kahjude hindamisel. Siinkohal on oluline märkida, et kahju hüvitamise nõude

[126] Ziolkowski, K. 2012. Stuxnet – Legal Considerations. Publication. Nato Coperative Cyber Defence Centre of Excellence. Tallinn, 8.
[127] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations [in the following referred to as Friendly Relations Declaration], UN GA Res. 2625 [XXV] of 24 October 1970, Annex, Principle 1
[128] Kunig, P. 2008. Prohibition of intervention. *Max Planck Encyclopedia of Public International law*, p. 1.
[129] Kohtuotsus, ICJ. 27.06.1986. the case concerning Military and Paramilitary Activities in and against Nicaragua brought by Nicaragua against the United States of America, I.C.J. 39, p.110.
[130] Vida, M.A.J. 2005 Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places, 51 Naval L. Rev, 132.

puhul on oluline tuvastada mittesekkumise printsiibi rikkumine iga küberründe puhul eraldi. Küberrünnakute kahjude analüüsimisel ei tuvasta autor mittesekkumise printsiibi rikkumist,vaid eeldab, et mittesekkumise printsiibi rikkumine on toimunud.

3.1 Küberrünnakute liigid

Küberrünnakut võib kõige lihtsamalt defineerida kui tahtlikku tegevust õõnestamaks teise riigi arvutisüsteeme. Samuti saab küberrünnakut defineerida kui riigi meetmeid, millega tungitakse teise riigi arvutisüsteemidesse, eesmärgiga kahjustada või häirida sealseid süsteeme.[131] Küberoperatsioonidele kohalduva rahvusvahelise õiguse käsiraamatu täiendatud väljaanne *Tallinn Manual 2.0* defineerib küberrünnakut kui küberoperatsiooni, kas ründava kui kaitsva iseloomuga, mille toimumisel saab mõistlikult eeldada, et sellega põhjustatakse inimestele vigastusi või surma või kahjustatakse ja hävitatakse vara.[132] Samuti saab küberrünnakut defineerida kui riigi meetmeid, millega tungitakse teise riigi arvutisüsteemidesse, eesmärgiga kahjustada või häirida sealseid süsteeme.[133] Antud töö kasutab küberrünnaku definitsiooni, mis hõlmab riigi poolset tegevust, millega tungitakse teise riigi arvutisüsteemidesse ning sissetungimise tagajärjel tekib kahju.

Poliitiliselt motiveeritud küberrünnakud on igapäevaste küberrünnakutega võrreldes äärmiselt haruldased. Et küberrünnakut kvalifitseerida poliitiliselt motiveerituks tuginevad teadlased peamiselt ohverriigi poliitilise olukorra ja kasutatud küberrünnaku andmete analüüsimisele. Esimesed poliitiliselt motiveeritud küberrünnakute juhtumid on teada juba 20. sajandi lõpuaastatest. Esimesteks näideteks saab tuua NATO arvutisüsteemide vastaseid rünnakuid 1990. aastate lõpul endises Jugoslaavias ning ka Hiina häkkerite rünnakud USA sõjaväe saitidele pärast Hiina saatkonna pommitamist USA lennukiga endises Jugoslaavias. Viimase 10 aasta jooksul on aga poliitiliselt motiveeritud küberrünnakud muutunud järjest tavapärasemaks nähtuseks, ning neid saab vaadelda ka kui 21. sajandi välispoliitika instrumenti.[134]

---

[131] Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A. Perdue, W., Spiegel, J. (2012). *The Law of Cyber-Attack. California Law Review*, Vol 100, 823.
[132] Tallinn Manual 2.0 on the International law applicable to cyber operations. (2017). /Eds. Schmitt, M.N., Vihul, L. London: Cambridge Univesity Press, 415.
[133] Hathaway, O.A. (2012), supra nota 121, lk 823.
[134] Nazario, J. Politically Motivated Denial of Service Attacks. Arbor Networks. United States, 2. Kättesaadav: https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf 14.05.2018.

Küberrünnaku tagajärjel tekkinud kahjud võivad olla väga erinevad. Küberrünnak võib tekitada inimestes usaldamatust e-teenuste suhtes, seda eriti pangandus ja tervishoiu valdkondades. Küberrünnaku tagajärjeks võib samuti olla kulutuste kasv, mis puudutab arvutisüsteemide kindlustamist, mis võib tõsta pakkumise hinda. Küberrünnaku psühholoogilised mõjud võivad olla märkimisväärsed, levitades laialdselt inimeste seas hirmu ja paanikat, mis võib põhjustada ka poliitilisi muutusi. Lisaks kaudsetele küberrünnaku mõjudele, võib küberrünnaku tagajärjel tekkitda ka käega katsutav kahju, seda eriti juhul kui arvutisüsteemid on tihedalt integreeritud füüsilise maailmaga ja mis kontrollivad kriitilise tähtsusega teenuste kättesaadavust.[135] Potensiaalselt võib kõige enam kahju põhjustada küberrünnak, mis on suunatud riigi kriitilise infrastruktuuri ja selle infosüsteemide vastu.[136]

Välisasjade nõukogu poolt kogutud andmete põhjal pandi ajavahemikul 2005-2017 toime 208 rahvusvahelist küberrünnakut, mille toimepanemises on alust kahtlustada riiki. Uuringu kohaselt moodustas suur osa riigi vastu toime pandud küberrünnakutest luureinfo kogumine, mille uurimine väljub aga antud töö uurimisalast. Uuringu kohaselt esines 4 erinevat rünnaku liiki: teenustõkestusrünnak, näotustamine, sabotaaž ja andmete hävitamine. Järgenvalt analüüsib autor milline kahju riigivastaste küberrünnakutega tekkida võib, lähtudes riigivastutuse printsiibi kahju käsitlusest. Oluline on märkida, et autori poolt kasutatav käsitlus lähtub küberrünnakute praktikast, kuid tegemist ei ole ammendava loeteluga küberrünnaku tagajärjel tekkida võivatest kahjudest.

3.1.1 Hajutatud teenustõkestusrünnak

Teenustõkestusrünnakuks saab lugeda tegevust, kus ründaja sihilikult blokeerib arvutisüsteemi või arvutivõrgu ressursse selliselt, et lõppkasutajal ei ole võimalik neid kasutada. Teenustõkestusrünnaku mõte seisneb ohvri arvutisüsteemi ressursside nagu vahemälu, võrgu läbilaskevõime või protsessori jõudluse ära kasutamises, takistades seeläbi teistel kasutajatel ohvri pakutavate teenuste kasutamist. Seega on rünnaku eesmärk muuta arvutisüsteem võimetuks pakkuma teenust.[137] Hajutatud teenusetõkestusrünne (edaspidi DDoS) on tehniliselt sarnane tavalise teenustõkestusrünnakuga, kuid rünnaku toimepanemiseks kasutatakse arvutisüsteemi või

[135] Ghandi, R., Sharma, A., Mahoney, W., Sousan, W,. Zhu, Q., Laplante, P. 2011. Dimensions of Cyber-Attacks. Social, Political, Economic and Cultural. *Ieee Technology And Society Magazine*. Spring 2011, 7.

[136] Kaitseministeerium. Eesti Küberjulgeoleku strateegia 2008-2013. (2008), 10. Kättesaadav: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf 14.05.2018.

[137] Douligeris, C., Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. Department of Informatics. Computer Networks 44. 643-666.

sihtvõrgu liikluse mahu oluliseks suurendamiseks suurt arvu ründavaid süsteeme, näiteks robotvõrke. Robotvõrk koosneb enamasti kasutaja teadmata ülevõetud arvutitest, mida kasutatakse koordineeritud küberründe toimepanemiseks.[138] Kasutajate arvutid võetakse üle viiruse abil, mis võimaldab ründajal suunata kõik nakatanud arvutid ründe objektiks olevasse sihtvõrku, põhjustades sageli sihtvõrgu ajutist seiskamist.[139]

DDoS rünnete käigus koormatakse võrgus asuvad teenused või nende taga olev infrastruktuur sissetuleva võrguliiklusega üle, muutes selle välistele klientidele kättesaamatuks. Sarnaselt teenustõkestusrünnakuga ei ole DDoS rünnaku eesmärk tungida rünnatavasse arvutisüsteemi eesmärgiga varastada või hävitada seal leiduvaid andmeid, vaid selle ülesanne on takistada süsteemi tööd. DDoS rünnaku tagajärgi ei saa alati lühiajaliselt tuvastada, muutes tekkinud kahju hindamise raskeks.[140]

Arvestades, et DDoS rünnaku tagajärjed olenevad suuresti küberrünnaku ulatusest ja kestvusest, saab võimalikeks tagajärgedeks lugeda saamata jäänud tulu, organisatsiooni sisese töö seiskumist, klienditoe lakkamist, tark- ja riistvara asendamist ning tööjõukulude kasvu. Samuti võivad DDoS rünnakud mõjutada kommunikatsioonimehhanisme. DDoS rünnaku mõjud võivad hõlmata ka aeglustunud või ülekoormatud võrguühendust ning sihtarvutite eraldamist arvutivõrgust.[141]

Üheks näiteks poliitilisest vastuseisust, milles rakendati DDoS rünnakuid saab pidada 2007 aastal Eestis vastast küberrünnakut, mille tagajärjel sattusid Eesti riigiasutuste, pankade ning uudiste väljaannete leheküljed teenusetõkestusrünnakute alla. Küberründed, mille eesmärk oli häirida erinevaid Eesti infotehnoloogiliste süsteemide käideldavust, kestsid kokku 22 päeva. Kõik eelmainitud organisatsioonid langesid DDoS rünnaku ohvriks. Rünnakut vaadeldi kui emotsionaalset ja spontaanset vastust poliitilistele sündmustele Eestis, mis rullusid lahti punaarmee sõjamonumendi teisaldamisel. Küberründe ründeobjektid sai jagada kolmeks: interneti teenusepakkujad, riigi- ja poliitilised institutsioonid ning viimasena kommertsteenuse ettevõtted.

---

[138] Riigi Infosüsteemi amet. Turvainsidentide käsitlemine. (2012) Kättesaadav: https://www.ria.ee/public/Programm/Tarkeriik_2012/SOHO_materjalid16181012/Turvaintsidentide_kasitlemine.pdf 13.05.2018.

[139] Margulies, P. (2013). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, Melbourne Journal of International Law. Vol 14. No. 496, 6.

[140] Pau, L.F. (2010). Business and Social Evaluation of Denial of Service Attacks in View of Scaling Economic Counter-measures. Copenhagen Business School and Rotterdam School of Management. Kättesaadav: http://www.ccdcoe.org/publications/virtualbattlefield/20_PAU_Business%20and%20Social%20Evaluation%20of%20DDoS.pdf 13.05.2018.

[141] *Ibid*.

Eesti vastase küberrünnaku keskseks sihtmärgiks oli valitsusasutuste internetiliiklus ja veebiserverid. Küberrünnaku alla sattusid korraga nii valitsuse, presidendi, riigikogu ning välis- ja kaitseministeeriumi koduleheküljed. Võttes arvesse DDoS rünnaku iseloomu, mille eesmärk on takistada teenuse toimimist, ei teki üldjuhul taolise rünnaku puhul otsest füüsilist kahju seadmetele või informatsiooni infrastruktuurile. Küberrünnaku tagajärjel ei tekkinud teadaolevalt otsest füüsilist kahju riigi kui ka eraettevõtete informatsiooni infrastruktuurile. Samuti ei ole teada, et küberrünnaku tagajärjel oleks tekkinud intellektuaalomandi vargusest või muust ärisaladusest tulenevat kahju. Puuduvad andmed ka selle kohta, et küberrünnak oleks põhjustanud kahju riigi kodanike varale. Nagu eelpool mainitud hõlmab moraalne kahju endas kodanike individuaalset valu ja kannatusi, lähedaste surma või isiklike rünnakuid, mis on seotud eraelu- ja kodu puutumatusega. Autorile teadaolevalt, ei põhjustanud küberrünnak ka moraalset kahju.

Arvestades, et küberrünnaku keskseks sihtmärgiks oli Eesti valitsusasutuste internetiliiklus ja veebiserverid, oli valitsuse veebisaitide puudumise ja ametlike e-posti aadresside ülemäärase rämpspostamise tõttu tavaline suhtlemine valitsusega kodanike jaoks takistatud. Riigivastutuse printsiibi kohaselt mõeldakse materiaalse kahju all kahju riigi või tema kodanike varale või muudele hüvedele, mis on rahaliselt hinnatav. Veebilehe www.eesti.ee kaudu pakutavate võrgupõhiste teenuste toimimise takistamine küberrünnakuga avaldas teatud osale elanikkonnast nähtavat mõju, kuna neid teenuseid kasutati laialdaselt maksuaruannete esitamiseks, sotsiaaltoetuste taotlemiseks ning muuks suhtluseks valitsusega, omades seeläbi otsest praktilist või rahalist tähendust.[142] Seega võis veebilehe www.eesti.ee kaudu pakutavate teenuste takistamisest tuleneda otsene majanduslik kahju nii füüsilistele- kui ka juriidilistele isikutele, mis on rahaliselt hinnatav.

Et täpsemalt mõista e-teenuste katkemisest tulenevat kahju, tuleb kõigepealt analüüsida nende eesmärki. Eesti riik on seadnud avalike teenuste arendamise eesmärgiks osutada teenuseid kiiresti ja võimalikult väikese halduskoormusega. Seega on oluliseks märksõnaks siinkohal kulude minimeerimine. Eesti riik on saavutanud e-teenuste arendamise ja uuendamisega märkimisväärse aja – ja rahasäästu. E-teenuse kasu koosneb vahetust rahalisest kasust, mis tuleneb kulude ja halduskoormuse vähenemisest, mis omakorda võimaldab vabanevat ressurssi kasutada

[142] Tikk, E., Kaska, K., Vihul, L., Vihul, K. (2010). International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence. Tallinn, 25.

uuendusteks, asjaajamise lihtsustamiseks või aja ja raha säästmiseks.[143] E-teenuse toimimise takistamine võib endaga kaasa tuua kulutuste kasvu, mis võib seisneda nii vajaduses kaasata rohkem tööjõudu kui teenuse kättesaadavuse parandamiseks tehtavatest kulutustest, kui ka tööprotsesside ja organisatsiooni juhtimise muutmises. Tegemist on seega kahjuga, mis häirib tavapärast organisatsiooni tööd ning seega ei võimalda saavutada tavapärast töömahtu. Suurenenud halduskulud on samuti rahaliselt hinnatav kahju, mis mahub ka riigivastutuse eelnõu kahju määratluse raamidesse.

Küberrünnaku üheks tagajärjeks saab lugeda ka riigi edasisi samme küberjulgeoleku tugevdamiseks, mille elluviimine eeldab finantsilisi kulutusi. Küberjulgeoleku strateegia aastateks 2008-2013 kohaselt võttis riik eesmärgiks karmistada Eesti kriitilise infrastruktuuri ettevõtete, kuid ka teiste infosüsteemide turvalisusnõudeid ning kehtestada selged standardid. Samuti nägi strateegia ette IT-infrastruktuuri käideldavuse tugevdamist, sealhulgas nii avaliku kui erasektori asutuste teenuseserverite koormustaluvuse suurendamist ning võrguliikluse monitooringu ja intsidentide strateegilise ja taktikalise analüüsi suutlikkuse tugevdamine. Samuti võeti eesmärgiks korraldada kriitilise infrastruktuuri küberkaitset ja parandada riigisisest koordinatsiooni küberohtude vastu võitlemisel. Et eelkirjeldatud eesmärke ellu viia, nägi strateegia ette 8,5 miljoni euro täiendava ressursi vajadust.[144]

Küberrünnakul saab samuti olla ka psühholoogilised mõjud. Küberrünnaku ohvriks langesid kõik suuremad meediaväljaandeid Eestis. Eesti valitsus tugines teabe jagamiseks veebipõhisele keskkonnale, mida ka rahvusvahelised meediaorganisatsioonid laialdaselt kasutasid. Küberrünnete tõttu oli seega osaliselt takistatud ka informatsiooni jagamine, mistõttu ei saanud inimestele edastada informatsiooni küberründega põhjustatud häiretest.[145] Lisaks mõjutasid pronksiöö küberrünnakud ka riigi infovoogu välismaale. Arvestades, et riigi meediaväljaannete tegevus, sealhulgas riigi poolse informatsiooni edastamine oli takistatud, koosmõjus riigipoolsete e-teenuste lakkamisega võib antud küberrünnak mõjutada tugevalt inimeste usaldust valitsuse, kui ka riigi vastu üldiselt. Seega saab pronksiöö küberrünnaku vaadelda kui rünnakut riigi

[143] Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis. (2013). E-teenuste kasutamise tulemuslikkus ja mõju. (Toim.) Kalvet, T., Tiits, M., Hinsberg, H. Tallinn. Kättesaadav: http://www.praxis.ee/fileadmin/tarmo/Projektid/Valitsemine_ja_kodanike%C3%BChiskond/E-teenuste_kasutamise_tulemuslikkus_ja_moju.pdf 13.05.2018 13.05.2018.
[144] Kaitseministeerium (2008), *supra nota* 126, lk 36.
[145] E. Tikk, K. Kaska, L. Vihul, K. Vihul. (2010), *supra nota* 137, lk 25.

mittemateriaalseid huvide vastu, mille tagajärjeks saab lugeda kahju riigi aule, väärikusele või prestiižile.

DDoS rünnaku kasutamine poliitilistel eesmärkidel leidis aset ka 2016 ja 2017 aastal Montenegros. 2016 aasta oktoobris toimunud Montenegro parlamendi valimiste keskseks küsimuseks oli suurem integratsioon Euroopaga või tihedam koostöö Venemaaga. 16. oktoobril kui algasid parlamendi valimised, jäid mitmed riigi valitsusasutuste veebilehed, meediaväljaanded, sh koalitsiooni erakonna veebileht ning riigi informatsiooni infrastruktuur küberrünnaku alla. Sarnaselt 2007 aastal Eestis aset leidnud küberrünnakuga oli ka siinjuhul küberrünnak läbi viidud professionaalselt ning süstemaatiliselt. Taoline rünnakumuster leidis aset ka 2017 aasta veebruaris, kui Montenegro valitsus otsustas liituda Põhja-Atlandi Organisatsiooniga. Sarnaselt 2007 aastal toimunud küberrünnakuga Eestis, ei tekkinud ka Montenegros küberrünnakute tagajärjel füüsilist kahju, sellegipoolest esinesid mõjutused kommunikatsioonimehhanismide tavapärases töös. Uudistekanalite, erakondade- ja valitsuse veebilehtede ründamine iseloomustab küberrünnaku eesmärki, mille kohaselt püüti takistada inimestele suunatud infovoogu. Sarnaselt pronksiöö küberrünnakuga, ei tekkinud ka siinjuhul kahju riigi ega kodanike varale. Samuti puudub riigi kodanikele põhjustatud moraalne kahju. Autorile teadaolevalt ei tekkinud ka muud materiaalset kahju. Sarnaselt pronksiöö küberrünnakuga, on ka siinjuhul tekkinud riigile kahju mittemateriaalsete huvide vastu, mille tagajärjeks saab lugeda kahju riigi aule, väärikusele või prestiižile.[146]

Riigivastaseid DDoS rünnakuid on Välisasjade Nõukogu uuringu kohaselt toimunud aastatel 2005-2017 kokku 15 korral.[147] 2007. aasta oktoobris jäi arvatava massiivse teenustõkestus rünnaku alla Hiina välisministeeriumi ning mitmed kaitsetööstuse organisatsiooni veebilehed. Hiina kahtlustuse kohaselt pani rünnaku toime Taiwani riigiagent.[148] 2008. aasta augustis sattusid Gruusia informatsiooni infrastruktuur, sealhulgas meedia, side ja transpordi ettevõtted laiaulatusliku DDoS rünnaku alla. Märkimisväärseks teeb rünnaku asjaolu, et paralleelselt küberrünnakuga oli Venemaa alustanud sõjalist tegevust Gruusias.[149] 2009. aasta juulis jäi DDoS

[146] Farmer, B. Montenegro asks for British help aftercyber attacks in wake of Russian-backed coup plot. – The Telegraph, 28. Veebruar.
[147] Council of Foreign Affairs. Cyber Operations tracker. Cyber Incident Data. Kättesaadav: https://www.cfr.org/interactive/cyber-operations 15.05.2018.
[148] Chung, L. (2007), Beijing seeks Taiwanese secret agent over hacking. – South China Morning Post, 1. November.
[149] Markoff, J. (2008). Before the Gunfire, Cyberattacks. – New Tork Times, 12. August.

rünnaku alla mitmed Ameerika Ühendriikide valitsusasutuste veebilehed ning finantsettevõtted.[150] Sarnane juhtum leidis aset ka 2011. aasta aprillis kui Lõuna-Korea valitsusasutuste ning Lõuna-Koreas paiknevate Ameerika Ühendriikide sõjaväe üksustega seotud veebilehed jäid kümneks päevaks DDoS rünnaku alla.[151] 2012. aasta septembris jäid mitmed Ameerika Ühendriikide finantseerimisasutused koordineeritud teenustõkestusrünnaku alla, mistõttu ei olnud klientidel võimalik pääseda ligi finantsasutuse e-teenustele[152]. 2013. aasta mai kuus sattusid jällegi Lõuna-Korea meediaväljaannete ning pankade veebilehed teenustõkestusrünnaku alla.[153]

3.1.2 Sabotaaž

Kübersabotaaž hõlmab tahtlikke ja pahatahtlikke tegusid, mille tagajärjeks on normaalsete protsesside ja funktsioonide katkemine või seadmete või teabe hävitamine või kahjustamine, mis saavutatakse läbi arvuti, riist- või tarkvara kasutamise või manipuleerimise. Kübersabotaaž ei piirdu veebipõhiste materjalide saboteerimisega, vaid mõjutab inimesi ka väljaspool arvutisüsteeme.[154]

Tuntuim kübersabotaaži juhtum leidis aset 2010. aastal kui arvutiviirus Stuxnet viis rivist välja suure hulga Iraani Nantazi uraanirikastamisjaama tsentrifuugidest. 2010. aastal teatas Iraan avalikult, et küberrünnaku tagajärjel on Nantazi uraanirikastamisejaama gaasitsentrifuugid saanud kahjustada. Küberrünnaku teeb eriliseks asjaolu, et tegemist oli esimese juhtumiga, kus küberrünnak viidi ellu konkreetse eesmärgiga kahjustada, häirida, ja hävitada konkreetne sihtmärk.[155] Stuxnet oli täpsemalt suunatud sagedusmuundurite ajamite vastu, mis kontrollisid gaasitsentrifuugide mootoritite kiirust. Stuxnet muutis gaasitsentrifuugidele suunatud elektrivoolu sagedust, pannes nad tööle pööretel, milleks nad ei olnud disainitud.[156] Iraani ametnikud ei ole tänaseni kinnitanud, et arvutiviiruse oleks põhjustanud materiaalselt laadi kahju tsentrifuugide või

[150] Harden, B., Krebs, B., Nakashima, E. Who's behind cyber assults? – The Seattle Times, 9. Juuli.
[151] BBC News. (2011). South Korea hit by cyber attacks. – 4. Märts..
[152] Perloth, N., Hardy, Q. (2013). Bank Hacking Was the Work of Iranians, Officials Say. New York Times, 8. Jaanuar.
[153] Braningan, T. (2013). South Korea on alert for cyber-attacks after major network goes down. – The Guardian, 20. Märts.
[154] O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity College Law Review*. Vol 16, 137-160.
[155] Iasiello, E. (2013). Cyber attack: A dull tool to shape foreign policy. *2013 5th International Conference on Cyber Conflict*. (Toim.) Podins, K., Stinissen, J., Maybaum, M. Tallinn, Estonia. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 7-11.
[156] Farwell, J.P., Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival. Global Politics and Strategy*. Vol. 53, 24.

muudele süsteemidele.[157] Iraani Presidendi sõnul tekkisid teatud tsentrifuugidega probleemid.[158] Erinevate autorite hinnangul pikendas arvutiviirus Iraani tuumaprogrammi aga mõne aasta võrra ning kahjustada sai kuni 1000 gaasitsentrifuugi.[159] Küberrünnaku tagajärjel tekkis seega materiaalne kahju, mis sisaldas endas tsentrifuugide väljavahetamisest tulenevaid kulusid. Gaasitsentrifuuge kasutatakse isotoopide eraldamiseks, mis on oluline protsess uraani rikastamisel. Gaasitsentrifuugi kahjustamine võib seega mõjutada ka uraanirikastamisejaama tööd. Samuti peab antud juhul arvestama mittemateriaalsete huvide kahjustamisega. Uraanirikatamisejaamad on riikliku tähtsusega ehitised, mistõttu nende ründamine võib kahjustada ka riigi au ja mainet.

Järgmine oluline kübersabotaaži juhtum leidis aset 2015. aastal Ukrainas, mille tagajärjel kaotas kuni 225 000 inimest elektriühenduse. Vahetult enne küberrünnaku toimumist, jõudis Ukraina parlamendis arutusele eelnõu, mille kohaselt plaaniti riigistada eraomandis olevad elektriettevõtted. Mitmed Ukrainas asuvad elektriettevõtete omanikud on Venemaa kodanikud, ning arvestades Krimmi annekteerimist 2014. aastal arvatakse, et tegemist oli poliitiliselt motiveeritud küberrünnakuga, mille eesmärgiks survestada Ukraina riigivõimu elektriettevõtete riigistamise mõttest loobumiseks.[160] Küberrünnakuga tungiti kolme Ukraina elektripakkuja ettevõtte arvuti- ja SCADA süsteemidesse, mille tagajärjel lõpetasid 30 alajaama elektri jagamise mitmeks tunniks.[161] Elektripakkujad pidid minema üle käsitsi juhtimisele, et taastada elektri jõudmine inimesteni. Vahetult enne elektrilevi katkestamist, rünnati ka elektripakkujate kõnekeskusi teenustõkestusrünnakuga. Telefoni teenustõkestusrünnakuga ujutati kõnekeskused üle tuhandete võltskõnedega, mis takistasid klientidel elektrikatkestuse teatamisest. Tegemist oli esmakordselt dokumenteeritud juhtumiga, kus küberrünnaku tagajärjel põhjustati elektrienergia kaotus. Küberrünnaku lõppfaasis kustutati elektripakkujate poolt kasutatavate arvutisüsteemide olulised failid, mille tõttu ei olnud võimalik hiljem enam arvuteid käivitada. Autorile teadaolevalt saab antud juhul materiaalseks kahjuks lugeda ainult elektrijagamise protsessi juhtinud arvuitsüsteemidele ja arvutitele põhjustatud kahju, mis muutusid rünnaku järgselt kasutamiskõlbmatuks.

[157] Ziolkowski (2012), supra nota 116, lk 5.
[158] Broad, W.J., Markoff, J. Sanger, D.E. (2011), Israeli Test on Worm Called Crucial in Iran Nuclear Delay. – The New York times, Jaanuar 15.
[159] Lindsay, J.R. (2013). Stuxnet and the Limits of Cyber Warfare, Security Studies. Vol 22-3, 390.
[160] Zetter, K, (2016). Inside the cunning, unprecedented hack of Ukraines power grid. – Wired, 3. Märts.
[161] Alford, T.J. (2017). Off the Grid: Facilitating the Acquisition of Microgrids for Military Installations to Achieve Energy Security and Sustainability. *George Washington journal of energy & environmental law*. Vol 8-2, 101.

Riigi elutähtsate infrastruktuuride vastu suunatud küberünnakud on kõige suurema kahju potentsiaaliga. Euroopa Nõukogu direktiiv Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta sätestab, et elutähtsad infrastruktuurid on ELi liikmesriikides asuv vara, süsteem või nende osa, mis on hädavajalikud eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku, inimeste majandusliku ja sotsiaalse heaolu toimimiseks ning mille kahjustada saamine või hävimine mõjutaks nimetatud toimingute toimimishäire tulemusena oluliselt liikmesriiki. Direktiivi kohaselt kuulub elutähtsate infrastruktuuride valdkondade loetellu elektrienergia tootmiseks ja ülekandmiseks vajalikud infrastruktuurid ja rajatised seoses elektrienergia tarnimisega.[162] Elektrikatkestuse tõttu võivad katkeda mitmed elutähtsad teenused ning väheneda võib oluliselt ühiskonna turvalisus. Elutähtsa infrastruktuuri vastu suunatud küberründed sisaldavad endas ka psühholoogilist kahju, vähendades inimeste usaldust nii riigi kui ka elektripakkujate vastu.

Kübersabotaaži juhtum leidis aset ka 2014. aastal Saksamaal, kui küberrünnakuga tungiti terasetehase arvutisüsteemidesse. Küberrünnakuga manipuleeriti ja häiriti arvutisüsteemi selliselt, et rünnaku tagajärjel ei olnud võimalik kõrgahju korralikult sulgeda, mistõttu sai seade oluliselt kannatada.[163] Sarnaselt 2015. aastal Ukrainas toimunud kübersabotaaži juhtumiga, sattus 2016, aastal Ukrainas Kiievi elektrivõrk küberünnaku alla, mille tagajärjel lakkas Kiievi lähedal paiknenud elektrijaotusjaam töötamast, jättes inimesed kodudes ilma elektrita.[164]

3.1.3 Andmete hävitamine

Andmete hävitamine saab toimuda arvutisüsteemi sissetungimisrünnakuga. Sissetungimisrünnakud kasutavad ära arvutisüsteemi haavatusi, et saada ligipääs süsteemi ressurssidele. Sissetungimisrünnakud võivad toimuda otsese süsteemi sissetungimisega või kaudse sissetungimisega, kus kasutatakse arvutivüsteemile ligipääsu saamiseks pahavara.[165]

[162] Euroopa Parlamendi ja nõukogu 8. detsember 2008 aasta direktiiv 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta, 80.
[163] Zetter, K. (2015). A cyberattack has caused confirmed physical damage for the second time ever. – Wired, 1. August.
[164] Polityuk, P. (2016). Ukraine investigates suspected cyber attack on Kiev power grid. – Reuters, 20. Detsember.
[165] Nguyen, R. (2013). Navigating Jus Ad Bellum in the Age of Cyber Warfare. California Law Review. Vol 101-4, 1094.

Saudi Araabia riikliku naftakompaniid Saudi Aramcot tabas 2012. aasta 15. augustil arvutiviirus, mis võis levida üle 30 000 Windosi-põhise personaalarvuti, mis tegutsesid ettevõtte arvutivõrgus. Küberrünnaku teeb märkimisväärseks asjaolu, et Saudi Aramco on maailma suurim naftaeksportija, kelle toodang moodustab 10% kogu maailma naftatoodangust.[166] Arvutiviiruse peamiseks eesmärgiks oli arvuti kõvakettal olevad andmed kustutada ning muuta arvutid kasutamiskõlbmatuks.[167] Arvutiviirus Saudi Aramco tootmist juhtivaid arvutisüsteeme ei mõjutanud, mistõttu maavarade puurimise ja rafineerimise protsessid arvutiviiruse tagajärjel ei seiskunud. Samuti ei tekkinud riigi infrastruktruurile rünnaku tagajärjel materiaalset kahju.[168] Saudi Aramco palkas mitmeid arvutisüsteemi eksperte tuvastamaks kui suures ulatuses arvutiviirus kahju põhjustas. Viiruse tagajärjel hävis aga ligi 30 000 Windowsi baasil oleva arvuti andmed, muutes need kasutajatele kasutamiskõlbmatuks. Ettevõtte oli sunnitud sulgema ettevõtte sisese suhltemisvõrgu, peatama interneti ühenduse ning e-posti teenused, et vältida arvutiviiruse edasi liikumist teistesse süsteemidesse. Olenemata, et arvutiviiruse tagajärjel ei saanud tootmisprotsess kannatada, olid ettevõtte äriprotsessid sellest olenemata mõjutatud. Kaks kuud pärast küberrünnakut ei olnud endiselt töötajatel võimalik kasutada ettevõttesisest e-posti ning sisemist suhtlusvõrku. Ettevõtte veebilehele ei olnud võimalik ligi pääseda pikalt ka peale seda, kui Aramco sõnul oli tavapärane tööprotsess taastunud.[169] Materiaalseks kahjuks saab siinkohal pidada ligi 30 000 arvuti välja vahetamisest tulenevat rahalist kahju. Materiaalseks kahjuks saab pidada ka küberrünnaku kahju ulatuse tuvastamise, kõrvaldamise ning kahju vähendamisega seotud kulutusi. Arvestades, et ettevõtte sisesed tööprotsessid olid oluliselt mõjutada saanud, võib küsimuse alla tulla ka saamata jäänud tulu.

Saudi Araabiat tabas sarnane küberrünnak ka 2016. aastal. Ründajad olid seekord sihtmärgiks võtnud Saudi Araabia transpordisektori ning ründe käigus õnnestus neil kustutada ja tekitada segadust arvutisüsteemides, mida kasutati mitmetes riigi lennujaamades.[170] Sama aasta detsembris sattus küberrünnaku alla mitmed Ukrainas tegutsevad pangad, kelle arvutid muutusid küberrünnaku tagajärjel kasutamiskõlbmatuks. [171]

[166] Tikk-Ringas, E., Bronk, C.(2013). Hack or Attack? Shamoon and the evolution of cyber conflict. Working paper. James. A. Baker III Institute for Policy Rice University, 3.
[167] *Ibid*., lk 17.
[168] Perlroth, N. (2012). In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. – The New York Times, 23. Oktoober.
[169] *Ibid*.
[170] Riley, M., Carey, G., Fraher, J. (2016). Destructive Hacks Strike Saudi Arabia, Posing Challenge to Trump. – Bloomberg, 1. Detsember.
[171] Leyden. J. (2016). BlackEnergy power plant hackers target Ukrainian banks. – The Register, 15. Detsember..

3.1.4 Näotustamine

Näotustamist saab lugeda küberründeks, mis rikub veebisaidi ametliku sisu. Tihti asendatakse ründe käigus veebilehe originaalne sisu mõne äärmusliku või poliitilise sõnumiga.[172] Näide näotustamisega seotud ohtudest ilmnes 2017. aasta juulis, kui Katari uudisteagentuur langes küberrünnaku ohvriks. Küberrünnaku tagajärjel võeti Katari rahvusliku uudisteagentuuri veebileht koos sotsiaalmeedia platvormidega üle, ning esitati vale informatsiooni, mille kohaselt olevat Katari emiir toetanud Iraani, Iisraeli, Hezbollaht ning Hamasi. Vale informatsiooni õnnestus ründajatel esitada rahvusringhäälingu saadetesse libauudiste lisamisega ning sotsiaalplatvormi Twitter postitustena, kasutades selleks Katari ametlikku kasutajakontot. Küberrünnaku tagajärjel keelasid Saudi Araabia, Araabia Ühendemiraadid, Bahrein ja Egiptus kogu Katari meedia, millele järgnes ka kaubandus- ja diplomaatiline boikott, saates regiooni järjekordsesse poliitilisse patiseisu.[173] Olenemata, et küberrünnak kestis väga lühikest aega (4 tundi) oli sellest tulenev kahju kahtlemata suur. Ainuüksi Katari aktsiaturg kukkus kriisi esimese nelja nädala jooksul turuväärtuses umbes 10%, ehk umbes 15 miljardit dollarit[174] ning võitlemaks boikotist tuleneva negatiivse mõjuga süstis Katari valitsus majandusse 39 miljardit dollarit riigireservide vahendeid.[175] Seega halvendas küberrünnak Katari majandus- ja poliitilist seisu oluliselt sundides Katari tahtevastaselt vastu võtma otsuseid nii sise- kui välispoliitiliselt.

Sarnane rünnakumuster leidis aset ka 2015. aastal Prantsuse televisoonivõrgu TV5 Monde ründamisel. Küberrünnakuga häiriti TV5 Monde saadete edastamist ning saadi ligipääs televisoonivõrgu sotsiaalmeedia platvormide kasutajakontodele. Küberrünnaku käigus asendati eetrisse minevad saated musta ekraaniga ning televisioonivõrgu veebilehe ning Facebooki ja Twitteri kasutajakontode kaudu levitati džihaadi propaganda sõnumeid.[176] Edastatud info sisaldas endas väidetavalt terrorismivastaste operatsioonidega seotud Prantsuse sõdurite sugulaste isikuandmeid ja muud isikliku informatsiooni ning ähvardusi mis olid suunatud Prantsuse sõdurite endi vastu.[177] TV5 Monde Facebooki kasutajakontole postitati sarnase sisuga teateid, milles

[172] Riigi Infosüsteemi Amet. (2014). Ohtlike internetiressursside eemaldamine internetist. Juhend. Kättesaadav: https://www.ria.ee/public/Kuberturvalisus/Ohtlike_internetiressursside_eemaldamine_Internetist.pdf 13.05.2018.
[173] Deyoung, K., Nakashima, E. (2017). UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials. – The Washington Post, 16. Juuli.
[174] BBC News. (2017). Qatar crisis: What you need to know. – 19. Juuli.
[175] The Economist. (2017). The boycott of Qatar is hurting its enforcers. – 19. Oktoober.
[176] Lichfield, J. (2015). TV5Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link. – Independent, 10. Juuni.
[177] Brangetto, P., Veenendaal, M.A. (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. *8th International Conference on Cyber Conflict.* (Toim.). Pissanidis, N., Rõigas, H., Veenendaal, M.A. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 122.

ähvardati Prantsuse sõdurite lähedasi. Lisaks kritiseeriti Prantsusmaa Presidendi otsuseid terrorismivastases sõjas.[178] TV5 Monde arvutisüsteemid olid küberrünnaku tagajärjel saanud tõsiselt kahjustada - televisioonivõrgu 11 erinevat kanalit olid töökorrast väljas ning kõik arvutisüsteemid olid suletud.

Sarnaselt Saudi Aramco juhtumiga, saab ka siinjuhul rääkida materiaalsest kahjust mis hõlmab kahjustada saanud seadmete vahetamist, küberrünnaku tuvastamist, rünnaku ulatuse ning tekkinud kahju ja allika kindlaks tegemist. Mittemateriaalseks kahjuks saab pidada sarnaselt pronksiöö rünnaku tagajärjel tekkinud riigile kahju mittemateriaalsete huvide vastu, mille tagajärjeks saab lugeda kahju riigi aule, väärikusele või prestiižile. Näotustamise juhtum leidis aset ka 2010. aastal, kui ründajat võtsid Hiina suurim interneti otsingumootori Baidu enda kontrolli alla ning edastasid veebilehel poliitilise motivatsiooniga teksti.[179]

3.2 Kahju rahalise hindamise analüüs

Küberkuritegevuse kulude hinnangud näitavad märkimisväärset variatsioon. See kajastab andmete puudumist ja erinevust kahjude hindamise metoodikates. Strateegiliste ja rahvusvaheliste uuringute keskuse ja arvutiturbefirma McAfee poolt läbi viidud uuringu kohaselt, ulatuvad globaalse küberkuritegevuse kulud hinnanguliselt 400 kuni 600 miljardi dollarini.[180] Accenture ja Ponemon Instituudi 2017. aastal läbi viidud uuringu kohaselt ulatub keskmise küberkuriteo kulu 11.27 miljoni dollarini. Oluline on märkida, et küberkuritegevuse kulud erinevad oluliselt riigiti, organisatsiooni suuruse ning küberrünnaku tüübi ja tõhususe seisukohast.[181] Samuti erinevad käsitlused küberrünnaku tagajärjel tekkinud kahjudest ja nende liigitusest.

Euroopa Parlamendi ja Nõukogu isikuandmete kaitse üldmääruse (2016/679) kohaselt saab isikuandmete töötlemisel tulenevatest ohtudest tekkida füüsiline, materiaalne või mittemateriaalne

[178] Campbell, J. (2015). French TV network TV5Monde 'hacked by cyber caliphate in unprecedented attack' that revealed personal details of French soldiers. – Independent, 9. April.
[179] BBC News. (2010). Baidu hacked by 'Iranian cyber army'. – 12. Jaanuar.
[180] Center for Strategic and International Studies & McAfee. (2018). Economic Impact of Cybercrime — No Slowing Down. Report. Kättesaadav: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70- 13.05.2018.
[181] Ponemon Institute & Accenture. (2017). Cost of cybercrime study. Inshigts on the security investments that make difference. Kättesaadav: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf 13.05.2018.

kahju ning antud kahju saab tekkida eelkõige juhtudel, kui isikuandmete töötlemine võib põhjustada diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, maine kahjustamist, ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu, pseudonümiseerimise loata tühistamist või mõnda muud tõsist majanduslikku või sotsiaalset kahju.[182] Isikuandmete kaitse üldmäärus on suunatud füüsiliste isikute isikuandmete kaitsele, seega on kahjude käsitlus füüsilise isiku põhine, jättes arvestamata organisatsioonile ja riigile tekkida võivad kahjud. Euroopa Parlamendi ja Nõukogu direktiiv meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisus ühtlaselt kõrge tase kogu liidus (2016/1148) kirjeldab, et võrgu- ja infosüsteemide tahtlik kahjustamine võib takistada majandustegevust, põhjustada olulist finantskahju, vähendada kasutajate usaldust ja tekitada liidu majandusele suurt kahju.[183] Antud käsitlus ei anna aga täielikku ülevaadet küberrünnaku tagajärjel tekkida võivatest kahjudest.

Küberrünnakute kahjusid on rahvusvahelisel tasemel uuritud eelkõige küberkuritegevuse võtmes. Globaalse küberkuritegevuse kahju arvutamise uuringute valimi moodustavad enamjaolt ettevõtted, ning kahju tuvastamise lähtekohaks on ettevõtetele tekitatud majanduslik kahju. Võttes aluseks erinevad uuringud, saab küberkuritegevuse kahjude hindamise metoodika koostada järgmiselt[184]:

Organisatsiooni välised kulukomponendid:

a) Andmete kadu või vargus: Tundliku ja konfidentsiaalsete andmete kaotusest või vargusest tulenev kahju. Hõlmab ka intellektuaalomandi või ärisaladuse vargusest, kliendiinfo ning töötajate andmete kaotusest tulenevat kahju. Sisaldab ka andmete rikkumisega seotud teavituskulusid.

[182] Euroopa Parlamendi ja nõukogu 27. aprill 2016 määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus), 15.
[183] Euroopa Parlamendi ja nõukogu 6. juuli 2016 direktiiv meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus, 1.
[184] The Council of Economic Advisers. (2018). The Cost of Malicious Cyber Activity to the U.S. Economy. Report. Kättesaadav: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf; Ponemon Institute 2016. Cost of cyber Crime Study & the Risk of Business Innovation. Report. Kättesaadav: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf; Center for Strategic and International Studies & McAfee. (2018). Economic impact of Cybercrime – No slowing down. Report. Kättesaadav: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70- 13.05.2018.

b) Äritegevuse häirimine: hõlmab majandusliku kahju, mis tuleneb organisatsiooni tavapärase töömahu mittesaavutamises.
c) Saamata jäänud tulu: hõlmab endas nii klientide kui investeerijate kaotusest tulenevat kahju, mis on tingitud arvutisüsteemide töös esinevatest viivitustest või nende sulgemisest. Sisaldab endas ka tekitatud mainekahju.
d) Seadmetele tekitatud kahju: hõlmab kahjustada saanud seadmete ning infrastruktuuri asendamist ning parandamist.

Organisatsiooni sisesed kulukomponendid:

e) Tuvastamine ja uurimine: tegevused ja kulud, mis on vajalikud küberrünnaku tuvastamiseks, selle ulatuse, tekitatud kahju ning allika kindlaks tegemiseks. Siia hulka kuuluvad ka esialgsed kulutused seoses tööprotsesside ümberkorraldamisega. Andmetelekete kahjude hindamise metoodika kohaselt hõlmab tuvastamine endas uuringute ja ekspertiiside läbiviimist, tõenäoliste ohvrite kindlaksmääramist, intsidentide reageerimise meeskonna korraldamist ning ohvrite ja järelevalve asutuste teavitamist ning varustamist vajalike andmetega.[185]
f) Kahjude minimeerimine: hõlmab tegevusi, mis on suunatud küberrünnaku peatamisele või vähendamisele. Nende hulka kuulub ka teiste kõrge riskiga teenuste ja rakenduste sulgemisest tulenev kahju.
g) Taastamine: tegevused ja kulud, mis on seotud organisatsiooni süsteemide ja põhiliste äriprotsesside parandamisega ja tööle saamisega. Samuti kulud mis on seotud hävitatud andmete ja muude IT süsteemide taastamisega.
h) Küberrünnaku järgsed tegevused: tegevused, mis aitavad organisatsioonil minimeerida võimalike tulelaseid rünnakuid. Sisaldab uute tehnoloogiate ja süsteemide lisamise kulusid. Andmelekete kahjude hindamise metoodika järgselt kuuluvad küberrünnaku järgsetesse tegevustesse lisaks auditite läbiviimine, isikuandmete kaitse teenused ning juriidilised teenused.[186]

Võttes aluseks eeltoodud kahjude hindamise metoodika, analüüsib autor selle asjakohasust riigi vastaste küberrünnakute kahjude hindamisel.

[185] Ponemon Institute.(2017). Cost of Data Breach Study. Global overview. Research Report, lk 30. Kättesaadav: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN 13.05.2018.
[186] *Ibid*.

3.2.1 Organisatsiooni välised tagajärjed

Küberkuritegevuse kahjude hindamise metoodika kohaselt on üheks väliseks kahjukomponendiks küberrünnaku tagajärjel kaotatud andmetest tulenev kahju. Siia alla kuuluvad tundliku ja konfidentsiaalse info kadumisest kui ka intellektuaalomandi või ärisaladuse vargusest tulenev kahju. Nende hulka kuulub lisaks ka ettevõtte töötajate ning klientide andmete vargusest ja sellest teavitamisest tulenev kahju. Andmete kadu või vargus on Accenture ja Ponemon Instituudi uuringu kohaselt küberrünnaku kõige kallim kulukomponent välistest teguritest, moodustades küberrünnaku kogu kahjust 43%.[187] Andmete kaotusest tuleneva kahju näiteks saab tuua Saksamaa ettevõtte SolarWorld AG vastu toimepandud küberrünnakut, mille tagajärjel varastati ettevõtte arvutiandmed. Varastatud andmetes oli teave SolarWorld'i finantsseisundi, tootmisvõimsuste, kulude ja äristrateegia ning käimasolevate kaubandusvaidluste kohta. Varastatud andmete tulemusel ei pidanud Hiina konkurent investeerima toote arendusse ja testimisse, mis võimaldas tal hinnata oma tooteid selliselt, mis annaks talle olulise eelise SolarWorld'i toodete ees. Küberrünnaku tulemusel langes SolarWorldi turuväärtusest 35%, mis tähendas 178 miljoni euro suurust kahjumit.[188] Kahju arvutamisel võrreldi ettevõtte aktsiahinda enne ja peale küberrünnakut.

Eelnevalt kirjeldatud riigivastaste küberrünnakute puhul saab rääkida võimalikust andmete kaotamise juhtumist Saudi Aramco küberrünnaku kontekstis, kui arvutiandmete hävimisega võis kaduma minna olulised puurimis- ja tootmisandmed.[189] Saudi Aramco on Saudi Araabia riiklik naftakompanii ning maailma suurim naftaeksportija, kelle naftaeksport moodustab 10% kogu maailmaturu ekspordist. Teadaolevalt ei tekkinud Saudi Aramcole puurimis- ja tootmisandmete kadumisest kahju, kuid võib eeldada, et puurimisandmete- ja tootmisandmed võivad, sarnaselt SolarWorld'i näitele, sisaldada tundlike ja konfidentsiaalseid andmeid, mille avaldumisel võib ettevõttele tekkida kahju. Riigivastutuse printsiibi kohaselt on kahju hüvitamise eesmärk kõrvaldada kõik kahjud, mis tekkisid õigusvastase teoga, ehk taastada olukord, mis oli enne rikkumist. Seega on oluline tuvastada rünnaku ja kahju vaheline põhjuslik seos. Kohtuasjas *Adminitrative Decision No.II* märkis, et põhjusliku seose hindamisel on oluline hinnata kahju vahetut mõju õigusvastase teoga. Kohus lisas, et põhjusliku seose analüüsimisel ei ole oluline kas kahju on tekkinud otseselt või kaudselt, seniks kui esineb selge ja katkematu sündmuste ahel õigusvastase teo ja kahju vahel. Oluline on, et sündmusteahel ei oleks katkenud ning kahju saab

[187] Ponemon Institute & Accenture (2017), *supra nota* 174, lk 29.
[188] The Council of Economic Advisers (2018), *supra nota* 177, lk 17.
[189] Bronk, C., Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. Survival. *Global Politics and Strategy*. Vol 55-2, 81.

selgelt, eksimatult ja kindlalt omistada rikkujale.[190] Antud seisukohta kinnitab ka ÜRO resolutsioon 687, mis sätestab et Iraan on vastutav otsese kahju eest, sealhulgas keskkonnakahju ja kahju loodusvarade ammendumisest. Samuti kahju eest mis on tekitatud välismaistele valitsustele, kodanikele või ettevõtetele, eeldusel, et kahju on tekkinud õigusvastase teo tagajärjel. Seega mahub andmete kaotusest tuleneb kahju riigivastutuse printsiibi kohaldamisalasse mille hüvitamist on riigil võimalik taotleda, eeldusel, et andmete kaotusest tekib ohvrile reaalne kahju ja seda suudetakse tõestada.

Järgmiseks väliseks kulukomponendiks küberkuritegevus kahjude hindamise metoodika kohaselt on äritegevuse häirimisest tulenev kahju. Tegemist on kahjuga, mis tuleneb organisatsiooni töö seiskumisest või tavapärase töömahu mittesaavutamises. Accenture ja Ponemon Instituudi uuringu kohaselt moodustab äritegevuse häirimine kulukomponendina küberrünnaku väliste tegurite kogu kahjust 33%.[191] Nagu eelnevalt mainitud mõjutas 2007. aastal Eesti riigi vastu suunatud küberrünnak enim valitsuse, presidendi, riigikogu ning välis- ja kaitseministeeriumi veebilehti. 34 % Eesti elanikkonnast teadis veebilehe www.eesti.ee kaudu pakutavate võrgupõhiste teenustest ning neid kasutas 19 % kogu elanikkonnast, mis on arvuliselt kuni 250 000 inimest. Seega leidsid e-teenused Eesti elanike seas laialdast kasutust. Nagu autor on eelnevalt selgitanud koosneb e-teenuste kasu vahetust rahalisest kasust, mis tuleneb kulude ja halduskoormuse vähenemisest, mis omakorda võimaldab vabanevat ressurssi kasutada uuendusteks, asjaajamise lihtsustamiseks või aja ja raha säästmiseks.[192] Katkestades e-teenuse toimimist kaotab riik kulude minieerimisest tuleneva kasuteguri, mille tagajärjel tõuseb organisatsiooni tööjõu- ja halduskulud (töömahu suurenemine tuleneb kasutajate arvust, kes tavaliselt kasutab e-teenust ning selle katkemise järel pöördub alternatiivsete meetodite poole). Seega kuulub materiaalse kahju alla suurenenud tööjõu- ja halduskulud, kui ka võimalikud kulutusted teenuse kättesaadavuse parandamiseks ja organisatsiooni tööprotsesside ja organisatsiooni juhtimise muutmises. Tegemist on seega kahjuga, mis häirib tavapärast organisatsiooni tööd ning mida on võimalik rahaliselt hinnata. Erinevus antud juhul avalik-õigusliku organisatsiooni ja ettevõttele tekkiva kahju puhul võib olla selle tekkimise viis. Riigiasutuse tegevust ei kuulu äritegevuse alla ning küberrünnaku kahju seisneb kulutuste suurenemises. Äritegevuse häirimine võib seisneda tootmismahu mitte saavutamises, mille tõttu võib ettevõttel jääda osa müügitulust saamata. Kuid olenemata kahju

[190] Cheng (1993), supra nota 86, lk 241-253.
[191] Ponemon Institute & Accenture (2017), *supra nota* 174, lk 29.
[192] Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis (2013), supra nota 138, lk 59.

tekkimise viisist, on võimalik antud kulukomponenti rakendada nii riigi kui ettevõtte vastu suunatud küberrünnaku kahju hindamisel.

Järgmiseks väliseks kulukomponendiks küberkuritegevus kahjude hindamise metoodika kohaselt on saamata jäänud tulu. Saamata jäänud tulu moodustab välise kulukomponendina Accenture ja Ponemon Instituudi uuringu kohaselt 21% küberrünnaku maksumusest. Küberkuritegevuse metoodika kohaselt hõlmab saamata jäänud tulu endas nii klientide kui investeerijate kaotusest tulenevat kahju, mis on tingitud arvutisüsteemide töös esinevatest viivitustest või nende sulgemisest. Antud metoodika võtmes seisneb saamata jäänud tulu ka maine kahjus. Üks kohtuasjadest, kus kohus rahuldas saamata jäänud tulu nõude oli *Cape Horn Pigeon*. Ameerika Ühendriikide lipu all sõitev vaalapüügi laev Cape Horn Pigeon peeti Okhotsk'i merel Venemaa sõjalaeva poolt kinni ning vabastati peale vaalapüügi hooaega. Kohus hüvitas vaalapüügist saamata jäänud tulu, võttes aluseks keskmise saagi hinna.[193] Suurbritannia ametivõimude poolt ebaseaduslikult kinni peetud Ameerika Ühendriikide laeva *Betsey* puhul, hüvitas hüvitas kohus saamta jäänud tulu, mis oleks kaubalaeva lasti müügist tulnud, kui laeva ei oleks kinni peetud.[194] Kohtuasjas *Libyan American Oil Company* hüvitas kohus saamata jäänud tulu, mis oleks tulnud petrooleumi müügist, kui ettevõtet ei oleks riigistatud.[195] Eelnevatest näidetest hoolimata on aga kohtud üldjuhul saamata jäänud tulu hüvitamisse suhtunud rangelt ning jätnud kahju hüvitamata nõuete korral, mida iseloomustavad spekulatiivsed elemendid. Materiaalse põhivaraga võrreldes on kasumid haavatavad kaubanduslikele ja poliitilistele riskidele. Kaasustes, kus saamata jäänud tulu on hüvitatud, on leidnud aset juhtudel, kus on võimalik piisava kindlusega tõdeda, et õigusvastase teo tagajärjel jäi tulu saamata. Taoline olukord on saavutatud lepinguliste kohustuste olemasolu tõestamisega või hästi väljakujunenud tehingute ajalooga, mis võimaldavad kindlusega tõdeda, et just õigusvastase teo tulemusel jäi tulu saamata.[196] Küberkuritegevuse kahjude hindamise metoodika võtab saamata jäänud tulu arvestamisel aluseks kaotatud kliendi ja aktsionäri väärtuse. Kulu arvutamisel lähtutakse kliendi „eluaegsest väärtusest" iga organisatsiooni puhul eraldi. Seega on küberkuritegevuse kahju hindamise metoodikal ja riigivastutuse printsiibi metoodikal saamata jäänud tulu arvutamiseks erinevad lähtepositsioonid. Riigivastutus printsiibi lähtekohaks on vara ning küberkuritegevuse metoodikal klient, mistõttu ei ole võimalik viimast kahju hindamise meetodit riigivastaste küberrünnakute kahjude hindamisel rakendada. Juhul, kui

[193] Kohtuotsus.R.I.A.A. 29.11.1902 Affaire des navires Cape Horn Pigeon, James Hamilton Lewis, C. H. White et Kate and Anna, vol. IX (Sales No. 59.V.5), p. 63.
[194] U.S. Supreme Court. 8 U.S. 443. The United States v. the Schooner Betsey and Charlotte, and her cargo, p. 113.
[195] Kohtuotsus. Ad Hoc Tribunal. Libyan American Oil Company v The Libyan Arab Republic. ILR, vol. 53, p. 140.
[196] United Nations (2008), *supra nota* 9, lk 104.

Saudi Aramco'le oleks küberrünnakuga tekkinud kahju ka saamata jäänud tulust, peaks naftakompanii sel juhul tõestama, et planeeritav tulu ei saabunud küberrünnakust tingitud tööprotsesside katkemise tõttu.

Küberkuritegevuse kahjude hindamise metoodika kohaselt on saamata jäänud tulu eelduseks maine kahju. Riigivastutuse printsiip käsitleb maine kahju saamata jäänud tulust eraldiseisva kahju liigina. Eelnimetatud printsiibi kohaselt, saab õigusvastase teoga tekkida riigile mittemateriaalne kahju. Kohtuasjas *Rainbow Warrior* märkis kohus, et Prantsusmaa õigusvastane tegu tekitas Uus-Meremaal viha ja avalikku pahameelt, põhjustades seega täiendava mittemateriaalse kahju – mis oli moraalset, poliitilist ja õiguslikku laadi ning mis väljendus mitte ainult Uus-Meremaa riigi üldise, vaid ka riigi kõrgeimate kohtu- ja täidesaatva ametivõimude maine kahjustamises.[197] Riigile tekkinud mainekahju puhul on tegemist mittemateriaalse kahjuga, mis tekib rahvusvahelise kohustuse rikkumisest. Mittemateriaalse kahju juhtumid rahvusvahelises praktikas hõlmab rikkumisi, mis seisnevad riigi sümboli solvamises, suveräänsuse ja territoriaalse terviklikkuse rikkumises, riigile kuuluvate laeva või õhusõidukite ründamises, riigipeade või tähtsate ametnike väärkohtlemises või ründamises ning saatkondade ja konsulaatide puutumatuse rikkumises.[198] 2007. aastal Eesti riiki tabanud küberrünnaku ohvriks langesid kõik suuremad meediaväljaandeid. Eesti valitsus tugines teabe jagamiseks veebipõhisele keskkonnale, mida ka rahvusvahelised meediaorganisatsioonid laialdaselt kasutasid. Küberrünnete tõttu oli osaliselt takistatud informatsiooni jagamine, mistõttu ei saanud inimestele edastada informatsiooni küberründega põhjustatud häiretest. Lisaks mõjutasid küberrünnakud ka riigi infovoogu välismaale. Arvestades, et riigi meediaväljaannete tegevus, sealhulgas riigi poolse informatsiooni edastamine oli takistatud, võib inimestes tekitada pahameelt, mõjutades seega inimeste usaldust nii valitsuse, kui ka riigi vastu üldiselt. Sarnaselt *Rainbow Warrior* kohtuasjale, saab ka siinjuhul rääkida mittemateriaalsest kahjust, mis on oma olemuselt moraalset, poliitilist ja õiguslikku laadi ning mille hüvitamist on võimalik nõuda, ilma, et oleks tekkinud materiaalset kahju. Küberkuritegevuse metoodika hindab maine kahju seoses saamata jäänud tuluga, sidudes mõlemad üheks kulukomponendiks. Autor leiab, et küberkuritegevuse kahjude hindamise metoodika ei võimalda hinnata riigile tekkinud maine kahju. Riigivastutuse õiguse kohaselt, saab riigile tekkida mainekahju ka ilma materiaalse kahju esinemiseta.

[197] Rainbow Warrior (1990), supra nota 23, p 23.
[198] United Nations (2008), supra nota 9, lk 104.

Järgmiseks väliseks kulukomponendiks on seadmetele tekitatud kahju. Accenture ja Ponemon Instituudi uuringu kohaselt moodustab seadmetele tekitatud kahju 3% küberrünnaku maksumusest. Seadmetele tekitatud kahju kulukomponent hõlmab kahjustada saanud seadmete ning infrastruktuuri asendamisest ning parandamisest tulenevat kulu. Stuxnet arvutiviiruse tagajärjel läks hinnanguliselt uraanirikastamise jaamas ära vahetamisele kuni 1000 gaasitsentrifuugi. Saudi Aramco vastase küberrünnaku tagajärjel vahetas naftakompanii välja kuni 30 000 arvutit ning 2015 aastal Prantsusmaa riikliku televisoonivõrgu vastase küberrünnaku tagajärjel olid ettevõtte kõik arvutisüsteemid suletud. Seadmetele tekitatud kahju on võimalik kulukomponendina kohalda riigivastase küberrünnaku korral.

3.2.2 Organisatsiooni sisesed tagajärjed

Küberrünnaku kahjude hindamise metoodika kohaselt on sisesteks kulukomponentideks tuvastamine ja uurimine, kahjude minimeerimine, taastamine ning küberrünnaku järgsed tegevused. Riigivastutuse printsiibi kohaselt on vastutav riik kohustud hüvitama õigusvastase teo toimepanemise tagajärjed. Kohustuse ulatus on piiritletud kahjuga, mida on võimalik rahaliselt hinnata. Rahaliselt hinnatav kahju hõlmab nii riigile endale kui ka tema kodanikele põhjustatud kahju, sealhulgas kulud, mis on seotud õigusevastase teost tulenevate kahjude leevendamise ja parandamisega. Riigile tekitatud kahju võib väljenduda kuludes, mis on tekkinud reageerides reostuskahjudele ja ettenägematutele kahjudele, mis tuleneb näiteks pensioni maksmise vajadusest või ravikulude tasumisest.[199] Kohtuasjas *Corfu Channel* rahuldas kohus Suurbritannia taotluse ning kohustas Albaaniat maksma kompensatsiooni 840 000 naelsterlingi eest. Suurbritannia taotles materiaalse kahju hüvitamist Kuningliku mereväe S-klassi hävitaja „Saumarez“ hävimise, kahjustada saanud seadmete ja tehtud töö eest hävitajal „Volage“ ning viga saanud laeva meeskonna pensionide, ravikulude ja halduskulude eest.[200] Kohtuasjas *M/V “Saiga” (No. 2)* rahuldas kohus kompensatsiooni kaebuse, kus kulukomponentideks olid laevale tekitatud kahjustused, laeva remontimisest ja kinnipidamisest tulenev kahju, laeva meeskonnaliikmete kinnipidamisest ning äritegevuse takistamisest tulenev kahju.[201] Seega leiab autor, et sisemisi kulukomponente (tuvastamine ja uurimine, kahjude minimeerimine ning taastamine) on võimalik kohaldada ka riigi vastu toime pandud küberrünnakute kahjude hindamisel ning need on kooskõlas riigivastutuse printsiibi kahju käsitlusega.

[199] United Nations (2008), supra nota 9, lk 105.
[200] Kohtuotsus, ICJ. 1949. Corfu Channel (Suurbritannia v. Albaania), GL No 1, ICJ Rep 4, ICGJ 199, p. 249.
[201] Kohtuotsus. R.I.I.A. 01.07.1999. The M/V “Saiga” (No. 2) case (Saint Vincent and the grenadines v. Guinea), p. 176.

Järgmiseks sisemiseks kulukomponendiks on küberrünnaku järgsed tegevused, mis aitavad organisatsioonil minimeerida tulevikus aset leidvaid rünnakuid. Sisaldab uute tehnoloogiate ja süsteemide lisamise kulusid. Andmelekete kahjude hindamise metoodika järgselt kuuluvad küberrünnaku järgsetesse tegevustesse ka auditite läbiviimine, isikuandmete kaitse teenused ning juriidilised teenused.[202] Riigivastutuse printsiibi kahjukäsitlus välistab igasuguse abstraktse kahju, nagu riigi üldised huvid. Küberkaitse võimekuse arendamine järgib riigi üldisi huve, mille arendamine toimub ka ilma küberrünnaku ohvriks olemast. Kohtuasjas *Adminitrative Decision No.II* selgitas kohus, et põhjusliku seos eeldab selget ja katkematut sündmuste ahelad õigusvastase teo ja kahju vahel, mis antud juhul ei ole täidetud.[203] Seega ei ole võimalik kahju selgelt, eksimatult ja kindlalt omistada rikkujale. Autori hinnangul jääb antud kuluartikkel riigivastutuse printsiibi kahju käsitlusest välja ning seda ei ole võimalik kasutada riigivastaste küberrünnakute kahjude hindamisel.

3.3.Kahju hüvitamise eeldused

3.3.1 Seadmetele tekitatud kahju ja kaotatud andmetest tulenev kahju

Nagu autor on varasemalt tõdenud võib küberrünnaku tagajärjel tekkida varaline kahju. Varaline kahju riigivastutuse õiguse kohaselt hõlmab mis tahes rahaliselt hinnatavat kahju. Seega on varalise kahju hüvitamise esimeseks eelduseks kahju rahaline hinnatavus. Rahaliselt hinnatav kahju hõlmab riigi (sh ametnikele) või diplomaatilise kaitse all olevate isikutele tekitatud kahju. Küberrünnakute nagu Stuxnet, Saudi Aramco, TV5 Monde ja Ukraina puhul on kahju rahaliselt hinnatavuse eeldus täidetud.

Teine oluline eeldus varalise kahju hüvitamiseks on põhjuslik seos. Kohtuasjas *Adminitrative Decision No.II* märkis kohus, et põhjusliku seose hindamisel on oluline hinnata kahju vahetut mõju õigusvastase teoga. Kohus lisas, et põhjusliku seose analüüsimisel ei ole oluline kas kahju on tekkinud otseselt või kaudselt, seniks kui esineb selge ja katkematu sündmuste ahel õigusvastase teo ja kahju vahel. Oluline on, et sündmusteahel ei oleks katkenud ning kahju saab selgelt, eksimatult ja kindlalt omistada rikkujale.[204] Rahvusvahelised kohtud on siinkohal põhjusliku seose

[202] Ponemon Institute. (2017), supra nota 178, lk 30.
[203] Cheng (1993), supra nota 86, lk 241-253.
[204] Cheng (1993), supra nota 86, lk 241-253.

kirjeldamiseks kasutanud termineid nagu „otsesus“, „prognoositavus“ ning „vahetu“.[205] Autori hinnangul on ka põhjuslikuse seose eeldus täidetud.

3.3.2 Saamata jäänud tulu ja äritegevuse häirimine

Varalise kahju hüvitamise eelduseks saamata jäänud tulu ja äritegevuse häirimise puhul on põhjusliku seose olemasolu. Kaasustes, kus saamata jäänud tulu on hüvitatud, on leidnud aset juhtudel, kus on võimalik piisava kindlusega tõdeda, et õigusvastase teo tagajärjel jäi tulu saamata. Taoline olukord on saavutatud lepinguliste kohustuste olemasolu tõestamisega või hästi väljakujunenud tehingute ajalooga, mis võimaldavad kindlusega tõdeda, et just õigusvastase teo tulemusel jäi tulu saamata.[206] Ameerika Ühendriikide lipu all sõitev vaalapüügi laev Cape Horn Pigeon peeti Okhotsk'i merel Venemaa sõjalaeva poolt kinni ning vabastati peale vaalapüügi hooaega. Kohus hüvitas vaalapüügist saamata jäänud tulu, võttes aluseks keskmise saagi hinna.[207] Suurbritannia ametivõimude poolt ebaseaduslikult kinni peetud Ameerika Ühendriikide laeva *Betsey* puhul, hüvitas hüvitas kohus saamta jäänud tulu, mis oleks kaubalaeva lasti müügist tulnud, kui laeva ei oleks kinni peetud.[208] Kohtuasjas *Libyan American Oil Company* hüvitas kohus saamata jäänud tulu, mis oleks tulnud petrooleumi müügist, kui ettevõtet ei oleks riigistatud.[209]

3.3.3 Tuvastamise, uurimise, kahjude minimeerimise ning taastamisega seotud kulud

Rahaliselt hinnatav kahju hõlmab nii riigile endale kui ka tema kodanikele põhjustatud kahju, sealhulgas kulud, mis on seotud õigusevastase teost tulenevate kahjude leevendamise ja parandamisega. Kohtuasjas Corfu Channel rahuldas kohus Suurbritannia taotluse ning kohustas Albaaniat maksma kompensatsiooni 840 000 naelsterlingi eest. Suurbritannia taotles materiaalse kahju hüvitamist Kuningliku mereväe S-klassi hävitaja „Saumarez“ hävimise, kahjustada saanud seadmete ja tehtud töö eest hävitajal „Volage“ ning viga saanud laeva meeskonna pensionide, ravikulude ja halduskulude eest. Kohtuasjas M/V "Saiga" (No. 2) rahuldas kohus kompensatsiooni kaebuse, kus kulukomponentideks olid laevale tekitatud kahjustused ja remontimis kulud. Kahjude leevendamise ja prandamisega seotud kulud võivad seotud olla ka reostuskahjude likvideerimisega või ettenägematute kulutustega, milleks võib olla pension. või

[205] United Nations (2008), *supra nota* 9, lk 105.
[206] Ibid., lk 105.
[207] Kohtuotsus.R.I.A.A. 29.11.1902 Affaire des navires Cape Horn Pigeon, James Hamilton Lewis, C. H. White et Kate and Anna, vol. IX (Sales No. 59.V.5), p. 63.
[208] U.S. Supreme Court. 8 U.S. 443. The United States v. the Schooner Betsey and Charlotte, and her cargo, p. 113.
[209] Kohtuotsus. Ad Hoc Tribunal. Libyan American Oil Company v The Libyan Arab Republic. ILR, vol. 53, p. 140.

ravikulude hüvitamine. Autori hinnangul on antud kulukomponent täidetud iga küberrünnaku juhtumil, kus on tekkinud varaline kahju.

3.3.3 Mainekahju

Riigivastutuse eelnõu artikkel 37 sätestab, et õigusvastase teo eest vastutav riik on kohustatud hüvitama mittevaralise kahju, kuivõrd seda ei ole võimalik kõrvaldada varalise kahju hüvitamise või ennistamise korral. Mittevaralise kahju hüvitamine hõlmab neid kahjusid, mida ei ole võimalik rahaliselt hinnata, teisisõnu riigile tekitatud moraalne kahju. Mittevaralise kahju hüvitamise nõude eelduseks on, et kahju ei ole võimalik muu kahju hüvitamise vormiga täielikult kõrvaldada. Mittevaralise kahju hüvitamine võib toimuda ka rahalise hüvitisena. Et mittevaralise kahju hüvitamist saaks nõuda rahalise maksena, peab riigil esinema moraalne kahju. Kohtuasjas Rainbow Warrior otsustas kohus, et Prantsusmaa peab Uus-Meremaale maksma 7 miljonit dollarit mittevaralise kahju vormis, mis ületas oluliselt varalise kahju ulatuse. Seega kuuluvad antud peatüki alla rikkumised mis on oma olemuselt sümboolsed, olenemata ohverriigile tekkinud materiaalsetest kahjustustest.[210] Moraalse kahju näidetena saab tuua juhtumeid, kus on solvatud riigi sümboleid, rikutud riigi suveräänsust ja territoriaalset terviklikust, väärkoheldud riigi diplomaatilisi esindajaid või valitsusjuhte ning rikutud saatkondade või konsulaatide puutumatust.[211]

Artikli kolmas lõige kirjeldab heastamise nõude piire, sätestades kaks tingimust: esiteks peab olema heastamise nõue olema proportsionaalne tekkinud kahjuga ning teiseks ei tohi nõue olla vastutavale riigile alandav. Riigivastutuse eelnõu kommentaarid tõdevad, et mõiste „alandav“ on ebatäpne, kuid selliseid juhtumeid on ajaloo vältel juhtunud.[212]

[210] United Nations (2008), supra nota 9, lk 105.
[211] United Nations (2008), supra nota 9, lk 106.
[212] *Ibid*., lk 107.

KOKKUVÕTE

Rahvusvaheliste suhete puhul, nagu ka kõikide teiste sotsiaalsete suhete korral, toob õigussubjekti õiguste rikkumine kaasa rikkuja poolse vastutuse. Traditsioonilise teooria kohaselt kujutab riigivastutus endas õigussuhet, kus õigusvastase teo toimepanijal on kohustus hüvitada tekitatud kahju ning õigustatud riigil on õigus kahju hüvitamiseks. Tänapäevast riigivastutuse käsitlust iseloomustab kõige paremini riigivastutuse eelnõu artikkel 1, mis ütleb, et iga rahvusvahelise õiguse vastane tegu toob endaga kaasa riigi vastutuse. Rahvusvahelise õigusvastase teo olemasolu teine tingimus on see, et riigile omistatav käitumine peab rikkuma selle riigi rahvusvahelisel tasandil võetud kohustust.

Rahvusvahelise tavaõiguse kohaselt tekib rahvusvahelise õigusvastase teo toimepanemisel kohustus tekitatud kahju hüvitada. Kahju hüvitamise eesmärk on esmajärjekorras olukorra taastamine, mis oleks valitsenud, kui ei oleks toimunud rahvusvahelise kohustuse rikkumist. Seega on kahju hüvitamine suunatud primaarsete kohustuste täieliku täitmise tagamisele ja rikkumise tagajärjel tekkinud kahju kompenseerimiseks. Mõiste „kahju“ tähendab igasugust kahju, mille on põhjustanud õigusvastane tegu, hõlmates mis tahes tekkinud materiaalset või moraalset kahju, kuid välistades igasuguse abstraktse kahju, millel ei ole kindlat alust.

Enamasti toetutakse küberrünnakute õiguslikul hindamisel ÜRO põhikirja artiklile 2 (4), mille kohaselt on jõu kasutamine rahvusvahelistes suhetes keelatud. Artikkel 2 (4) sätestatud jõu kasutamise keeldu peetakse rahvusvahelise õiguse imperatiivnormiks, mille rahvusvaheline riikide ühendus on omaks võtnud ja tunnustab tervikuna kui normi, millest kõrvalekaldumine on lubamatu ja mida võib muuta ainult järgneva samasuguse iseloomuga üldise rahvusvahelise õiguse normiga. Riigi poliitiline ja majanduslik sfäär on aga kaitstud mittesekkumise printsiibiga, mida loetakse sarnaselt jõu kasutamise keeluga rahvusvaheliseks imperatiivnormiks. Õigusteadlased on mõtestanud interventsiooni kui sekkumist teiste riikide sise- või välisasjadesse. Mittesekkumise printsiibi rikkumine võimaldab riigil tugineda riigivastutuse printsiibist tulenevale kahju hüvitamise õigusele. Antud töö eesmärk on välja selgitada, kuidas hinnata poliitilist laadi küberrünnakute tekitatud kahju, ning analüüsida kas hüvitamisele kuuluvat kahju tekib või mitte.

Riigivastutuse eelnõu artikkel 34 näeb ette kolm kahju hüvitamise vormi: ennistamine, varalise ning mittevaralise kahju hüvitamine. Kahju hüvitamise eesmärk on täielikult kõrvaldada õigusvastase teo tagajärjel tekkinud kahju, kas ühe või mitme kahju hüvitamise vormi koosmõjus. Täielikult kahju kõrvaldamine eeldab tekitatud kahju suuruse ja ulatuse täpset tuvastamist. Kahju hindamine õigusvastase teo puhul, mille tagajärjel tekib ainult materiaalne kahju ei valmista probleeme, kuna mõju avaldub üldjuhul ainult füüsilises keskkonnas. Küberrünnaku kahjud võivad ulatuda aga füüsilisest keskkonnast kaugemale, mõjutades nii füüsilist keskkonda, seadmetes sisalduvaid andmeid ja informatsiooni kui ka üldist elukeskkonda. Küberründed demokraatlike protsesse võimaldava tehnoloogia vastu võivad kahju tekitada aga kõikides eelnimetatud valdkonnas, muutes nendest tekkinud kahju hindamise keeruliseks.

Enamasti toetutakse küberrünnakute õiguslikul hindamisel ÜRO põhikirja artiklile 2 (4), mille kohaselt on jõu kasutamine rahvusvahelistes suhetes keelatud. Õigusteadlased on võtnud seisukoha, et küberrünnakut saaks liigitada jõua kasutamise alla, peab küberrünnakul esinema kineetilise-, bioloogilise- või keemiarelvaga sarnane mõju. Antud seisukohta kinnitavad ka ÜRO Peaassamblee resolutsioonid, mis ei näe poliitilist ja majandusliku sunni rakendamist kui „jõu“ kasutamist. Riigi poliitiline ja majanduslik sfäär on kaitstud mittesekkumise printsiibiga, mida loetakse sarnaselt jõu kasutamise keeluga rahvusvaheliseks imperatiivnormiks. Õigusteadlased on mõtestanud interventsiooni kui sekkumist teiste riikide sise- või välisasjadesse. Mittesekkumise printsiibi rikkumine võimaldab riigil tugineda riigivastutuse printsiibist tulenevale kahju hüvitamise õigusele. Antud töö kontekstis defineeritakse küberrünnak kui midagi, mis hõlmab riigi poolset tegevust, millega tungitakse teise riigi arvutisüsteemidesse ning sissetungimise tagajärjel tekib kahju.

Kolmandas peatükis keskendub autor küberrünnakute kahjude analüüsimisele. Autor analüüsib nelja erinevat küberrünnak liiki tuvastamaks millist laadi kahju nende tagajärjel tekkida võib. Autor on analüüsis lähtunud Välisasjade komisjoni uuringust, mille kohaselt on 4 peamiseks riigivastaseks küberrünnakuks teenustõkestusrünnak, näotustamine, sabotaaž ja andmete hävitamine. Järgnevalt tutvustab autor küberkuritegevuse kahjude hindamise metoodikat ning kontrollib selle asjakohasust riigivastastele küberrünnakutele. Autor on jõudnud seisukohani, et küberkuritegevuse kahjude hindamise metoodikat on võimalik osaliselt kohaldada riigivastastele küberrünnakutele.

SUMMARY

EVALUATION OF DAMAGED CASUED BY NON-MILITARY CYBER-ATTACKS BASED ON THE NON-INTERVENTION PRINCIPLE

Andres Vaet

Modern day society keeps on challenging the parties concerned, everyday. No matter the role or position, most possibly one has had to face the obstacles that modern day society's core, the cyberspace, has thrown at their feet. Regarding the aformentioned, the given paper aims to find answer to the question, how to assess the damages caused using modern day weapons – cyberattacks - which in turn includes an analyze whether the damages caused by the attacks are subject to compensation. The work research methodology includes an analysis of whether it is possible to solve the new legal problems arising in today's world with already existing principles of international law or does the international law society has to come up with new concepts to fit the law in cyberspace. This Master's thesis consists of three chapters, the first chapter of which opens the concept of state responsibility and explains the history of the formation of the principle in international law. In the second chapter the author analyzes the theory of damages and case law and the third chapter includes an analysis of damage assessment. This is a qualitative study in which the research process is the interpretation of international treaties, the study of the principles of international law, the definition of concepts, the analysis of judicial decisions and the study of legal texts.

Based on the law of the state, the author examined what are the exact tools that the countries which have fallen under a politically motivated attack can put into practice to protect their rights and which are the prerequisites for the implementation of these instruments. The aim of the work is also to explain how to assess the damage caused by political cyber attacks and whether

damages will be subject to compensation. In 2017, more than 10,000 cybercrime cases were registered in Estonia of which a quarter had direct impact on the confidentiality, availability and integrity of information or systems. Modern day society keeps on challenging the parties concerned, everyday. No matter the role or position, most possibly one has had to face the obstacles that modern day society's core, the cyberspace, has thrown at their feet. Regarding the aformentioned, the given paper aims to find answer to the question, how to assess the damages caused using modern day weapons – cyberattacks - which in turn includes an analyze whether the damages caused by the attacks are subject to compensation.

The work research methodology includes an analysis of whether it is possible to solve the new legal problems arising in today's world with already existing principles of international law or does the international law society has to come up with new concepts to fit the law in cyberspace. This Master's thesis consists of three chapters, the first chapter of which opens the concept of state responsibility and explains the history of the formation of the principle in international law. In the second chapter the author analyzes the theory of damages and case law and the third chapter includes an analysis of damage assessment. This is a qualitative study in which the research process is the interpretation of international treaties, the study of the principles of international law, the definition of concepts, the analysis of judicial decisions and the study of legal texts.

In 2017, two major malicious campaigns WannaCry and Petya / NotPetya shook the world. WannaCry infected about 400,000 devices and the estimated losses are calculated aproximately up to $ 4 billion. The cyber attack hit more than 600 healthcare facilities in the United Kingdom alone, with North Korea believed to be behind the cyber attack. Petya / NotPetya infected up to 20,000 different devices and caused an estimated $ 1.2 billion in damage. In February this year, the United States Government attributed responsibility to the Russian government and the military. According to a survey made in 2017, losses caused by cybercrimes are calculated aproximately up to $ 600 billion a year. Thus, it can be concluded that cyber-attacks have a significant impact on the economy and also on democratic processes. The author concentrates on four different type of cyber attacks, which, according to the statistics of the Foreign Affairs Committee, have been committed against the state. The author compared the types of attacks with the Draft articles on Responsibility of States for Internationally Wrongful acts and case law and concludes that according to the principle of non-intervention, the damage caused by cyber attacks can be compensated on the basis of the principle of state responsibility.

KASUTATUD ALLIKATE LOETELU

Teadusraamatud:

1. Brownlee, I. (2003). Principles of Public International law. Fifth Edition. New York: Oxford University Press.
2. Land. K. (2002). Rahvusvaheline vastutus. Rahvusvaheline õigus. Tallinn: Juura.
3. Kaczorowska, A. (2010) Public International Law. The fourth editition. London: Routledge.
4. Shaw, M. N. (2008). International law. Sixth Edition. Cambridge: Cambridge Univesity Press.
5. Shaw, M.N. (1997). International Law. Fourth edition, Cambridge (UK). Cambridge University Press.
6. Tallinn Manual 2.0 on the International law applicable to cyber operations. (2013). /Eds. Schmitt, M.N., Vihul, L. London. Cambridge Univesity Press.

Teadusartiklid:

7. Cheng, B. 1993. General Principles of law as applied by International Courts and Tribunals. New York: Cambridge University Press.
8. Stern, B. The obligation to make reparation. The law of International responsibility. Oxford commentaries on International law. New York: Oxford university press.564-571.
9. Bories, C. (2010). The Hague conference of 1930“ The law of International responsibility. Oxford commentaries on International law. New York: Oxford university press.
10. Momtaz, D. (2010). Attributin of conduct to the state: state organs and entities empowered to exercise elements of govermental authority. The law of International responsibility. Oxford commentaries on International law. New York: Oxford University Press.
11. Shelton, D. (2009). Reparations. Max Planck Encyclopedia of Public International Law, Volume VIII. Max Planck Insitute for Comparative Public Law and International Law. New York: Oxford University Press.
12. Tonkin, H. (2011) State Control over Private Military and Security Companies in Armed Conflict. New York, Cambridge University Press.
13. Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A. Perdue, W., Spiegel, J. (2012). The Law of Cyber-Attack. California Law Review.
14. Hoss, C., Villalpando, S., Sivakumaran, S. (2012) Nicaragua: 25 years Later. Leiden Journal of International Law.
15. Crawford, J. (2010). The system of International responsibility. Oxford commentaries on International law. New York: Oxford University Press.
16. Crawford, J. (2012). State Responsibility. Max Planc Encoclopedia of Public International Law. Volume IX.
17. Crawford, J. (2013). State Responsibility. In State Responsibility: The General Part (Cambridge Studies in International and Comparative Law, p. I). Cambridge: Cambridge University Press.

18. Shen, J. 2001. The Non-Intervention Principle and Humanitarian Interventions under International Law, 7 Int'l Legal Theory 1. HeinOnline.
19. Dimitrovska, M. (2015) The concept of International responsibility of state in the International public law system. Journal of Liberty and International Affairs Vol. 1, No. 2.
20. Jamnejad, M., Wood, M. (2009). Current Legal Developments. The Principle of Non-Intervention. Leiden Journal of International Law.
21. Wood, M., Pronto, A. (2010). The international law commission 1999-2009. Volume IV: Treaties, final draft articles and ohter meterials. New York: Oxford University Press.
22. Aloupi, A. (2015). The Right to Non-intervention and Non-interference, 4 Cambridge J. Int'l & Comp. L. 566.
23. Kunig, P. (2008). Prohibition of intervention. Max Planck Encyclopedia of Public International law.
24. Argent, P. (2009). Reparations after World War II. The Max Planck Encyclopedia of Public International Law, Volume VIII. Max Planc Institute for Comparative Public Law and International Law. New York: Oxford University Press.
25. Pellet. A. (2010). The ICL articles on state responsibility for internationally wrongful acts and related texts. The law of International responsibility. Oxford commentaries on International law. New York: Oxford university press.
26. Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions, 17 J. Conflict & Sec. L.
27. Stern, B. (2010). The elements of an internationally wrongful act. The Law of International Responsibility. Oxford commentaries on International law. New York: Oxford university Press.
28. Mattessich, W. (2016). Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage. Columbia Journal Of Transnational Law. No. 54:873.
29. Vida, M.A.J. (2005). Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places, 51 Naval L. Rev.
30. Bronk, C., Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. Survival. Global Politics and Strategy. Vol 55-2.
31. Lindsay, J.R. (2013). Stuxnet and the Limits of Cyber Warfare, Security Studies. Vol 22-3.
32. Margulies, P. (2013). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. Melbourne Journal of International Law. Vol 14. No. 496.
33. Nguyen, R. (2013). Navigating Jus Ad Bellum in the Age of Cyber Warfare. California Law Review. Vol 101-4.
34. O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. Trinity College Law Review. Vol 16.
35. Farwell, J.P., Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival. Global Politics and Strategy. Vol. 53, 24.
36. Achieve Energy Security and Sustainability. George Washington journal of energy & environmental law. Vol 8-2.

EL-i ja rahvusvahelised õigusaktid:

37. Euroopa Parlamendi ja nõukogu 8. detsember 2008 aasta direktiiv 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta.
38. Euroopa Parlamendi ja nõukogu 27. aprill 2016 määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).
39. Euroopa Parlamendi ja nõukogu 6. juuli 2016 direktiiv meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.
40. Montevideo Convention on the Rights and Duties of States, 26.12.1933, Montevideo.

Rahvusvahelised kohtulahendid:

41. Kohtuotsus, PCIJ. 26.07.1927, Factory at Chorzow, (Saksamaa v Poola). (ser. A), No. 9.
42. Kohtuotsus, PCIJ. 14.07.1938, Phosphates in Morocco, (Itaalia v Prantsusmaa), A/B No 74.
43. Kohtuotsus, Prantsuse-Uus-Meremaa Arbitraaži Tribunal. 30.04.1990, Rainbow warrior (Uus-Meremaa vs Prantsusmaa), 82 I.L.R. 500.
44. Kohtuotsus, R.I.A.A. 1931. Dickson Car Wheel Company (Ameerika Ühendriigid v. Mehhiko), No.669.
45. Kohtuotsus, R.I.A.A. 1931. International Fisheries Company (Ameerika Ühendriigid v. Mehhiko), No. 691.
46. Kohtuotsus, R.I.A.A. 1924. British Claims in the Spanish Zone of Morocco (Suurbritannia vs Hispaania), No. 615.
47. Kohtuotsus, R.I.A.A. 1953. Armstrong Cork Company (Ameerika Ühendriigid vs Itaalia), No. 159.
48. Kohtuotsus, ICJ. 1949. Corfu Channel (Suurbritannia v. Albaania), GL No 1, ICJ Rep 4, ICGJ 199.
49. Kohtuotsus, PCIJ. 1980. United States Diplomatic and Consular Staff in Tehran (Ameerika Ühendriigid vs Iraan), No.64.
50. Kohtuotsus, PCIJ. 1930.Greco-Bulgarian “Communities“. Advisory Opinion. Series B, No. 17.
51. Kohtuotsus, R.I.A.A. Claim of the Salvador Commercial Company ("El Triunfo Company") (El Salvador vs Ameerika Ühendriigid) No.15.
52. Kohtuotsus, R.I.A.A. 1926. Youmans (Ameerika Ühendriigid vs Mehhiko), 4 R.I.A.A. 110.
53. Kohtuotsus, R.I.A.A 08.05.1872. Alabama arbitration (Suurbritannia v Ameerika Ühendriigid). Reports of International Arbitral awards. Volume XXIX, pp.125-134.
54. Behrami and Behrami v. France and Saramati v. France, Germany and Norway. ECHR 02.05 2017.
55. Kohtuotsus. R.I.I.A 1931. Chevreau (Prantsusmaa v Suurbritannia), 2 RIIA 1113.
56. X and Y v Switzerland. 20 ECHR 1977.
57. Kohtuotsus, R.I.A.A. 1929. Jean-Baptiste Caire Claim (Prantsusmaa v Mehhiko). 5 R.I.A.A 516.
58. Kohtuotsus, ICJ. 27.06.1986. the case concerning Military and Paramilitary Activities in and against Nicaragua brought by Nicaragua against the United States of America, I.C.J. 39.

59. Kohtuotsus. ICTY Appeals Chamber, 15.07.1999, Prosecutor v. Duško Tadic. No. IT-94-1-A.
60. Kohtuotsus, ICJ. 1997.Gabcikovo-Nagymaros Project (Ungari v Slovakkia) I.C.J. 7.
61. Kohtuotsus. Prantsusmaa - Uus-Meremaa Arbitraaži Tribunal. 1990. Rainbow warrior (Uus-Meremaa v Prantsusmaa), 82 I.L.R. 500.
62. Kohtuotsus. R.I.I.A. 31.07.1928. Portuguese Colonies case (Naulilaa incident), 2 RIIA 1011.
63. Kohtuotsus. Iraan-Ameriika Ühendriikide Arbitraaži Tribunal. 28.12.1998 in The Islamic Republic of Iran v. The United States of America cases A15 (IV) and A24. No. 590–A15 (IV)/A24–FT.
64. Kohtuotsus, R.I.A.A. 2009. Ethiopia's Damages Claim (Eritrea vs Etioopia). No. 2001-02.
65. Kohtuotsus. Kreeka-Saksamaa Arbitraaži Kohus. 1926. Antippa (The Spyros). No. 285.
66. Kohtuotsus. ICJ. 1962. Temple of Preah Vihear Case (Kamboodža v Tai), ICGJ 160.
67. Kohtuotsus. P.C.I.J. 1933. Legal Status of Eastern Greenland case. Series A/B, No. 53.
68. Kohtuotsus. ICJ . 1996. Aerial Incident of 3 July 1988 (Iraan v. Ameerika Ühendriigid), No. 674.
69. Otsus. ICSID. 1990. Asian Agricultural Products v Sri Lanka. No. ARB/87/3.
70. Kohtuotsus. PCIJ. 04.04.1928. Island of Palmas (Ameerika Ühendriigid v Madalmaad), 2 U.N. Rep. Intl. 4rb. Awards 829.
71. Kohtuotsus.R.I.A.A. 29.11.1902 Affaire des navires Cape Horn Pigeon, James Hamilton Lewis, C. H. White et Kate and Anna, vol. IX (Sales No. 59.V.5).
72. Kohtuotsus. Ad Hoc Tribunal. Libyan American Oil Company v The Libyan Arab Republic. ILR, vol. 53.
73. U.S. Supreme Court. 8 U.S. 443. The United States v. the Schooner Betsey and Charlotte, and her cargo.
74. Kohtuotsus. R.I.I.A. 01.07.1999. The M/V “Saiga” (No. 2) case (SAINT VINCENT AND THE GRENADINES v. GUINEA), p. 176.

Muud allikad:

75. Alford, T.J. (2017). Off the Grid: Facilitating the Acquisition of Microgrids for Military Installations to
76. Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis. (2013). E-teenuste kasutamise tulemuslikkus ja mõju. (Toim.) Kalvet, T., Tiits, M., Hinsberg, H. Tallinn. Kättesaadav: http://www.praxis.ee/fileadmin/tarmo/Projektid/Valitsemine_ja_kodanike%C3%BChiskond/E-teenuste_kasutamise_tulemuslikkus_ja_moju.pdf 13.05.2018.
77. BBC News. (2010). Baidu hacked by 'Iranian cyber army'. – 12. Jaanuar.
78. BBC News. (2011). South Korea hit by cyber attacks. – 4. Märts.
79. BBC News. (2017). Qatar crisis: What you need to know. – 19. Juuli.
80. Brangetto, P., Veenendaal, M.A. (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. 8th International Conference on Cyber Conflict. (Toim.). Pissanidis, N., Rõigas, H., Veenendaal, M.A. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 122.
81. Braningan, T. (2013). South Korea on alert for cyber-attacks after major network goes down. – The Guardian, 20. Märts.

82. Broad, W.J., Markoff, J. Sanger, D.E. (2011), Israeli Test on Worm Called Crucial in Iran Nuclear Delay. – The New York times, Jaanuar 15.
83. Campbell, J. (2015). French TV network TV5Monde 'hacked by cyber caliphate in unprecedented attack' that revealed personal details of French soldiers. – Independent, 9. April.
84. Center for Strategic and International Studies & McAfee. (2018). Economic Impact of Cybercrime — No Slowing Down. Report. Kättesaadav: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70- 13.05.2018.
85. Center for Strategic and International Studies & McAfee. (2018). Economic impact of Cybercrime – No slowing down. Report. Kättesaadav: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70- 13.05.2018.
86. Chung, L. (2007), Beijing seeks Taiwanese secret agent over hacking. – South China Morning Post, 1. November.
87. Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations [in the following referred to as Friendly Relations Declaration], UN GA Res. 2625 [XXV] of 24 October 1970, Annex, Principle 1.
88. Deyoung, K., Nakashima, E. (2017). UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials. – The Washington Post, 16. Juuli.
89. Draft articles on Responsibility of States for Internationally Wrongful Acts: with commentaries. Uniten Nations 2008.
90. Ghandi, R., Sharma, A., Mahoney, W., Sousan, W,. Zhu, Q., Laplante, P. 2011. Dimensions of Cyber-Attacks. Social, Political, Economic and Cultural. Ieee Technology And Society Magazine. Spring 2011.
91. Greenberg, A. (2018). The White House blames Russia for notpetya, the 'most costly cyberattack in history'. – Wired, 15. Veebruar.
92. Harden, B., Krebs, B., Nakashima, E. Who's behind cyber assults? – The Seattle Times, 9. Juuli.
93. Iasiello, E. (2013). Cyber attack: A dull tool to shape foreign policy. 2013 5th International Conference on Cyber Conflict. (Toim.) Podins, K., Stinissen, J., Maybaum, M. Tallinn, Estonia. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.
94. K. Ziolkowski. 2012. Stuxnet – Legal Considerations. Publication Nato Coperative Cyber Defence Centre of Excellence.Tallinn.
95. Kaitseministeerium (2008). Eesti Küberjulgeoleku strateegia 2008-2013. Kättesaadav: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf lk 10.
96. Leyden. J. (2016). BlackEnergy power plant hackers target Ukrainian banks. – The Register, 15. Detsember.
97. Lichfield, J. (2015). TV5 Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link. – Independent, 10. Juuni.
98. Majandus- ja kommunikatsiooniministeerium. (2014). Küberjulgeoleku strateegia 2014-2017. Kättesaadav:

https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf 14.05.2018.
99. Markoff, J. (2008). Before the Gunfire, Cyberattacks. – New Tork Times, 12. August.
100. McAfee & Centre for Strategic and International Studies. (2014). Net losses: Estimating the Global Cost of Cybercrime. Kättesaadav: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf 14.05.2018.
101. Nazario, J. Politically Motivated Denial of Service Attacks. Arbor Networks. United States. Kättesaadav: https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf 14.05.2018.
102. National Audit Office. (2017). Investigation: WannaCry cyber attack and the NHS. – 27. Oktoober.
103. Pau, L.F. (2010). Business and Social Evaluation of Denial of Service Attacks in View of Scaling Economic Counter-measures. Copenhagen Business School and Rotterdam School of Management. Kättesaadav: http://www.ccdcoe.org/publications/virtualbattlefield/20_PAU_Business%20and%20Social%20Evaluation%20of%20DDoS.pdf 13.05.2018.
104. Perloth, N., Hardy, Q. (2013). Bank Hacking Was the Work of Iranians, Officials Say. - New York Times, 8. Jaanuar.
105. Perlroth, N. (2012). In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. – The New York Times, 23. Oktoober.
106. Polityuk, P. (2016). Ukraine investigates suspected cyber attack on Kiev power grid. – Reuters, 20. Detsember.
107. Ponemon Institute & Accenture. (2017). Cost of cybercrime study. Inshigts on the security investments that make difference. Kättesaadav: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf 13.05.2018.
108. Ponemon Institute 2016. Cost of cyber Crime Study & the Risk of Business Innovation. Report. Kättesaadav: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf .
109. Ponemon Institute.(2017). Cost of Data Breach Study. Global overview. Research Report, lk 30. Kättesaadav: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN 13.05.2018.
110. R. Värk. Sissejuhatus rahvusvahelisse õigusesse. Tartu Ülikooli kirjastus.
111. Request fo interpretation of the judgment of 31 March 2004 in the case concerning Avena and other Mexican Nationals. ICJ rep 2009.
112. Riigi Infosüsteemi amet. (2012). Turvainsidentide käsitlemine. Kättesaadav: https://www.ria.ee/public/Programm/Tarkeriik_2012/SOHO_materjalid16181012/Turvaintsidentide_kasitlemine.pdf 13.05.2018.
113. Riigi Infosüsteemi Amet. (2014). Ohtlike internetiressursside eemaldamine internetist. Juhend. Kättesaadav: https://www.ria.ee/public/Kuberturvalisus/Ohtlike_internetiressursside_eemaldamine_Internetist.pdf 13.05.2018.
114. Riigi Infosüsteemide Amet. (2018). Küberturvalisus 2018. Kättesaadav: https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf 14.05.2018.
115. Riley, M., Carey, G., Fraher, J. (2016). Destructive Hacks Strike Saudi Arabia, Posing Challenge to Trump. – Bloomberg, 1. Detsember.

116. Zetter, K, (2016). Inside the cunning, unprecedented hack of Ukraines power grid. – Wired, 3. Märts.
117. Zetter, K. (2015). A cyberattack has caused confirmed physical damage for the second time ever. – Wired, 1. August.
118. Zetter, K. (2016). Inside the cunning, unprecedented hack of ukraine's power grid – Wired, 3. Märts.
119. The Council of Economic Advisers. (2018). The Cost of Malicious Cyber Activity to the U.S. Economy. Report. Kättesaadav: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.
120. The Economist. (2017). The boycott of Qatar is hurting its enforcers. – 19. Oktoober.
121. Tikk, E., Kaska, K., Vihul, L., Vihul, K. (2010). International Cyber Incidents: Legal Considerations. Cooperative Cyber Defence Centre of Excellence. Tallinn.
122. Tikk-Ringas, E., Bronk, C. (2013). Hack or Attack? Shamoon and the evolution of cyber conflict. Working paper. James. A. Baker III Institute for Policy Rice University.
123. Farmer, B. Montenegro asks for British help aftercyber attacks in wake of Russian-backed coup plot. – The Telegraph, 28. Veebruar.