RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Analüüs

Põhja-Atlandi Lepingu artikkel 5 kohaldatavus "uutele" julgeolekuohtudele

Jaanuar 2010

Maria Mälksoo

Põhja-Atlandi Lepingu Organisatsiooni (NATO) uue strateegilise kontseptsiooni (SK) kujundamise protsessis on muuhulgas tõstatunud küsimus, kuhu peaksid uues kontseptsioonis paigutuma ohud, mida ei ole rangelt võttes võimalik kvalifitseerida vahetu sõjalise rünnakuna ja seega ka Põhja-Atlandi Lepingu artikkel 5 toimealasse kuuluvana. Alljärgnevalt analüüsitakse lühidalt küber- ja energiajulgeolekualaste väljakutsete "artikkel 5-tüüpi" ohtudena käsitlemise probleemi.

1. Põhiküsimus

NATO aluslepingu artikkel 5 kohaselt käsitlevad lepinguosalised *relvastatud rünnakut neist ühe või mitme osalisriigi vastu Euroopas või Põhja-Ameerikas rünnakuna nende kõigi vastu ning sellest tulenevalt lepivad kokku, et niisuguse relvastatud rünnaku korral asub igaüks neist, rakendades Ühinenud Rahvaste Organisatsiooni Harta artiklis 51 sätestatud õigust individuaalsele või kollektiivsele enesekaitsele, sel viisil rünnatud lepinguosalist või lepinguosalisi abistama, rakendades koos teiste lepinguosalistega abinõusid, mida ta peab vajalikuks, sealhulgas relvajõudude kasutamist, eesmärgiga taastada ja säilitada Põhja-Atlandi julgeolek.* Võtmeküsimuseks on seega: **kas (ja kui, siis millistel tingimustel) võiksid küberrünnakud (või mistahes muud rünnakud riigi kriitilise infrastruktuuri, sh kriitilise informatsiooni infrastruktuuri pihta) olla kvalifitseeritud "relvastatud rünnetena" NATO alusleppe artikkel 5 ja jõu kasutamisena ÜRO Harta artikli 2 lõige 4 mõistes?** Lõppeks ei täpsusta ju NATO aluslepingu artikkel 5 (ega tegelikult ka mitte ÜRO Harta, millega Washingtoni lepe vaimus ühte sammu käia püüab), milliseid *relvi* silmas peetakse.

Juriidilises plaanis on siin õigupoolest ka teine probleem: ülalviidatust tuleneb omakorda küsimus, **kas juhul, kui nn uut tüüpi julgeoleku õõnestamise katsed toovad riigile kaasa reaalse(d) füüsilise(d) kahju(d) või ohu inimeste elule, on riikide enesekaitse** (olgu siis individuaalne või NATO raames toimuv kollektiivkaitse, tulenevalt ÜRO Harta artiklist 51) **õigustatud ka füüsilise relvajõu vahenditega** (ehk siis mitte pelgalt poliitiliste ja küberkaitseliste vastulahenditega). Et jõu kasutamist reguleeriv rahvusvaheline õigus ei kirjuta tegelikult ette, milliseid vahendeid võib riik enesekaitseks kasutada – senikaua, kui need on proportsionaalsed riigile tehtud rünnaku kahju ulatuse suhtes ning hädavajalikud rünnaku pareerimiseks, võiks ju *de facto* rünnaku ohvriks langenud riigil olla õiguspärane kasutada ka

sõjalist jõudu, kui küberründed (või muud analoogset tüüpi mittetraditsioonilised ründed) on põhjustanud riigile reaalset kahju.

Et momendil on vastavasisuline rahvusvaheline õigus alles kujunemas, on ka vähetõenäoline saavutada alliansipoolne üheselt mõistetav õiguslik "kristallisatsioon" küber- ja energiajulgeoleku pihta suunatud rünnakute kvalifitseerimise kohta NATO kollektiivkaitse klausli võimalike käivitajatena uue SK kavandatud valmimise ajaks. Hetkel on siiski tõenäolisim nn "uute" julgeolekuohtude liigitamine Washingtoni lepingu artikkel 4 alla, mille kohaselt *lepinguosalised konsulteerivad omavahel alati, kui neist kellegi arvates on ohustatud mis tahes lepinguosalise territoriaalne terviklikkus, poliitiline sõltumatus või julgeolek.*

2. Artikkel 5 kohaldatavuse probleemid nn "uutele" julgeolekuohtudele

Analüüsides Washingtoni leppe artikkel 5 kohaldatavust nn "uutele" julgeolekuohtudele tuleks kõigepealt lahti harutada, mis teeb "uutest" ohtudest, nagu küber- ja energiajulgeolekuprobleemid, kvalitatiivselt *uued* ohud. Üldiselt peetakse nn "uute" ohtude erijooneks traditsioonilistega võrreldes pretsedenditut ebaselgust ja määramatust. Kindlus puudub nii potentsiaalsete vaenlaste identiteedi ja eesmärkide kui ka ohtude ilmnemise tõenäolise ajaraamistiku osas.[1] Vastavalt tingib "uute" ohtude eripärast tulenev ebakindlus riikide jaoks ka teatava peataoleku vajalike võimete osas, kuna leidub terve hulk erinevaid potentsiaalseid konfliktitüüpe, mille vastu tuleks riiklikult ja kollektiivselt valmistuda. Paratamatult viib see järelduseni, et mistahes katse määratleda objektiivselt nn "uutest" ohtudest tõusetuva riski taset NATO kui terviku jaoks on juba ette määratud luhtumisele. Need pinged on selgelt välja joonistunud ka aruteluprotsessis NATO uue SK üle.

2.1. Küberohud

Küberründeid võib pidada paradigmaatiliseks näiteks kaasaegsete julgeolekuohtude teistsuguse loomuse kohta traditsioonilistega võrreldes: küsimus, *kes* ründab, jääbki küberrünnete puhul sageli tõestamatuks.[2] Vastavalt kätkeb ka (kollektiivsete) vastumeetmete organiseerimine ja käivitamine küberrünnete puhul ohtu maabuda identifitseerimata ründaja vastu peetava sõja sohu George W. Bushi administratsiooni "terrorismivastase sõja" kampaania laadis. Niisiis on traditsioonilise sõjalise ründe definitsiooni keerukas kohaldada kübersõdadele ning vastavalt on ka keeruline kohaldada küberründeile NATO kollektiivkaitse klausli käivitumist analoogselt traditsioonilisele sõjalisele rünnakule. Samas peab NATO arvestama tõsiasja, et

[1] Vt nt Cavelty, Myriam Dunn (2007) "Is Anything Ever New? – Exploring Specificities of Security and Governance in Information Age", teoses Myriam Dunn Cavelty, Victor Maner and Sai Felicia Krishna-Hensel, toim, *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate (19-44), lk 35.

[2] Richard J. Harknett ongi pidanud just raskesti omistatavust või ohuallika selge identifitseerimise võimatust (*attribution*) nn uutele ohtudele iseloomulikumaks jooneks kui laialtkasutatavat "asümmeetriat". – Harknett, Richard J. (2004) "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few", teoses Emily O. Goldmann, toim, *National Security in the Information Age*. London & Portland, OR.: Frank Cass (13-45), lk 14.

traditsioonilise sõjalise ründe tõenäosus Euro-Atlandi ruumis võrreldes ülalloetletud ebatraditsiooniliste julgeolekuriskide omaga on liitlaste jaoks küllaltki madal. Et niisugune sõda, nagu rahvusvaheliste suhete distsipliinis definitsioonijärgselt "sõjaks" tunnistatakse (s.o. vähemalt 1000 lahingusurmaga päädinud konflikt) on alliansi territooriumil vähetõenäoline võrreldes asümmeetriliste ohtudega liitlasriikide elanikkondade "inimväärsele elule", on vajadus traditsioonilise "relvastatud rünnaku" ümbermõtestamise järele alliansi kollektiivkaitse seisukohalt ilmne. Muutunud on niisiis mitte ainult ohud ja nende olulisuse taju liitlaste poolt, vaid muutunud on ka "sõja" definitsioon ning tegelikult avardunud ka "inimväärse elu" käsitlus. Tõepoolest, poliitiliselt relevantse elu kaitsmiseks (nt subjekti poliitilise suveräänsuse kaitsmiseks) ei ole "lahingusurmad" füüsilises mõttes isegi eelduseks. Teisalt ei tohi unustada, et kaasaegsed konfliktid on valdavalt mitmeplaanilised ja -mõõtmelised. Küberrünnet ei ole sestap otstarbekas käsitleda tingimata eraldiasetseva nähtusena traditsioonilisest sõjalisest rünnakust – on üsna tõenäoline, et tänapäeval saadab traditsioonilist rünnakut ka tegevus küberrindel, nagu ilmnes näiteks ka Vene-Gruusia sõjas 2008. aasta augustis.

2.2. Küberrünnete identifitseeritavuse probleem

Samas jääb tõsiasjaks, et küberründeid, nagu paljusid teisigi tänapäevaseid asümmeetrilisi julgeolekuohte, on reeglina väga raske territorialiseerida – üheselt seostada konkreetse "ründava riigi" territooriumi ja poliitilise võimu keskusega (nagu tõestasid muuhulgas 2007. aastal Eesti vastu suunatud küberrünnakud). Ehkki teoorias võivad küberründed ohustada ka riigi poliitilist suveräänsust ja isetegutsemisvõimet, olles sestap tinglikult kvalifitseeritavad NATO kollektiivkaitse aluseks oleva Washingtoni lepingu artikkel 5 käivitajatena, eeldaks tegelikkuses igasugune ohu piiritlemine kollektiivkaitse klausli käivitumiseks ühtlasi võimet selgelt määratleda allikas, millest oht lähtub. Küberohtude puhul on see aga harva üks-üheselt selge ning reeglina märkimisväärselt keerukas. Informatsioonitehnoloogiate spetsiifika tingib *tunnetuslikkuse* veelgi rõhutatuma olulisuse ohtude hindamisel, kuivõrd antud valdkonnas puuduvad n-ö käegakatsutavad faktid. Küberohtude kvalitatiivne uudsus seisneb ennekõike nende lahutatuses territoriaalsest riiklikust moodustisest. Küberrünnete lähtekoha avastamine – liiati veel ründe toimumise ajal – on äärmiselt raske. Võib ju küberrünnakuid korda saata paljudel erinevatel viisidel, noortest hobihäkkeritest organiseeritud kuritegevuse, poliitilise aktivismi puhangute ja strateegilise sõjapidamiseni välja.

Valdavalt sooritavad küberrünnakuid teadlikult, ent sageli ka täiesti tahtmatult näiteks arvutite "ülevõtmise" tagajärjel üksikisikud ja mitteriiklikud toimijad, ning neid seostada konkreetse riigi tahtliku vaenutegevuse ning suunatud käitumisega on reeglina äärmiselt keeruline. Riigi vastutusest (ja vastavalt ka rünnatud riigi/riikide sihitud vastulöögist) saaks rääkida vaid juhul, kui:

i) küberründajaid oleks võimalik kvalifitseerida x-riigi poolt toetatud toimijatena (ehk siis *de facto* riigi esindajatena, kui õnnestub tõestada "terroristidele"[3] x-riigi poolt antud toetus ja tugi);

ii) või juhul, kui suudetakse tõestada, et x-riigi valitsus seisis otseselt y-riigi pihta organiseeritud küberrünnete taga.

Kahjulikud tegevused võivad siinkohal varieeruda spioneerimisest (mida ei ole kuidagi võimalik jõu kasutamisena kvalifitseerida) kommunikatsioonisüsteemidesse sekkumise (mis ei põhjusta tingimata inimestele kahjusid ega ületa sestap piisavalt raskete kahjude lävepakku, et kvalifitseeruda jõu kasutamisena rahvusvahelise õiguse mõttes) ja inimestele reaalset kahju põhjustavate küberründeini. Tegelikult ületab alles viimasena loetletud kategooria jõu kasutamise lävepaku, ent ka eelnevad on käsitatavad riigi vastutuse kontekstis.[4] Lähtudes küberrünnete iseloomust ning juriidilistest defineerimisnüanssidest võiks küberohte kvalifitseerida ka terrorismi alaliigina, mis tähendaks omakorda potentsiaalselt erinevaid reageerimisvõimalusi, muuhulgas ka artikkel 5 raames. Eraldi kategooria küberprobleemide valdkonnas moodustab küberkuritegevus, mille vastustamine kuulub pigem Euroopa Liidu (EL) kui NATO pädevusse.

Rahvusvahelises õiguses puudub seega hetkel veel kindlalt kokkulepitud verstapost, kus küberrünnete puhul algab jõu kasutamine (ning on vastavalt õigustatud jõu kasutamine vastulöögina – ka traditsioonilises sõjalises, mitte ainult küberkaitse mõttes). Samas on aga rahvusvahelise õiguse praktika üsna pragmaatiline ja küllap tuleb kord ka hetk, kui riigid ütlevad *I will know it when I see it*. Eestile 2007. aastal tehtud küberrünnakute järel selle punktini ilmselgelt veel jõutud ei ole.

Tänaseks on alliansil olemas küll küberkaitsepoliitika ja küberkaitsekontseptsioon. Alliansi küberkaitse põhimõtete väljatöötamisel lähtuvad liikmesriigid NATO solidaarsusprintsiibist, mis on kooskõlas liitlaste suveräänsusega. Eesmärgiks on seega saavutada olukord, kus liitlased oleksid võimelised ja valmis vajadusel üksteisele küberrünnakute tõrjumisel abi osutama ning kus kõik alliansi liikmesriigid arendaksid oma riigisisest küberkaitsevõimet. On ilmne, et küberrünnete kvalifitseerimine artikkel 5 vaimus fundamentaalse liitlastevahelise solidaarsuskohustuse käivitajatena otsustatakse lähitulevikus siiski konkreetsete juhtumite põhiselt liitlaste praktikas, üldist reeglit poliitiliselt siduvaks kokkuleppeks, saati siis rahvusvahelis-õiguslikuks lepinguks, veel sedastamata.

[3] "Terrorism" on rahvusvahelises õiguses paraku korralikult ja kõiki riike siduvalt defineerimata, mistõttu kasutatakse siin antud mõistet vaid mööndustega.

[4] Vt pikemalt Kodar, Erki (2010) "Computer Network Attacks and the Grey Areas of *Jus ad* Bellum and Jus in Bello", *The Baltic Yearbook of International Law* (ilmumas).

2.3. Küberrünnete käsitlemise võimalikkus relvastatud rünnetena

Üldiselt on valdav osa tunnustatud rahvusvahelise õiguse teadlasi, kes on süvenenud küberrünnete kvalifitseerumise probleemi lähtuvalt jõu kasutamise perspektiivist, seisukohal, et küberründeid võib võrdsustada relvastatud ründega kui vastavate rünnete tagajärjed on võrdsustatavad füüsilise relvastatud ründe tagajärgedega (nt lennuõnnetused õhuliikluse kontrollisüsteemidesse häkkimise tagajärjel või tuumajaamade kontrollisüsteemisse sissemurdmise tagajärjel tekitatud õnnetused).[5] Reaalse ja ulatusliku füüsilise kahju tekitamine on seega küberrünnakute relvastatud rünnetena käsitlemise eeltingimus, pelgast poliitilisest ja majanduslikust surveavaldusest vastavaks kvalifikatsiooniks ei piisa.[6] Seega on küberohtude kontekstis iga olukorra ainulaadsust arvestav hindamine vältimatu ning etteulatuvalt absoluutset üldreeglit luua on raske.

Kui ohustatakse kriitilisi digitaalseid infrastruktuure, mis reguleerivad näiteks riigi elanikkonna elektri- või kütteenergiaga varustamist, finants- ja liiklusvõrke, kujutavad küberründed reaalset ohtu riigi majandusele, kriitiliste infrastruktuuride toimepidevusele ning ühiskonna sidususele. Küberründed võivad sihtida konkreetseid kaitseotstarbelisi arvutivõrke, pärssida valitsuse kommunikatsioonivõime tõhusust kriisiolukorras ning külvata üldist paanikat ning demoraliseerumistunnet elanikkonna hulgas. Mõningail ekstreemjuhtudel võiksid küberrünnakud niisiis käivitada Põhja-Atlandi lepingu artikkel 5 kollektiivkaitse klausli – juhul, kui nende põhjustatud tagajärjed küünivad jõu kasutamise standardini.

Oluline küsimus küberrünnete käsitatavuse puhul artikkel 5 tüüpi ohtudena on niisiis nende seos kriitilise infrastruktuuri haavatavusega laiemalt. Ehk kui vastav seos oleks enam-vähem automaatne ja laiapõhjaline, võiks *case* küberrünnete käsitlemiseks artikkel 5 raames samaväärselt traditsioonilise sõjalise ründe ohuga olla märksa tugevam ja põhjendatum. Kriitiliste infrastruktuuride all käsitletakse reeglina vee- ja toidumajandust, tervishoidu, transporti, energiasüsteeme, telekommunikatsiooni ning finantsteenuseid. Probleemi uurinud USA analüütik James A. Lewis peab aga eksitavaks arvutivõrkude haavatavuse automaatset seostamist kriitilise infrastruktuuri haavatavusega. Kriitilised infrastruktuurid – iseäranis suurtes turumajanduslikes riikides – on tema hinnangul oluliselt pihustatumad, mitmekesisemad, kahjustuste suhtes vastupidavamad ning enesetaastamisvõimelisemad kui esmapilgul paista võib, muutes nad kokkuvõttes kübervõrkudega võrreldes haavamatumaks.[7]

---

[5] Vt teemaarenduseks Kodar 2010.

[6] Viidatud on näiteks järgmistele kriteeriumitele, millele vastamise korral võiks küberrünnakuid käsitada jõu kasutamisena ÜRO Harta artikkel 2 lõige 4 mõttes: 1) *raskus* (tagajärjeks füüsilised vigastused või hävitamine); 2) *vahetus* (tagajärgede kohesus); 3) *otsekohesus* (tagajärjed on jõu kasutamisega tihedalt seotud); 4) *sekkuvus* (kõrgel tasemel sissetung sihtriigi õigustesse); 5) *mõõdetavus* (tagajärjed on kergesti identifitseeritavad); 6) tõenäoline legitiimsus (mittelubatavuse eeldus kuni tõestuseni, et tegu on enesekaitsega). – Vt Schmitt Benatar, Marco (2009) "The Use of Cyber Force: Need for Legal Justification", Göttingen Journal of International Law 1 (3) kaudu.

[7] Niisugune seisukoht näikse siiski tuginevat kitsalt USA kogemusele ega vasta tingimata näiteks Eesti olukorrale. – Vt Lewis, James A. (2002) *Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats*. Washington: Center for Strategic and International Studies.

Hindamaks kriitiliste infrastruktuuride tegelikku haavatavust küberrünnete suhtes, tuleks teostada detailne vastupidavushinnang iga kõnealuse infrastruktuuri kohta eraldi.[8] Arvestada tuleks lisaks vastavate infrastruktuuride vastupanuvõimet ning ebaõnnestumissagedust normaaljuhtudel; kriitilistele funktsioonidele ligipääsetavust avalikest võrkudest ning inimkontrolli, -jälgimise ning interventsiooni võimalikkuse määra kriitilistes operatsioonides.[9] Kahel põhjusel on see aga raske või isegi võimatu: esiteks puudub kriitiliste süsteemide haavatavuse kohta avalikult või kergesti kättesaadav informatsioon. Vastavasisuline info on riiklikult klassifitseeritud ja sageli mähitud mitme saladusloori sisse ning eraettevõtted on harva valmis vabatahtlikult asjassepuutuvat infot väljastama. Lisaks relevantse info raskele ligipääsetavusele on kriitiliste infrastruktuuride *tegeliku haavatavuse* hindamine keerukas ka seetõttu, et ainuüksi asjassepuutuvate andmete põhjal ei ole võimalik reaalselt määratleda ohu "kriitilisust", s.o. selle kriitilist olulisust riigi toimepidevuse seisukohalt. Esiteks on see, mida peetakse "kriitiliseks", pidevas muutumises; teiseks ei ole võimalik infrastruktuuri või teenuse "kriitilisust" kunagi ennetavalt määratleda, vaid seda saab kindlaks teha vaid *ex post facto* – alles pärast sündinud kriisi ja sellele järgnenud hindamisprotsessi. Ja viimaseks, ent mitte vähimoluliseks ei tohiks unustada, et igasugune haavatavuse potentsiaal eeldab ohuna realiseerumiseks siiski ka teatud toimijate *võimet* ja *tahtlust/motivatsiooni* vastavat haavatavust rünnata.

Üldiselt näikse NATO senist poliitikat ja seisukohavõtte jälgides siiski tõenäolisim, et küberjulgeolekuohte käsitletakse lähitulevikus pigem Washingtoni leppe artikkel 4 raames, mis sedastab liitlaste omavaheliste konsultatsioonide kokkukutsumise võimaluse ühe (või mitme) liitlase ettepanekul, kui nähakse ohtu mistahes NATO liikme territoriaalsele terviklikkusele, poliitilisele iseseisvusele või julgeolekule. Oluline oleks mõista *ohtu julgeolekule* siiski võimalikult avaralt ning ühtlasi hoida artikkel 4 raames sätestatud formaalsete liitlastevaheliste konsultatsioonide kokkukutsumise lävi võimalikult madalana, et artikkel 4 oleks vajadusel reaalselt kättesaadav.

Momendil valitseb vähemalt rahvusvahelis-õiguslikus plaanis konsensus, et küberohte ei saa üheselt käsitleda ÜRO Harta artikli 2(4) vaimus. Vastava sätte kohaselt hoiduvad *kõik ÜRO liikmed oma rahvusvahelistes suhetes jõuga ähvardamisest või jõu tarvitamisest nii iga riigi territoriaalse puutumatuse, poliitilise sõltumatuse vastu kui ka mõnel muul viisil, mis ei ole kooskõlas ÜRO eesmärkidega.* Eelnevast tulenevalt on raske üheselt ette määrata ka

---

[8] Eesti küberjulgeolekustrateegia tõstab esile *kriitilise infrastruktuuri* ja *kriitilise informatsiooni infrastruktuuri* eristuse. *Kriitilise infrastruktuuri* all mõistetakse neid varasid, teenuseid ja süsteeme (või nende osi ja süsteemidevahelisi ühendusi), mille hävitamine, kahjustamine või hõivamine võib ohustada inimeste elu või tervist või tuua kaasa vara, teenuse, süsteemi või nende osade hävimise või ulatusliku majandusliku kahju ning põhjustada ühiskonna turvatunde vähenemist, vähendada riigi usaldusväärsust, kahjustada riigi mainet ja halvata riigi toimimist. *Kriitilise informatsiooni infrastruktuuri* all mõistetakse omakorda neid informatsiooni infrastruktuuri komponente, mis on kas ise kriitilised või mis on hädavajalikud kriitilise infrastruktuuri toimimiseks. – Vt *Küberjulgeoleku strateegia 2008-2013* (2008). Tallinn: Kaitseministeerium, Küberjulgeoleku strateegia komisjon.

[9] Vt Cavelty, 2007: 34.

individuaalse ja kollektiivse enesekaitselahendi, mida võimaldab ÜRO Harta artikkel 51, spetsiifikat. Samas tuleb silmas pidada, et isegi kui küberjõudu ei ole võimalik aprioorselt jõu kasutamisena kvalifitseerida (nii nagu seda seni rahvusvahelises õiguses on mõistetud), on tegu ometi interventsiooni, teise riigi siseasjadesse sekkumise alaliigiga, mida saab omakorda selgelt rahvusvahelise õiguse rikkumiseks lugeda. Nii ehk teisiti võib olla tegemist rahvusvahelise õiguse riigi vastutuse põhimõtete rikkumisega, nii nagu need on fikseeritud 2001.a. Rahvusvahelise Komisjoni poolt sõnastatud ja ÜRO peaassamblee poolt heaks kiidetud Riigi vastutuse artiklites (*ILC Articles on State Responsibility*).[10]

Kas aga konkreetsete küberrünnakute puhul käivitatakse NATO lepingu artikkel 5 või mitte, jääb esialgu veel *ad hoc* liitlaste otsustada. Selge on see, et küberrünnete puhul on NATO artikkel 5 rakendamine tihedalt seotud artikkel 4 rakendamisega. Kui küberkonflikt ületab reaalselt artiklis 5 sätestatud relvastatud ründe (ehk siis relvastatud ründe tagajärgedega samaväärsuse) künnise, hakkavad võtmerolli mängima rahuajal välja töötatud ja artiklis 4 sätestatud koostöö tagamiseks rakendatavad õiguslikud ja poliitilised mehhanismid (sh info vahetamine võimalike ohtude ja kaitsemeetmete kohta).[11]

NATO lähituleviku tegevusagendas on küberjulgeoleku tagamisel vaieldamatult kõrge koht, ent tegevuse põhirõhk peaks olema siiski suunatud ohtude ennetusele ja enese "ennetavale kaitsmisele" kui ka enese vastupidavusvõime suurendamisele võimalike rünnete korral. Sarnaselt riiklikule küberjulgeolekustrateegiale, mis sedastab Eesti küberruumi julgeoleku tagamisel olulisemate tegevustena küberruumi haavatavuse vähendamise, küberrünnakute ennetamise ning infosüsteemide toimimise võimalikult kiire taastamise rünnakute korral, peaks ka NATO küberjulgeolekukontseptsioon lähtuma loetletud põhimõtetest.[12]

Alliansi strateegiliseks eesmärgiks võiks olla nn heidutus läbistamatuse kaudu (*deterrence through denial*) – ehk nii enese kaitsevõime tõstmine potentsiaalsete küberrünnete vastu kui ka vastase vaenulike võimete tasalülitamisvõime ründe-eelse infosurveoperatsiooni käigus, eesmärgiga hoida vastast tagasi ründamast.[13] Heidutust traditsioonilises mõttes on nn "uutele ohtudele" kohaldada keeruline: on ju heidutuse eelduseks võime kiirelt välja selgitada ründe ulatus, hinnata vaenupoole poolt tekitatav tõenäoline kahju ning tunda ära ründeallikas ja aduda tema tegutsemismotiive.[14] Traditsioonilise heidutuse eeldus – vastase selge identifitseerimine –

[10] Nii kandsid näiteks ka Eesti vastu 2007. aasta kevadel suunatud DDoS (*Distributed Denial of Service*) rünnakud ühiskonna rahulolematuse suurendamise eesmärki demokraatlikult valitud valitsuse sisepoliitika suhtes – *ergo*, on käsitletavad sekkumisena demokraatlikesse süsteemidesse.

[11] Vt ka Toomas Hendrik Ilves, Vabariigi President rahvusvahelisel küberjulgeoleku õiguse ja poliitika konverentsil Tallinnas, 9.09.2009; http://www.president.ee/et/k6ned/k6ned.php?gid=130308 (viimati vaadatud 15.01.2010).

[12] Vt Küberjulgeoleku strateegia 2008: 7.

[13] Vrdl Bishop, Matt and Emily O. Goldman (2004) "The Strategy and Tactics of Information Warfare", in Emily O. Goldmann, ed., *National Security in the Information Age*. London & Portland, OR.: Frank Cass (113-39), lk 134.

[14] Vt Harknett, 2004: 34.

ei pruugi informatsiooniajastu ohutrendide kontekstis üldse pädeda, liiati arvestades, et asümmeetrilised rünnakud lähtuvad valdavalt mitteriiklike toimijate poolt.

2.4. Artikkel 5 ja energiajulgeolek

Arvestades energiajulgeoleku mõiste mitmemõõtmelisust, on selge, et NATO profiilile on keeruline kohaldada energiajulgeoleku majanduslike aspektide turvalisuse ja toimimiskindluse tagamist. NATO ei ole alliansi senist profiili arvestades sobilikem organisatsioon korraldamaks liikmesriikide varustuskindlust energiaga või nende "energeetilist iseseisvust" (ehk sõltumatust impordist), rääkimata tarnijate stabiilsuse ja paljususe ning energiaallikate mitmekesisuse garanteerimisest. NATO ampluaasse võiks kuuluda pigem kriitilise infrastruktuuri turvalisuse, toimepidevuse ja kaitse organiseerimine laiemalt, sealhulgas valmisolek suurte alliansisiseste kriitilisi infrastruktuure puudutavate õnnetuste, terroriaktide, sabotaaži või organiseeritud kuritegevuse tagajärgedega toimetulekuks. Ambitsioonikam, püsiva alliansi-poolse energiastruktuuride kaitse korraldamine nafta- ja gaasimaardlatest torujuhtmete ja energiatransiitteede turvamiseni merel on liitlaste seas siiski suur vaidlusküsimus.

Kas "energiarelva" kasutamine energiatarnete tahtliku häirimise või tarnete peatamise kaudu, mis toob kaasa ulatuslikke kahjusid inimeste elule ja riigi põhiliste infrastruktuuride toimimisele, võiks kuuluda Washingtoni leppe artikli 5 toimealasse, nagu on soovitanud näiteks mõjukas USA senaator Richard Lugar,[15] on alliansis samuti veel vägagi vaieldav küsimus. Energiastruktuuride pihta tehtud füüsilise rünnaku pareerimine eeldab lõppeks teistsuguseid lahendusi kui reageerimine energiavarustuse tarnehäiretele (nt tarnete vähendamisele või lõpetamisele, hinnatõusudele, embargodele jne), mille puhul füüsilist vägivalda ei kasutata. Samas võiks näiteks gaasitarnete katkemine südatalvel mõne põhjapoolsema Euroopa riigi jaoks ikkagi tähendada inimeste hukkumist ja majanduslikke kahjusid, mis võrreldavad füüsilise relvastatud rünnaku tagajärgedega.

Senaator Lugari seisukoha järgi ei tähendaks "energiajulgeoleku artikkel 5" siiski mitte NATO sõjalist vastulööki energiatarnete lakkamise korral mõnesse alliansi liikmesriiki, vaid pigem kätkeks kollektiivset solidaarsuskohustust varustada pihtasaanud liitlast/liitlasi energiaga alternatiivsete mehhanismide kaudu. Lugari visiooni kohaselt peaks NATO identifitseerima olemasolevate energiavõrgustike alternatiivid; arendama välja strateegiad, varustamaks agressiivse energiavarustuskatkestuse ohvriks langenud liitlasi alternatiivse energiaga;[16] looma mehhanismid rünnakualuse riigi energiaga varustamiseks hädaolukorras ning kindlustama vastava rünnaku puhuks vajaliku infrastruktuuri olemasolu. Niisuguse käitumise loogika on lihtne: selgelt koordineeritud ning ka väljapoole kommunikeeritud alliansi reaktsioon energiarelvaga ähvardamisele toimiks juba iseenesest teatava heidutusena. Hetkel siiski

[15] Vt Richard Lugari sõnavõtt NATO tippkohtumisel Riias, märts 2007.

[16] Siinkohal mõistes "alternatiivset energiat" mitte tingimata "rohelise energia" tähenduses, vaid lihtsalt alternatiivsest energiaallikast/varustusvõrgust lähtumise mõttes.

puudub alliansis konsensus küsimuses, kas NATO vastutusala võiks laieneda ka hädaolukorra energiavarude haldamise valdkonda. Alliansiülese üksmeele leidmist ei kergenda ka Euroopa liitlaste ning USA erinevad energiajulgeolekualased tundlikkuspunktid, Euroopa liitlaste endi erinevast "energeetilise haavatavuse" tasemest rääkimata. Mõnedki liitlased Euroopas, nagu Prantsusmaa, eelistaksid Lugari visandatud "energiajulgeoleku artikkel 5" andmist pigem ELi pädevusse. Samas on suuresti just ELi senine võimetus adekvaatset ühist energiapoliitikat luua tinginud Lugari-sarnaste häälte süveneva rahulolematuse energiajulgeolekuprobleemide senise käsitlemisega Euroopas.

NATO deklareerib end momendil eelkõige keskenduvat kriitilise infrastruktuuri julgeoleku tagamisega seotud küsimustele, toetades liikmesriike vajadusel nende kriitilise energiainfrastruktuuri kaitsmisel (viimaste palvel), jälgides ning hinnates üldisi riske ja arenguid ning pakkudes kriisihaldust. Ühtse energiakriiside halduse süsteemi arendamine nõuab aga alliansis veel selgelt tööd. NATOl tuleks aktiivselt edasi tegutseda kriisiolukordades vastastikuse toetamise jaoks vajalike tegutsemismehhanismide ja -mudelite tagamise nimel. Oluline on ka üldiste tegutsemismehhanismide tugevdamine õnnetuste või energiavarustuskriiside puhuks.

NATO-poolt korraldatava kriitiliste energiastruktuuride kaitse raskuskese on siiski ennetusel, minimeerimaks juba eos rünnakute tõenäosust ja võimalikku mõju. Energiajulgeoleku probleemid kuuluvad nähtavas tulevikus samuti pigem Põhja-Atlandi leppe artikkel 4 kompetentsi. Lõppeks on energiajulgeoleku erinevate mõõtmete adresseerimisel EL oma majanduslikelt ja poliitilistelt vahenditelt siiski kohasem organisatsioon kui tänane NATO. Seega peaks energiavaldkonna alaste julgeolekuriskide ennetav maandamine toimuma pigem ELi ühise energiapoliitika (mis küll väga valuliselt sünnib) kaudu. Energia-alane kriisihaldus on NATO jaoks tegelikult juba poliitiliste lahenduste ebaõnnestumise ja mittetöötamise paratamatu tagajärg. Selge on siiski seegi, et energiajulgeoleku-alaste väljakutsetega toimetulek saab tulemuslikult toimida ennekõike ELi ja NATO vastastikku toetavas koostöös. Vastavalt on ka vajadus NATO-poolse tegevuse põhjalikumaks lahtikirjutamiseks energiajulgeoleku-alaste väljakutsete ennetaval maandamisel ja energiakriiside haldamisel uues SKs ilmne.

3. Kokkuvõte

Hetkel ei saa üheselt vastata küsimusele, kas küber- ja energiajulgeolekut puudutavad väljakutsed on kvalifitseeritavad Põhja-Atlandi lepingu artikli 5 alla käivana. Paratamatult peame praegu vaid spekuleerima, sest elame ise infoajastu spetsiifikast tulenevate protsesside keskel, mistõttu tuleb ka küber- ja energiajulgeoleku probleemidele reageerida enamasti n-ö poole pealt, ise asjade sees ja keskel olles. Selgelt peab eristama ka kaht küsimuse tasandit: missugune on normatiivne seis praegu (kehtiv õigus või *lex lata*) ja missugune õigus meie arvates võiks tulevikus olla (*lex ferenda*)? Kui küsime, kas praegune õiguse ja asjade seis võimaldaks näiteks konstrueerida küberründed artikkel 5 alla, on vastuseks pigem "ei" – mitte selles mõttes, et kehtiv õigus selle välistab, vaid selles mõttes, et teadlikult artikkel 5 seda teemat ei reguleeri. Ainsa erandina tulevad kõne alla need erakordsed juhtumid (ja mida sel

kujul pole liitlaste jaoks veel täies mahus esinenud), mis ülapool viidatud. Mis puudutab *lex ferenda*'t, siis siin tuleb arvestada sellega, et uue (laiendatud) sisu andmine õiguslikele kohustustele saab NATO-s sündida ainult konsultatsioonide ja konsensuse tulemusena. Tuleb arvesse võtta ka seda, et Washingtoni lepingu tõlgendamine tulevikus peab "kokku kõlama" ÜRO Harta valitseva tõlgendusega. See on aga ÜRO liikmelisusest tulenevalt (väikeriikide ja mitte-Lääne riikide enamus) jõu kasutamise suhtes konservatiivne. Kardetakse nimelt, et tugevad riigid võivad otsida ettekäändeid, et nõrgemate vastu jõudu kasutada.[17]

Arvestades küber- ja energiajulgeolekuprobleemide spetsiifikat on ka selge, et vastavatele sektoritele esitatavate julgeolekuväljakutsete vastustamist ei saa üheselt riiklike lahenditega reguleerida – nii küberohtude tõrjel kui ka energiajulgeoleku-alaste väljakutsete vastustamisel on vältimatu tihe koostöö erasektoriga. Ei tee ju küberruum vahet era- ja avaliku ega riikliku ja rahvusvahelise sfääri vahel. Vastavalt on ka juba kaitstava ulatuse määratlemine keeruline, rääkimata julgeoleku tagamiseks vajaliku koordinatsiooni sisseseadmisest. Eraldi probleemiks mitmemõõtmelise konflikti puhul, näiteks juhul, kui traditsioonilist jõudu ja küberründevahendeid kasutatakse samaaegselt, on riigi poolt oma heidutustahte ja -ja võimekuse kohta väljastatud signaalide väärtõlgendamine – olgu siis põhjusel, et oht, mida heidutada tahetakse, on tegelikult piisavalt täpsustamata või hoopis seetõttu, et heidutus on suunatud liiga kitsale ja konkreetsele julgeolekuprobleemile.[18]

Mõneti on Põhja-Atlandi lepingu telje – artikkel 5 – potentsiaalselt käivitavate ohtude spektri konstruktiivne ebamäärasus isegi hea, kuivõrd ohtude liigkonkreetne loetelu võiks viia olukorrani, kus seistakse vastamisi mõne liikmesriigi jaoks eksistentsiaalsena tajutud ohuga, mis ometi olemasoleva strateegilise kontseptsiooni loetelust mingil põhjusel välja on jäänud. Sellest, et ohtude liigtäpne defineerimine ja üleslugemine võib agressorile isegi lisavõimalusi tekitada, räägiti tegelikult juba enne Teist maailmasõda rahvusvahelist õigust kujundades. Alliansi uus SK ei tohiks seda vana tõde unustada.

[17] Sümptomaatiline oli juba 1986.a ÜRO Rahvusvahelise Kohtu otsus vaidluses USA vs. Nikaraagua, kus oli põhiküsimuseks, millal tohib riik artikkel 51 alusel teostada relvastatud enesekaitset. Kohtu otsusest võib niimoodi aru saada, et isegi mitte kõik artikkel 2 lg 4 rikkumised (ehk *use of force*, näiteks geriljade toetamine üle piiri) ei kvalifitseeru automaatselt "relvastatud rünnakuks" artikkel 51 tähenduses. Seda seisukohta on, eriti USAs, muidugi ka kritiseeritud, ent omalaadne indikaator on see rahvusvahelise üldsuse tõrksuse kohta asjassepuutuvat õigust paindlikult tõlgendada sellegipoolest.

[18] Vt Harknett, 2004: 33-35.