BY-NC-ND

ISSN 1392–6195 (print)
ISSN 2029–2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2013, 20(3), p. 1195–1212.

KIBERNETINIŲ TECHNOLOGIJŲ PANAUDOJIMO GINKLUOTUOSE KONFLIKTUOSE POVEIKIS TARPTAUTINEI HUMANITARINEI TEISEI

Justinas Žilinskas

Mykolo Romerio universiteto Teisės fakulteto
Tarptautinės ir Europos Sąjungos teisės institutas
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas (+370 5) 271 4669
Elektroninis paštas j.zilinskas@mruni.eu

Pateikta 2013 m. liepos 15 d., parengta spausdinti 2013 m. rugsėjo 20 d.

doi:10.13165/JUR-13-20-3-17

Anotacija. *Šiame straipsnyje nagrinėjama, kaip kibernetinių technologijų panaudojimas ginkluotų konfliktų (kibernetinio karo) kontekstuose veikia tarptautinę humanitarinę teisę. Konkrečiai aptariami trys probleminiai aspektai: ar egzistuojanti tarptautinė humanitarinė teisė iš principo gali reguliuoti tokius naujoviškus reiškinius kaip kibernetinis ar kibernetizuotas ginkluotas konfliktas, antra, kokią įtaką kibernetinių priemonių panaudojimas daro ginkluoto konflikto sampratai, trečia, kaip kibernetinių priemonių atsiradimas ginkluoto konflikto kontekste gali paveikti kombatanto (bei asmens, naudojančio ginkluotą jėgą) institutą. Pirmasis probleminis klausimas teoriškai sprendžiamas gana aiškiai, tačiau antrasis ir trečiasis rodo svarbius esamo teisinio reguliavimo aiškinimo pokyčius, kai nemaža dalis klasikinių kriterijų praranda prasmę, o naujieji kriterijai pasižymi tam tikru teisiniu neapibrėžtumu.*

Reikšminiai žodžiai: *ginkluotas konfliktas, kibernetinis ginkluotas konfliktas, tarptautinė humanitarinė teisė, kibernetinis ginklas.*

© Mykolo Romerio universitetas, 2013
© Mykolas Romeris University, 2013

Įvadas

Kai 2013 m. vasarą prasidėjo DDoS atakos prieš Lietuvos tinklalapius, įskaitant ir populiariausią naujienų portalą *delfi.lt*, ir Lietuvos pareigūnai prabilo apie kibernetines grėsmes, susirūpinta tiek, kad Lietuvos pirmininkavimo ES Tarybai laikotarpiu 2013 m. tam norima skirti papildomų pajėgumų[1], net sukurta speciali Vidaus reikalų ministerijos kibernetinio saugumo taryba[2]. Taigi, Lietuvoje jau irgi pripažįstama, kad kibernetinių puolimų grėsmės yra aktualios, realios ir esmingai kitokio pobūdžio nei ankstesnės. Ir gana keista, kad Lietuva valstybės lygmeniu tik taip vėlai susirūpino šiais klausimais. Juk šiuolaikinės visuomenės ir valstybės funkcionavimas jau nebeįsivaizduojamas be informacinių technologijų. Atitinkamai kyla vis daugiau grėsmių, kad netrukus puolimai prieš valstybių informacines sistemas galės sukelti net daugiau žalos nei įprastinės ginkluotos jėgos panaudojimas.

Kad problema nėra laužta iš piršto, jau patyrė mūsų kaimynė Estija – 2007 m. ji tapo kibernetinių puolimų taikiniu[3], kibernetiniai puolimai užklupo ir Gruziją 2008 m. karo su Rusija metu[4], o kol kas sėkmingiausias ir grėsmingiausias kibernetinio puolimo pavyzdys – STUXNET viruso, sugadinusio Irano urano sodrinimo gamyklos centrifugas, sukūrimas ir panaudojimas[5]. Mažesni incidentai, tokie kaip kibernetinis špionažas, duomenų vagystės ir pan., yra pasaulio kasdienybė. Tyrinėtojai pastebi, jog kibernetinių priemonių galimybės puikiai pildo vadinamųjų „ketvirtos kartos karų“, kuriems būdinga maoistų „slinkties strategija“ ir alternatyvių hierarchijų kūrimas, gresiantis valstybės teisėtumui ir stabilumui, konstruktą[6].

Galima skirti du variantus, kaip kibernetinių priemonių panaudojimas gali pasireikšti ginkluoto konflikto kontekste. Pirmas – tai kibernetinių priemonių taikymas vykstančio ginkluoto konflikto metu (pavyzdžiui, šalia tradicinių ginkluotos jėgos panaudojimo būdų pasitelkiamos kibernetinės priemonės – kaip nutiko Gruzijoje, tai būtų tarsi kibernetizuotas įprastinis ginkluotas konfliktas), antra, tai ginkluotas konfliktas, vykdomas vien kibernetinėmis priemonėmis (toks atvejis galėtų būti STUXNET, jeigu būtų įrodyta, kad jis buvo sukurtas ir panaudotas valstybių). Ir pirmasis, ir antrasis va-

---

1 Fuks, E. Išvada po susitikimo su prezidente: vargu ar apsiginsime nuo didesnės atakos. *delfi.lt* [interaktyvus]. [žiūrėta 2013-06-04]. <http://www.delfi.lt/news/daily/lithuania/isvada-po-susitikimo-su-prezidente-vargu-ar-apsiginsime-nuo-didesnes-atakos.d?id=61545466>.

2 Įsteigta Kibernetinio saugumo taryba. Lietuvos Respublikos vidaus reikalų ministerija [interaktyvus]. [žiūrėta 2013-07-09]. <http://www.vrm.lt/go.php/lit/Isteigta-kibernetinio-saugumo-taryba-/830>.

3 Traynor, I. Russia accused of unleashing cyberwar to disable Estonia. *The Guardian* [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.

4 Haddick, R. This Week at War: Lessons from Cyberwar I. *Foreign Policy* [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i>.

5 Kushner, D. The Real Story of Stuxnet. *IEEE Spectrum* [interaktyvus]. [žiūrėta 2013-07-01]. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

6 Liles, S.; Dietz, J. E.; Rogers, M.; Larson, D. Applying Traditional Military Principles to Cyber Warfare. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012, p. 175 [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf>.

riantai kelia daug klausimų. Pirmiausia jie diktuojami technologinės specifikos. Kaip visi suprantame, kibernetinio puolimo faktiškai neriboja geografinės valstybių sienos. Yra netgi dar sudėtingiau – kaip teisingai pastebėjo po kibernetinių puolimų prieš Estiją elektroninio saugumo firmų specialistai, nustatyti pradinį arba centrinį puolimo šaltinį (o ne jo išnaudojamus užvaldytus kompiuterių tinklus, vadinamus *botnet*) yra beveik neįmanoma[7]. Be to, netgi paties kibernetinio „ginklo“ analizė gali užtrukti labai ilgai – pavyzdžiui, STUXNET buvo aptiktas 2010 m., ir iki šiol nėra iki galo tikslios informacijos, kas jį sukūrė, daug kas vis dar paremta prielaidomis, maža to, teigiama, kad tai, kas galbūt prasidėjo kaip valstybių kuriamas ginklas, vėliau tapo kriminalinių nusikaltėlių įkvėpimu[8]. Taigi, temos aktualumas neturėtų kelti abejonių.

Kibernetiniai puolimai, kibernetinių priemonių panaudojimas – gana naujas reiškinys. Kyla pagrįstas klausimas, kaip kibernetinio ginkluoto konflikto klausimus spręstų tarptautinė teisė, o dar konkrečiau – tarptautinė humanitarinė teisė? Atsakymų į šį klausimą ieškoma aktyviai. Štai 2012 m. po NATO Kibernetinės gynybos kompetencijos centro (angl. *NATO Cooperative Cyber Defence Center of Excellence*) egida buvo parengtas „Talino vadovas dėl tarptautinės teisės, taikytinos kibernetiniams karams[9]“ (toliau – Talino vadovas), mėginantis atsakyti į daugelį klausimų, susijusių su kibernetiniais konfliktais[10]. Tačiau, nepaisant to, kad mokslininkai pasisako įvairiais kibernetinio karo klausimais[11], galutinio aiškumo daugeliu klausimų nėra, todėl tai – vis dar plati erdvė atsakymų paieškai.

Taigi, šio straipsnio tikslas – atsakyti į klausimą, kokios galimybės *de lege lata* tarptautinę humanitarinę teisę taikyti kibernetinių karų kontekste, identifikuoti teisinio reguliavimo problemas ir pasiūlyti galimus jų sprendimo būdus. Tyrimo objektas – įvairūs tarptautinės humanitarinės teisės mechanizmai bei institutai, konkrečiai – ginkluoto konflikto institutas bei asmens, naudojančio ginkluotą jėgą (kombatanto), institutas. Tyrimo metodai – šaltinių analizės, bylų analizės, sisteminės analizės, istorinis ir kiti.

Šis straipsnis susideda iš trijų teminių dalių: pirmoje aptariamas tarptautinės humanitarinės teisės pritaikomumas naujiems reiškiniams, antroje nagrinėjama, kiek dabartinė ginkluoto konflikto samprata tinkama kibernetinio karo realijoms, trečioje analizuojama, kokie pokyčiai galėtų laukti kombatanto sąvokos kibernetinio ginkluoto konflikto kontekste.

Pora pastabų dėl šiame straipsnyje vartojamos terminologijos. Straipsnio tekste žodis „karas“ vartojamas kaip aprašomasis, bendrosios prasmės terminas, apimantis patį

---

7 Anderson, N. Massive DDoS attacks target Estonia; Russia accused. *Arstechnica.com* [interaktyvus]. [žiūrėta 2013-07-01]. <http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/>.

8 Kushner, D., *supra* note 5.

9 *Tallinn Manual on the international Law Applicable to Cyber Warfare*. Schmitt, M. N. (ed.). Cambridge University Press, 2013.

10 Tiesiog būtų negražu nepasidžiaugti mūsų kaimynų estų tikslingumu, kai 2007 m. kibernetinės atakos prieš Estiją išprovokavo ne šiaip atsaką, o visą iniciatyvų seriją, įskaitant ir NATO Kibernetinės gynybos kompetencijos centro įsteigimą ir minėtąjį Talino vadovą.

11 Pavyzdžiui, 2012 m. Taline įvyko jau ketvirtoji Kibernetinių konfliktų konferencija, kurios medžiaga šis straipsnis gausiai paremtas.

įvairiausią ginkluotos jėgos panaudojimo pasireiškimą (tarptautinį ginkluotą konfliktą, netarptautinį ginkluotą konfliktą, mišrias arba sunkiai identifikuojamas situacijas, tokias kaip „antiteroristinės operacijos“), o ne kaip specifinis teisinis terminas, kaip jis buvo suprantamas klasikinėje karo teisėje. Terminas „kibernetinė priemonė“ šiame straipsnyje reiškia bet kokį programinį, technologinį ar kitą sprendimą, skirtą panaudoti kibernetinio karo metu priešui ar oponentui susilpninti, jam pakenkti, įskaitant ir kibernetinius ginklus (t. y. kibernetines priemones, savo poveikiu prilygstančias įprastinių ginklų poveikiui).

1. Tarptautinės humanitarinės teisės reguliavimo ypatybės ir nauji reiškiniai

Kibernetiniai puolimai ir apskritai jėgos panaudojimas kibernetiniu būdu yra neabejotinai naujas reiškinys. Tuo tarpu tarptautinė teisė nėra toji teisės sistema, kuri į kiekvieną pokytį gali reaguoti tuoj pat, naujomis, tiksliai nukreiptomis į reiškinį ir aiškiai suformuluotomis teisės normomis. Tarptautinių sutarčių sudarymo ar tarptautinių papročių susiformavimo procesas ilgas, daugialypis ir sudėtingas. Ši įžvalga tinka ir tarptautinei humanitarinei teisei. Pavyzdžiui, Ženevos konvencija dėl karo belaisvių apsaugos (pirmasis jos variantas[12]) buvo priimta 1929 m., nors jos poreikis tapo akivaizdus būtent Pirmojo pasaulinio karo metu, 1914–1918 m. Tačiau prireikė 11 metų, kad ji atsirastų popieriuje. Be abejo, jeigu dabar būtų pradėta galvoti apie atskirą konvenciją, skirtą kibernetiniam karui, procesas užtruktų, nors tokių bandymų yra. Bet laiko išsamių naujų normų kūrimui, kaip rodo tarptautiniai incidentai, nėra. Kibernetiniai karai – lygiai toks pats naujoviškas reiškinys, kaip privačių karinių / saugumo kompanijų veikla, nepilotuojamų orlaivių ir autonominių kovos sistemų specialaus reguliavimo nebuvimas. Taigi, reikia atsakyti į principinį klausimą, ar tarptautinė bei tarptautinė humanitarinė teisė gali ir yra pajėgi reguliuoti kibernetines priemones ginkluoto konflikto kontekste?

Taigi, kalbant apie tarptautinę teisę ir kibernetinio ginkluoto konflikto reguliavimą, vėlgi galima išskirti dvejopą požiūrį: pirmą, skeptišką, manant, kad tarptautinė teisė, o juo labiau – tarptautinė humanitarinė teisė – naujoms realijoms yra visiškai nepritaikyta ir netgi daranti kliūtis nacionaliniam saugumui. Būtent taip pasisako Jeremy A. Rabkinas ir Arielas Rabkinas[13]. Vis dėlto dauguma kitų autorių, įskaitant ir Talino vadovo autorius, mano, kad ir tarptautinės teisės, ir tarptautinės humanitarinės teisės normos taikytinos ir kibernetiniams konfliktams / kibernetinės kovos veiksmams[14].

---

12 1929 m. Convention relative to the Treatment of Prisoners of War. Geneva, 27 July 1929 [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=0BDEDDD046FDEBA9C12563CD002D69B1&action=openDocument>.

13 Rabkin, J. A.; Rabkin, A. To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict. *Koret-Taube Task Force on National Security and Law* [interaktyvus]. [žiūrėta 2013-07-01]. <http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf>.

14 *Tallinn Manual*, *supra* note 9, p. 17.

Pritartume nuomonei, kad, nepaisant visų naujausių technologinių, visuomeninių, politinių tendencijų, kad pagrindinės keturios Ženevos konvencijos buvo priimtos dar 1949 m.[15], kai kurios jų normos ateina dar iš XIX a. vidurio ir iš tiesų atrodo beviltiškai pasenusios naujųjų ginkluotų konfliktų kontekste, yra tarptautinės humanitarinės teisės normų, pritaikytinų ir kibernetiniams konfliktams. Pirmiausia tai pasakytina apie tarptautinės humanitarinės teisės principus. Dar 1899 m. F. Martensas pateikė išlygą: „*Kol nebus skurtas pilnesnis karo įstatymų rinkinys, Aukštosios Susitariančios Šalys mano, kad yra svarbu pabrėžti, kad atvejais, kurių neapima šie jų priimti Nuostatai* (t. y. II Hagos konvencija dėl sausumos karo įstatymų ir papročių patvirtinti Sausumos karo nuostatai – *aut. past.*)*, gyventojai ir kovotojai lieka apsaugoti tarptautinės teisės principų, kurie kyla iš civilizuotų tautų įpročių, žmoniškumo įstatymų ir visuomenės sąžinės reikalavimų.*“[16] Truputį performuluota ši nuostata buvo perkelta ir į 1949 m. Ženevos konvencijų 1977 m. I papildomą protokolą dėl tarptautinių ginkluotų konfliktų aukų apsaugos[17] (toliau – I protokolas) 1 straipsnio 2 dalį bei 1949 m. Ženevos konvencijų 1977 m. II papildomo protokolo dėl netarptautinių ginkluotų konfliktų aukų apsaugos[18] (toliau – II protokolas) preambulę. Taigi, ši formuluotė reiškia, kad ginkluoto konflikto metu iš principo yra neįmanoma situacija, kurios tarptautinė humanitarinė teisė visiškai nereguliuotų. Tos pačios nuomonės vėliau laikėsi ir Tarptautinis Teisingumo Teismas Branduolinių bandymų konsultacinėje išvadoje, pasisakęs, jog „ginkluoto konflikto teisė taikoma visoms ginkluotos kovos formoms ir visiems ginklams, praeities, dabarties ir ateities[19]“, kadangi bet kokia kita išvada būtų nesuderinama su humanitariniais principais ir šios teisės tikslu (tai diktuoja tarptautinės humanitarinės teisės paskirtis). Taigi, net jeigu neturime specialiųjų normų, visada galime pasitelkti tarptautinės humanitarinės teisės principus: karinės būtinybės, atskyrimo, žmoniškumo, proporcingumo. Šie principai ne tik turi aiškų paprotinį pobūdį, jie užfiksuoti tarptautinės teisės aktuose ir teismų jurisprudencijoje. Todėl atskyrimo principas ir kibernetiniame kare reikš tą patį, ką ir įprastame kare: visada privaloma skirti karinius ir civilius objektus[20], net jeigu kibernetinio konflikto metu dėl to gali kilti didelių technologinių sunkumų (pavyzdžiui, kaip pažymi EastWest

15 1949 m. rugpjūčio 12 d. Ženevos konvencija dėl sužeistųjų ir ligonių padėties veikiančiose armijose pagerinimo, *Valstybės žinios*. 2000, Nr. 63-1905 (I ŽK); 1949 m. rugpjūčio 12 d. Ženevos konvencija „Dėl sužeistųjų, sergančiųjų ir skęstančiųjų ginkluotųjų pajėgų narių jūrose padėties pagerinimo“. *Valstybės žinios,* 2000, Nr. 63-1906 (II ŽK); 1949 m. rugpjūčio 12 d. Ženevos konvencija „Dėl elgesio su karo belaisviais“. *Valstybės žinios*. 2000, Nr. 63-1907 (III ŽK); 1949 m. rugpjūčio 12 d. Ženevos konvencija „Dėl civilių apsaugos karo metu“. *Valstybės žinios*. 2000, Nr. 63-1908 (IV ŽK).

16 Hague Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899 [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=CD0F6C83F96FB459C12563CD002D66A1&action=openDocument>.

17 1949 m. Ženevos konvencijų papildomas protokolas dėl tarptautinių ginkluotų konfliktų aukų apsaugos (I protokolas). *Valstybės žinios*. 2000, Nr. 63-1909.

18 1949 m. Ženevos konvencijų papildomas protokolas dėl tarptautinių ginkluotų konfliktų aukų apsaugos (II protokolas). *Valstybės žinios*. 2000, Nr. 63-1910.

19 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, para. 86, p. 259.

20 *Supra* note 17, 52 straipsnis; *supra* note 18, 13 straipsnis.

instituto ataskaitos ekspertai, vienas iš svarbių sprendimų, kuriuos valstybės turėtų rimtai apsvarstyti, – tai atskyrimas civilinės ir karinės kibernetinės infrastruktūros, kurios šiuo metu yra visiškai susipynusios[21]).

Taip pat kibernetinio ginkluoto konflikto metu gali būti taikomos ir konkrečios, tarptautinėse sutartyse įtvirtintos normos. Pavyzdžiui, tikrai galime teigti, kad kombatanto sąvoka naujųjų ginkluotų konfliktų kontekste tam tikrais aspektais yra pasenusi ir jai keliami kai kurie klasikiniai reikalavimai, pavyzdžiui, fiksuotas iš toli matomas ženklas[22] turi prasmės tik fiziniame mūšio lauke. Kibernetinių priemonių panaudojimo kontekste fizinio mūšio nėra, tad „iš toli matomas nuolatinis ženklas“ skamba absurdiškai (ypač jeigu pamėgintume tai įsivaizduoti vizualiai); lygiai taip pat atrodo netgi I Protokolo modifikuota, atnaujinta taisyklė, kad puolimo metu užtenka, jog priešininkas mato atvirai nešiojamą ginklą, jeigu asmuo nori išsaugoti kombatanto statusą ir kartu – teisę būti karo belaisviu[23], tad šių normų taikymas kibernetiniam karui jau neturi prasmės. Bet, pavyzdžiui, specialios taisyklės, kad negalima pulti sanitarinių įstaigų ir dalinių[24], kad puolimo metu reikia imtis atsargumo priemonių, kad kuo mažiau nukentėtų civiliai objektai[25] (beje, STUXNET atvejis tuo ir įdomus, kad virusas buvo nutaikytas daryti žalos būtent kariniam (ar bent jau mišrios paskirties) objektui – urano sodrinimo gamyklai[26]), kuo puikiausiai taikytina ir ginkluoto konflikto, kurio metu naudojamos kibernetinės priemonės, atveju.

Taigi, galime konstatuoti, kad kibernetinio ginkluoto konflikto metu tarptautinė humanitarinė teisė yra taikytina, nors ir ne visas jos normas įmanoma objektyviai pritaikyti kibernetinio konflikto realijoms, tačiau tai nereiškia, kad kibernetinis konfliktas vyktų teisiniame vakuume. Net jeigu nėra specialaus reguliavimo, pirmiausia taikytini bendrieji tarptautinės humanitarinės teisės (paprotiniai) principai.

2. Ar vien kibernetinis ginklo panaudojimas gali būti pripažintas ginkluotu konfliktu?

Tai yra bene įdomiausias klausimas, kurį kelia kibernetinis ginklas. Norėdami į jį atsakyti turime grįžti prie gana komplikuotos ginkluoto konflikto sąvokos ir ją įvertinti naujų realijų kontekste. Ginkluoto konflikto terminas tarptautinėje teisėje pirmą kartą

---

21 Rauscher, K. F.; Korotkov, A. *Working towards rules for governing cyber conflict. Rendering the Geneva and Hague Conventions in Cyberspace*. New York: EastWest Institute, 2011 [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.ewi.info/working-towards-rules-governing-cyber-conflict>.

22 *Supra* note 15, 4 str.

23 I protokolas, *supra* note 17, 44 str.

24 I ŽK, *supra* note 15, 19 str.

25 I protokolas, *supra* note 17, 57−58 str.

26 Fanelli, R.; Conti, G. A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict. *2012 4th International Conference on Cyber Conflict Proceedings*, *supra* note 6, p. 327.

pasirodė 1949 m. Ženevos konvencijose (2 ir 3 bendrieji straipsniai), tačiau nė viename tarptautinės teisės akte ši sąvoka nebuvo tiksliai apibrėžta.

Ženevos konvencijų komentare, parengtame Tarptautinio Raudonojo Kryžiaus komiteto, akcentuojama, kad bet koks nesutarimas tarp valstybių, sukeliantis ginkluotųjų pajėgų panaudojimą, yra ginkluotas konfliktas[27]. Šiame apibrėžime yra du esminiai elementai: subjekto – valstybės, ir priemonės – ginkluotųjų pajėgų. Šis apibrėžimas buvo patvirtintas ir Tribunolo buvusiai Jugoslavijai spręstoje *Tadic* byloje[28], taip pat kitose bylose. I protokolas taip pat tarptautiniais ginkluotais konfliktais nurodė laikyti atvejus, kai tautos, įgyvendindamos Jungtinių Tautų Chartijoje įtvirtintą tautų apsisprendimo teisę, kovoja su svetimšalių okupacija, kolonijine priespauda ar rasistiniu režimu[29], taigi, šalia valstybės atsiranda dar vienas subjektas – tautos, siekiančios nepriklausomybės. Situacija kiek kitokia, kai kalbame apie netarptautinį ginkluotą konfliktą. Šiuo atveju, vėlgi daugiausia pagal Jugoslavijos tribunolo jurisprudenciją, tokiu konfliktu laikytina užsitęsusi ginkluota prievarta tarp valstybės ir organizuotų disidentų grupių arba tarp organizuotų disidentų grupių[30]. Taigi, atsiranda papildomi kriterijai, tokie kaip „užsitęsusi ginkluota prievarta“ ir reikalavimas, kad disidentinė konflikto pusė būtų „organizuota“. Pateikę šiuos kriterijus, turime pažiūrėti, kaip jie siejasi su kibernetinio konflikto ypatybėmis.

Be jokios abejonės, kibernetinė jėga ar ginklas yra priemonė, kuri panaudojama ginkluotos kovos veiksmų metu. Tiek tarptautinis, tiek netarptautinis konfliktas kaip faktinę situacijos vertinimo esmę iškelia patį ginkluotos kovos buvimo momentą. Tačiau atkreiptinas dėmesys, kad tarptautiniam ginkluotam konfliktui nekeliamas joks intensyvumo ar trukmės laike kriterijus, t. y. pirmenybė tarsi atiduodama ginkluotos jėgos panaudojimo subjektui. Kitaip tariant, vos ne bet koks ginkluotas susirėmimas panaudojant valstybės ginkluotas pajėgas (bent vienos) prieš kitą bus tarptautinis ginkluotas konfliktas. Taigi, jeigu valstybės ginkluotosios pajėgos panaudos kibernetinį ginklą prieš kitą valstybę, tai gali būti tarptautinio ginkluoto konflikto pradžia. Tokios nuostatos laikomasi ir Talino vadove[31]. Kita vertus, kibernetinės priemonės gali būti labai įvairaus pobūdžio: pavyzdžiui, DDoS atakos − tai tiesiog serverių darbo trikdymas; tai gali būti slaptos informacijos ieškojimas ir pasisavinimas; tai gali būti ir įrangos gadinimas. Taigi, kur toji riba, kai kibernetinė priemonė tampa ginklu, savo poveikio jėga galinčiu išprovokuoti ginkluotą konfliktą? Štai čia mes susiduriame su tam tikru požiūriu komplikuota tarptautinės humanitarinės teisės ir tarptautinės viešosios teisės santykio problema, kuri kibernetinio ginklo atveju sukuria papildomų sunkumų.

---

27 Commentary - Art. 2. Chapter I: General provisions [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?viewComments=LookUpCOMART&articleUNID=41229BA1D6F7E573C12563CD00519E4A>.

28 *Prosecutor v. Dusko Tadic*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, para. 70.

29 I protokolas, *supra* note 17, 1 str.

30 *Prosecutor v. Dusko Tadic*, *supra* note 28.

31 *Tallinn Manual*, Rule 22, *supra* note 9, p. 71.

Kaip jau minėjome, tarptautinė humanitarinė teisė techniškai arba materialiai žvelgia į ginkluotą konfliktą kaip į ginkluotos jėgos panaudojimo faktą, kurio kriterijų ar požymių teisės aktuose nedetalizuoja. Toks sprendimas suprantamas, nes bet kokių jėgos panaudojimo fakto tikslesnių ribų nustatymas leistų jais galimai manipuliuoti. Tačiau ginkluotos jėgos panaudojimą, t. y. ginkluotos jėgos panaudojimo teisėtumą, reguliuoja ne tik tarptautinė humanitarinė teisė (*jus in bello*), bet ir tarptautinės viešosios teisės dalis, vadinama *jus ad bellum* (arba *jus contra bellum*). Būtent joje yra vartojamos tokios sąvokos kaip „jėga“ ir – mums bene svarbiausia – „ginkluotas užpuolimas“, įtvirtinta Jungtinių Tautų Chartijos[32] 51 straipsnyje kaip pagrindas teisei į savigyną. Problema ir ta, kad tarptautinė humanitarinė teisė siekia sąmoningai atsiriboti nuo *jus ad bellum* reguliavimo, vėlgi, dėl skaudžių istorinių pamokų, kai valstybės, net ir vykdydamos plataus masto ginkluotos kovos veiksmus ar okupacijas, nepripažindavo tokių veiksmų ir netaikydavo karo teisės (vienas ryškiausių pavyzdžių – 1939 m. Sovietų Sąjungos įvykdytas Lenkijos užpuolimas).

Teoriškai, kalbėdami vien apie tarptautinę humanitarinę teisę, mes turėtume ignoruoti „ginkluoto užpuolimo“ sąvoką, kadangi tarptautinė humanitarinė teisė turi savus terminus: bendro pobūdžio „ginkluotos kovos veiksmai“ (angl. *hostilities*) bei specifiškai apibrėžiamą „puolimą[33]“ (angl. *attack*). Tačiau „puolimas“ ginkluoto konflikto pradžiai nustatyti yra netinkamas, nes jo paskirtis tarptautinėje humanitarinėje teisėje – kitokia, jis skirtas apibrėžti taisykles, taikomas puolimo metu, o ne atskleisti konflikto pradžios momentą. Tuo tarpu „ginkluotos kovos veiksmų“ sąvoka normatyviai neapibrėžta[34] ir, vėlgi, aktuali ne tik ginkluoto konflikto kvalifikavimo momentui, bet ir visai jo eigai. Taigi, pradinis ginkluoto konflikto momentas, tas, nuo kurio turi būti pradėta visa apimtimi taikyti tarptautinė humanitarinė teisė, bent jau aiškumo prasme, sietinas ir su „ginkluoto puolimo“ sąvoka, kaip minėta, ateinančia iš tarptautinės viešosios teisės ir konkrečiai – savigynos instituto.

Kaip pastebi Michaelis N. Smith'as, dar *Nicaragua* byloje Tarptautinis Teisingumo Teismas pasakė, jog ginkluotas puolimas turi turėti tam tikrą mastą ir pasekmes[35]. Kitaip tariant, šiuo klausimu mes turime šiek tiek nutolti nuo humanitarinės teisės ir grįžti prie bendrųjų ginkluotos jėgos draudimo klausimų tarptautinėje teisėje. Iš tiesų, dabartinė tarptautinė teisė ginkluotą užpuolimą vertina daugiau mažiau per įprastinių ginklų (vadinamų „kinetiniais“), kurie sukelia pasekmes žmogui ar turtui, prizmę. Kaip rašo Y. Dinsteinas, yra būtinas tam tikras, minimalus ginkluotos jėgos lygis, kurį lai-

---

32 Jungtinių Tautų Chartija. *Valstybės žinios*. 2002, Nr. 15-557.

33 I protokolo 49 str.: „„Puolimai“ reiškia prievartos veiksmus priešininko atžvilgiu, nepaisant, ar tai daroma puolant, ar ginantis.“

34 Pagal Tarptautinio Raudonojo Kryžiaus Komiteto ekspertų parengtas Tiesioginio dalyvavimo ginkluotos kovos veiksmuose aiškinamąsias gaires pagal tarptautinę humanitarinę teisę, ginkluotos kovos veiksmai apibrėžiami kaip „kolektyviai konflikto šalių naudojamos priemonės ir būdai pakenkti priešui“. *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law*. Melzer, N. (ed.). Geneva: International Committee of the Red Cross, 2009, p. 43.

35 Schmitt, M. N. "Attack" as a Term of Art in International Law: The Cyber Operations Context. *2012 4th International Conference on Cyber Conflict Proceedings*, *supra* note 6, p. 288.

kytume ginkluotu puolimu[36], bet iš esmės tas lygis niekur nėra tiksliai apibrėžtas, taigi, jis vertinamas kiekvienu konkrečiu atveju. Ir, kaip juokauja tas pats autorius, jeigu šūvis į kitos valstybės teritoriją pataikė į medį arba tik užmušė karvę, tai nebus ginkluotas užpuolimas[37]. Perkeliant šį klausimą į kibernetinių priemonių kontekstą, klausimų kyla dar daugiau. Pavyzdžiui, kaip pastebi Louise'as Arimatsu, kenkiančios programos (angl. *malware*) nesukurtos taip, kad žudytų ar žalotų žmones, ir jos nebūtinai gadins ar naikins turtą. Be to, tai priklauso nuo to, kaip apibrėšim „turtą": ar jis apimtų tinklo sistemas, programas ir duomenis[38]? Taip, pasekmėmis kibernetinis puolimas irgi gali žudyti – pavyzdžiui, sutrikdžius traukinių kontrolės sistemą ir sukėlus avariją, kurioje buvo žmonių aukų, tačiau kaip vertintinas kibernetinis puolimas, kuris, pavyzdžiui, paveiks šalies bankų sistemą, bet nieko nenužudys, netgi nesugadins turto? Vis dėlto yra svarstymų, jog kibernetiniai puolimai, skirti sunaikinti ar sugadinti kitos valstybės kritines infrastruktūras, nors ir neatnešantys mirtinos žalos, gali būti laikomi ginkluotu užpuolimu[39], ir vien tai jau yra didelis tradicinės paradigmos poslinkis. Todėl vadinamasis „kinetinis" vertinimo kriterijus, kuris reiškia, kad puolimas būtų vertinamas per tai, ar įprastomis, kinetinėmis priemonėmis (sprogmenys, šaudmenys, raketos, bombos, kt.) galima pasiekti tokio paties rezultato – tinka tik iš dalies. Tai pastebėta jau seniai, ir Michaelis N. Schmitas dar 1999 m. suformulavo platų kibernetinio puolimo vertinimo kriterijų sąrašą, kuris paremtas vadinamuoju „pasekmių požiūriu" (angl. *effects-based approach*). Štai kokie pasiūlyti kriterijai:

Sunkumas – puolimo intensyvumas ir apimtis, t. y. kaip plačiai buvo paliesta infrastruktūra, kokią žalą atnešė, kiek pajėgumų naudoja ir kt.;

Trukmė – kaip ilgai puolimas ar jo sukeltos pasekmės truko;

Tikslingumas – kiek neigiamų pasekmių priežastis yra būtent puolimas;

Invazyvumas – kiek glaudžiai puolimas buvo nukreiptas būtent prieš valstybę;

Išmatuojamumas – kaip lengvai galima nustatyti, apskaičiuoti nuostolius;

Teisėtumo prezumpcija – vertinama, ar veiksmas yra teisėtas pagal tarptautinę teisę[40].

Kaip matome, šie kriterijai gana plačiai ir lanksčiai leidžia analizuoti incidentą ir pagal juos net ir puolimai, kurie iš pirmo žvilgsnio neatrodytų kaip „ginkluoti", galėtų jiems prilygti. Talino vadove šis klausimas sprendžiamas per du lygius: 11 taisyklėje nurodoma: „Kibernetinė operacija yra jėgos panaudojimas, kai jos apimtis ir pasekmės yra

36 Dinstein, Y. *War Aggression and Self Defence*. 4th ed. Cambridge University Press, 2005, p. 173.

37 *Ibid*., p. 175.

38 Arimatsu, L. A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. *2012 4th International Conference on Cyber Conflict Proceedings*, *supra* note 6, p. 97.

39 Melzer, N. *Cyber Warfare and International Law*. UNIDIR Books and Reports. Geneva: United Nations Institute for Disarmament Research, 2011, p. 15 [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=134218>.

40 Schmitt, M. N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*. 1998−1999, 37: 885−938, p. 913–915; kriterijų kritinę analizę žr. Ziolkowski, K. *Ius ad bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force. *2012 4th International Conference on Cyber Conflict Proceedings*, *supra* note 6, p. 301−307.

prilygintinos nekibernetinei operacijai, prilygstančiai jėgos panaudojimui[41]“, o analizei taikomi minėti kriterijai dar papildomi kriterijumi *karinis pobūdis*, kuris aiškinamas, kad arba ginkluotosios pajėgos panaudojo kibernetinį puolimą, arba jos buvo kibernetinio puolimo taikinys[42]. Tačiau reikia nepamiršti, kad ne kiekvienas jėgos panaudojimas yra prilyginamas ginkluotam užpuolimui, kuris turi lemti ir tarptautinės humanitarinės teisės veikimą visa apimtimi, todėl Talino vadovo 13 taisyklė (kalbanti apie savigyną), nurodo, kad savigyna galima tik tokiu atveju, jeigu kibernetinis užpuolimas prilygo ginkluotam užpuolimui.

Taigi, vis dėlto ginkluotos jėgos panaudojimo vertinimas, bent jau pradiniame etape, vykdomas per *jus ad bellum* prizmę. Teoriškai neįmanoma, kad ginkluotas užpuolimas pagal *jus ad bellum* nebūtų ginkluotas konfliktas. Kita vertus, nėra aiškaus atsakymo, ar mažesnio masto užpuolimas (t. y. mažesnio masto ginkluotos jėgos panaudojimas) negalėtų būti ginkluotas konfliktas pagal „ginkluotos kovos veiksmų“ (angl. *hostilities*) požymį, kuris jau priklauso tik tarptautinei humanitarinei teisei. Čia svarbu atsiminti, kad ginkluoto konflikto galimo apibrėžimo tikslas yra kitoks nei ginkluoto užpuolimo – kaip jau minėjome, ginkluotas užpuolimas leidžia imtis savigynos (atsakomojo ginkluotos jėgos naudojimo), tuo tarpu ginkluoto konflikto, kurį sukelia ginkluotos kovos veiksmai, sampratos pirminė paskirtis – jo aukų apsauga. Ir etiškai, ir teoriškai galima būtų samprotauti, kad ginkluoto konflikto aukų apsauga turėtų atsirasti visais atvejais, kai atsiranda ginkluotos jėgos panaudojimo aukų (sužeistieji, žuvusieji) – tai atitinka ir Ženevos konvencijos kūrėjų siekius[43]. Talino vadovo kūrėjai irgi nurodo, kad „riba turi būti pakankamai žema“[44], kaip tokio atvejo pavyzdys nurodomas gaisro sukėlimas kibernetinėmis priemonėmis kariniame objekte. Mūsų nuomone, vertindami „ginkluotos kovos veiksmus“ kibernetinių priemonių kontekste kaip ginkluoto konflikto pradžią, mes taip pat galėtume naudoti „Schmith’o kriterijus“, minėtus prie „ginkluoto užpuolimo“. Tačiau čia susiduriame ir su klausimu, kad, vienai pusei pradėjus ginkluotą konfliktą, kita pusė turi teisę ir gintis, ir užpuoliką pulti. Taigi, pagal naująjį požiūrį, siūlomą doktrinos atstovų, gali būti taip, kad veiksmai, nesukėlę mirčių ar turto fizinio sunaikinimo (pavyzdžiui, sutrikdyta ar net sunaikinta informacinė bankininkystės sistema), gali sulaukti ir kinetinio atsako, kuris tokias pasekmes sukels. Vadinasi, galima situacija, kai tarptautinė humanitarinė teisė pradės veikti visa apimti ir dar nesant aukų. Galbūt tai ir gerai, ypač atsižvelgiant į šios teisės turimą prevencinę aukų apsaugos funkciją.

Tačiau taip pat reikia atkreipti dėmesį, kad ginkluotos kovos veiksmų vertinimas svarbus ir kituose, ne tik savigynos ar ginkluoto konflikto pradžios kontekstuose (pavyzdžiui, jis svarbus ir ginkluoto konflikto procese, kai į ginkluotos kovos veiksmus įsitraukia civiliai, tiesiogiai dalyvaujantys ginkluotoje kovoje (pavyzdžiui, reikia įvertinti, ar civilio atliktas veiksmas buvo „ginkluotos kovos veiksmai“); netarptautinio ginkluoto konflikto kontekste (kiek disidentai pajėgūs vykdyti kovos veiksmus).

---

41 *Tallinn Manual*, *supra* note 9, p. 47.

42 *Ibid.*, p. 51.

43 Commentary - Art. 2. Chapter I: General provisions, *supra* note 27.

44 *Tallinn Manual*, *supra* note 9, p 74−75.

Netarptautinio ginkluoto konflikto atveju ginkluotos kovos veiksmams turime dar papildomą kriterijų – užsitęsusi ginkluota prievarta[45] (angl. *protracted armed violence*), t. y. keliamas ir tam tikras prievartos intensyvumo kriterijus, kuris šiuo atveju apibrėžiamas labiau prievartos trukme, o ne mastu[46]. Tačiau niekur toji trukmė nėra nusakyta tiksliai ir vėl paliekama konkretaus atvejo analizei. *Haradinaj* byloje Jugoslavijos tribunolas pasisakė, kad intensyvumą atspindi susirėmimų skaičius, trukmė, aktyvumas, naudojamos ginkluotės ir įrangos rūšys, pajėgų dydis, aukų skaičius, Jungtinių Tautų Saugumo Tarybos įsikišimas ir pan.[47] Turbūt netgi galime teigti, kad netarptautinio ginkluoto konflikto kvalifikavimui prievartos, „tinkamos“ netarptautinio ginkluoto konflikto kvalifikavimui, trukmės nustatymui, svarbesnis yra ne materialusis, o būtent subjekto kriterijus, kadangi tik kai disidentai pasiekia tam tikrą organizuotumo lygį ir jų veiksmų nebegalime vertinti kaip sporadiškų prievartos veiksmų, riaušių ar neramumų[48], galime pradėti kalbėti apie netarptautinį ginkluotą konfliktą. Taigi, netarptautinio ginkluoto konflikto metu toji „užsitęsusi prievarta“ turi kilti iš specialaus subjekto – organizuotų disidentų. Organizuotumo klausimu Jugoslavijos tribunolas *Haradinaj* ir ypač *Limaj* bylose akcentavo, jog disidentų organizuotumą nurodo komandinių struktūrų buvimas, disciplinos taisyklės, grupės veikimas kaip vieningo subjekto, gebančio planuoti, koordinuoti, vykdyti karines operacijas[49]. Todėl dabar grįžkime prie subjektų klausimų ir jų ypatybių kibernetinių priemonių panaudojimo kontekste.

Taigi, faktinis ginkluotos jėgos panaudojimas – tik vienas ginkluoto konflikto, tiek tarptautinio, tiek netarptautinio, požymis. Bet taip pat svarbu ir kas ginkluotą jėgą naudoja. Tarptautinio ginkluoto konflikto atveju mažiausiai abejonių kyla tuomet, kai ginkluotą jėgą naudoja valstybės ginkluotosios pajėgos, su kuriomis mes įpratę sieti ginklus. Tačiau kibernetinių priemonių kontekste (taip pat ir, pavyzdžiui, nepilotuojamų aparatų) neretai veikia ir kiti subjektai – pavyzdžiui, CŽV. Talino vadovo kūrėjų manymu, jie taip pat laikytini valstybės ginkluotųjų pajėgų dalimi[50], nors įprastai tarptautinė humanitarinė teisė būtent valstybių vidaus teisei palieka apibrėžimą, kas yra „ginkluotosios pajėgos“. Matyt, Talino vadove tokia išvada daroma remiantis valstybių atsakomybės principais, kadangi tokiais atvejais šie subjektai tarsi vykdo priskirtas funkcijas, kurios paprastai priklauso kitoms institucijoms, tačiau nuo to neturėtų pakisti vertinimas. Sudėtingiau, kai į jėgos naudotojų ratą patenka subjektai, kurių ryšys su valstybe ar jos institucijomis būna visai kitokio pobūdžio. Pavyzdžiui, pasitelktos privačios kompanijos, kiti įvairūs „nevalstybiniai subjektai“ ar net tiesiog kompiuterių entuziastai, individų grupės, net pavieniai individai. Pavyzdžiui, 2007 m. kai buvo pradėti kibernetiniai puolimai prieš Estijos valstybės ir bankų tinklalapius, tai darė ir aktyvistai, vedami pačių įvairiausių motyvų[51]. Tarptautinėje teisėje yra mechanizmai, kai valstybė

45 *Prosecutor v. Dusko Tadic*, *supra* note 28.

46 Moir, L. *The Law of Internal Armed Conflict*. Cambridge University Press, 2004, p. 43.

47 *Prosecutor v. Haradijan*, Trial Chamer Judgement, IT-04-84-T, 3 April 2008, para. 49.

48 Šiuo atveju remiamasi II protokolo 1 straipsniu.

49 *Prosecutor v. Limaj*, Trial Chamber Judgement, IT-03-66-T, November 20, 2005, paras. 94−129.

50 *Tallinn Manual*, *supra* note 9, p. 75.

51 Kadangi 2007 m. Estijos įvykius interneto erdvėje teko stebėti „iš arti“, galime patvirtinti, kad bent dalis „aktyvistų“, organizavusių įvairias kibernetines priemones, buvo tiesiog Rusijos piliečiai, užsimanę

laikoma atsakinga ir už privačių asmenų veiksmus (pavyzdžiui, jeigu valstybė prisiima atsakomybę ar jeigu asmenys *de facto* veikė kaip valstybės organas[52]), tačiau tai vis dėlto yra išimtis, o ne taisyklė. Tad bet kuriuo atveju, norėdami vienokio ar kitokio subjekto kibernetinio puolimo veiksmus priskirti valstybei ginkluoto konflikto kontekste, turėsime remtis įprastiniais *efektyvios kontrolės*[53] ar *bendrosios kontrolės* testais, kurie šiuo metu koegzistuoja skirtingų tarptautinių teismų praktikoje. Jeigu šių veikų valstybei priskirti negalėsime, tuomet negalėsime konstatuoti tarptautinio ginkluoto konflikto.

Ir čia, mano manymu, gali kilti rimtas klausimas, ar minėti testai pakankami kibernetinio konflikto atvejais. Pavyzdžiui, *bendrosios kontrolės* testas reikalauja, kad valstybė turi koordinuoti, kartu planuoti karines operacijas su tam tikra grupuote (nevalstybiniu subjektu) ir pan.[54] Tačiau, kaip rodo ir Estijos situacijos pavyzdys, valstybės įsikišimas gali būti ir gana nedidelis, o kibernetinės priemonės – pakankamai grėsmingos, ypač nepasirengusiam puolimo objektui. Juolab, kibernetinėms priemonėms faktiškai neturint geografinių apribojimų, priskyrimo klausimas tampa ypatingai sudėtingas, pirmiausia technologiniu požiūriu, o jis egzistuojantiems priskyrimo būdams irgi nepalankus: kibernetinis puolimas gali būti suorganizuotas per tūkstančius užvaldytų kompiuterių iš pačių įvairiausių pasaulio vietų. Be to, kaip jau buvo minėta, išanalizuoti atakų šaltinį, programinės įrangos kūrėjus reikia daug laiko. Pavyzdžiui, įtariama, kad prie STUXNET viruso kūrimo galėjo prisidėti specialiosios JAV ir Izraelio tarnybos, bet konkrečių įrodymų iki šiol nėra, tik loginės prielaidos[55].

Ypač sudėtingas subjekto klausimas gali kilti netarptautinio ginkluoto konflikto kontekste. Kaip jau minėjome ir kaip pažymėta *Tadic* ir kitose Tribunolo buvusiai Jugoslavijai bylose, netarptautinio ginkluoto konflikto atveju disidentai turi būti „organizuoti“. Organizuotumas šiuo atveju taip pat apima, kad disidentai yra pajėgūs įgyvendinti bent jau bendrą Ženevos konvencijų 3-iąjį straipsnį (minimalias humanitarines garantijas)[56]. II protokolas[57] reikalauja, kad disidentai dar ir kontroliuotų teritoriją[58], tačiau šiuolaikinių ginkluotų konfliktų kontekste, matyt, tai pamažu taps fakultatyviu, o ne privalomu požymiu. „Kliba“ ir kitas įprastinis kriterijus – geografinis – t. y. kad netarptautinis ginkluotas konfliktas turėtų vykti vienos valstybės teritorijoje (pavyzdžiui, būtent prie šios išvados priėjo JAV Aukščiausiasis teismas *Hamdan* byloje[59]). Kita vertus,

---

„nubausti“ Estiją už „Bronzinio kario“ monumento iškeldinimą. Kitaip tariant, tai buvo tarsi „pilietinė akcija“, kuriai, žinoma, netrukdė ir Rusijos vyriausybė.

52 Žr. (Draft) Articles on Responsibility of State for Internationally Wrongful Acts, UN Doc. A/RES/56/83 (12 Dec. 2001), Art. 5, 8, 9.

53 Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*). Merits, Judgment. I.C.J. Reports 1986, p. 14, paras. 218–220.

54 *Prosecutor v. Dusko Tadic*, Appeals Chamber Judgement, IT-94-1-AR72, 27 February 2001, paras. 131, 145.

55 Cavelty, M. D. The Militarisation of Cyberspace: Why Less May Be Better. *2012 4th International Conference on Cyber Conflict Proceedings*, *supra* note 6, p. 148.

56 Moir, L., *supra* note 46, p. 43.

57 Tačiau reikia nepamiršti, kad II protokolas reguliuoja siauresnę situaciją nei ŽK bendras 3 str.

58 II protokolas, *supra* note 18, 1 str.

59 *Hamdan v. Rumsfeld* 126 S Ct 2749 (2006).

jau ir dabar disidentų organizuotumo kriterijus yra nebeaiškus. Pavyzdžiui, JAV teismų praktikoje buvo pripažinta, kad JAV ir Al Qaeda yra netarptautinio ginkluoto konflikto šalys, nors Al Qaeda yra apibūdinama kaip „palaidas tinklas“ (angl. *loose network*), ir apie kažkokią aiškią struktūrą, discipliną ar atsakomybę kalbėti ypač sudėtinga. Dar sudėtingiau bus, kai reikės vertinti vien kibernetinių kovotojų tinklus. Atsižvelgiant į tokius fenomenus kaip atvirojo kodo bendruomenės, jau minėtą „pilietinį aktyvizmą“, identifikuoti tokius darinius kaip organizuotą subjektą būtų itin drąsu. Mūsų manymu, įvertinant visą netarptautinio ginkluoto konflikto požymių neapibrėžtumą, labai maža tikimybė, kad jį galėtų sukelti vien kibernetinės priemonės.

3. „Kibernetinio kovotojo“ statuso problema

Tarptautinė humanitarinė teisė numato du pagrindinius asmenų statusus: tai kombatantas ir civilis. Pagrindinis mums aktualus jų skirtumas – kombatantas turi teisę dalyvauti ginkluotoje kovoje ir būti puolamas, civilis – turi būti saugomas ir neturi teisės dalyvauti ginkluotoje kovoje. Netarptautinio ginkluoto konflikto situacijoje kombatanto sąvokos mes nevartojame, bet iš esmės vis tiek tenka spręsti, kada prieš asmenį galima naudoti ginkluotą jėgą.

Kibernetinio konflikto situacijoje turbūt nekils didelių problemų, kai kalbėsime apie aiškius kombatantus – t. y. valstybės ginkluotųjų pajėgų narius, kurie naudotų kibernetinį ginklą. Tačiau, kaip jau ne kartą minėta, kibernetinės priemonės yra kompleksinis reiškinys. Pavyzdžiui, jeigu kalbėtume apie kenkiančią programą, prie jos gali dirbti daug žmonių: vieni projektuoja programos architektūrą, antri rašo kodą ar jo dalis, treti sukuria galimybes, kaip įdiegti ją į apsaugotas sistemas, ir pan. Galimas daiktas, kad šie asmenys bus iš skirtingų institucijų ir dažnai net nežinos, kam bus naudojamas jų galutinis produktas. Tad kas bus atsakingas už tokį kibernetinį ginklą? Jį panaudojęs, jį sukūręs, sukūręs jo dalį ar pan.? Be to, kibernetinė kova yra itin palanki aplinka į kovą įsitraukti bet kam. Net ir žmogui, pakankamai neįvertinančiam savo dalyvavimo svarbos. Kaip jau minėjome, kibernetinio karo metu prasmę praranda net ir elementariausi klasikiniai kombatanto statuso reikalavimai, įtvirtinti I Protokole (nešioti ginklą atvirai karinės operacijos metu kai mato priešas[60]). Kas juos pakeis, kai reikės spręsti, ar galima prieš asmenį naudoti ginkluotą jėgą ir kokį statusą jam suteikti? Teisinio manevro laisvė čia nėra plati. Seanas Wattsas siūlo, kad afiliacija su valstybe (matyt, platesnio supratimo nei dabar reikalaujama iš kombatanto) turėtų tapti pagrindiniu kriterijumi[61]. Mes prognozuotume, kad tais atvejais, kai asmuo dalyvaus kibernetiniame konflikte, bet nepriklausys valstybės ginkluotosioms pajėgoms, teks remtis arba ginkluotos grupės nario, vykdančio nuolatinę kovinę funkciją („nuolatinės kovinės funkcijos“), koncepcija, arba vadinamąja „civilio, tiesiogiai dalyvaujančio ginkluotos kovos

60 I protokolas, *supra* note 17, 44 str.

61 Watts, S. The Notion of Combatancy in Cyber Warfare Watts. *2012 4th International Conference on Cyber Conflict Proceedings*, *supra* note 6, p. 247.

veiksmuose“, koncepcija. Pirmoji koncepcija savo esme panaši į kombatanto (funkciškai: nuolatinė priklausomybė grupei (verbavimas, integracija į struktūrą, paklusimas įsakymams, dalyvavimas operacijose, faktinis ginkluotos jėgos naudojimas[62]), tačiau toks asmuo vis tiek neįgyja kombatantui taikomos teisinės apsaugos, o tik praranda apsaugą nuo puolimo. Tokių asmenų pavyzdžiu kibernetinio konflikto kontekste galėtų būti žmonės, kurie tikslingai suvienija pastangas atlikti kovos veiksmus kibernetinėje erdvėje. Sakyčiau, kad per šį statusą reikėtų vertinti ir privačių karinių / saugumo kompanijų personalą, jeigu jis įtraukiamas į kibernetinės kovos veiksmus ir jeigu valstybė kitaip neapibrėžė jų statuso, tarkim, pagal nacionalinę teisę. Tuo tarpu civilio, tiesiogiai dalyvaujančio ginkluotos kovos veiksmuose, koncepcija, kildinama iš I protokolo[63], apibrėžia situacijas, kai civilis tam tikram momentui įsitraukia į ginkluotą kovą ir to pagrindu praranda apsaugą nuo puolimo. Šiuo atveju vertinama, ar civilio veiksmai atitiko reikiamą žalos lygį (t. y. žala turi neigiamai paveikti karines operacijas ar pajėgumus arba sukelti saugomų asmenų ar objektų mirtį, sužalojimus, sunaikinimą); turėjo tiesioginį priežastinį ryšį (ryšys tarp veikos ir žalos) ir sąsają su ginkluota kova (t. y. aktu siekiama padėti vienai konflikto šaliai ir trukdyti kitai)[64]. Tokio asmens pavyzdžiu galėtų būti kompiuterių entuziastas, epizodiškai nusprendęs padėti kuriai nors kovojančiai pusei (nesvarbu, iš idėjos ar už atlyginimą), pavyzdžiui, nutupdyti nepilotuojamą skraidantį aparatą. Toks asmuo teisėtu taikiniu bus tik tol, kol veikia konflikto pusės naudai.

Žinoma, šios koncepcijos nėra idealios išeitys[65], kita vertus, jų gairės leidžia šiek tiek aiškiau apibrėžti jėgos naudojimo prieš tokius asmenis ribas ir kriterijus. „Nuolatinės kovinės funkcijos“ koncepciją susiejus su karo įstatymų ir papročių laikymųsi, galima būtų svarstyti apie kvazikombatanto statusą, nors valstybės iki šiol tokiems asmenims suteikdavo šį statusą tik konkrečiose situacijose (pavyzdžiui, netraukdavo baudžiamojon atsakomybėn vien už ginkluotos jėgos panaudojimą, sulaikytiems taikydavo statusą, analogišką karo nelaisvei). Vertėtų pabrėžti, jog realus kovojančių ir nekovojančių atskyrimas kibernetiniame konflikte pirmiausia aktualus kibernetinių kovotojų atžvilgiu yra tik tada, kai prieš juos naudojama kinetinė jėga (pavyzdžiui, identifikuojamas atakų centras ir jis puolamas įprastinėmis karinėmis priemonėmis). Wattsas teisingai pastebi, kad didžiausias pavojus kibernetiniame kare kyla ne dėl kovotojų / civilių neatskyrimo, o dėl to, kad kibernetinėje erdvėje nėra aiškiai atskirtos karinės ir civilinės infrastruktūros, be to, čia kaip niekur kitur patogu civiliais ištekliais maskuoti karinius objektus[66].

---

62 *Interpretive guidance*, *supra* note 34, p. 43.

63 I protokolas, *supra* note 17, 53 str. 3 d.

64 *Interpretive guidance*, *supra* note 34, p. 46−68.

65 Žr. Prescott, J. M. Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States? *2012 4th International Conference on Cyber Conflict Proceedings*, *supra* note 6, p. 255−259.

66 Watts, S., *supra* note 61, p. 247.

Išvados

Kibernetiniai ginkluoti konfliktai arba kibernetinių priemonių panaudojimas tradiciniame ginkluotame konflikte, naujas reiškinys vien tik dėl to, kad tai – naujas reiškinys, nėra teisiškai nereguliuojamas. Tarptautinė humanitarinė teisė jau turi mechanizmus, leidžiančius jos normas (ypač paprotinius principus) taikyti naujiems fenomenams. Tačiau, žinoma, atsiranda ir klausimų, kuriuos dabartinis reguliavimas gali išspręsti tik labai apytikriai. Vienas iš esminių klausimų – ar vien kibernetinėmis priemonėmis galima sukelti ginkluotą konfliktą. Atsižvelgiant į tai, kad tikslaus reguliavimo šiais klausimais nėra netgi įprastinių ginkluotos kovos veiksmų atveju, kibernetinis „mūšio laukas" šį klausimą daro dar sudėtingesnį. Vis dėlto atrodo, kad ginkluoto konflikto kvalifikavimo paradigma patirs pokyčių, paremtų „pasekmių požiūriu", t. y. ateityje ginkluotą konfliktą vertinsime ne tik per tradicinę žalos žmonėms / turtui, sukeltos kinetinės jėgos, prizmę, bet teks pasitelkti ir papildomus kriterijus, leidžiančius ginkluotu konfliktu laikyti situacijas, nesukeliančias tradicinės žalos. Manytume, didžiausia problema, jog šis pokytis gali sudaryti sąlygas būtent kinetinės jėgos panaudojimui, kai į virtualų puolimą nebus teisinių kliūčių atsakyti realia jėga. Kita vertus, tai pastūmėja tarptautinę humanitarinę teisę arčiau prevencinės paskirties įgyvendinimo: pradėti aukas saugoti anksčiau, nei jos realiai atsirado. Neabejotina, kad kibernetinių ir kibernetizuotų ginkluotų konfliktų kontekste pokyčius patirs ir kiti institutai, konkrečiai – kombatanto (bei asmens, naudojančio ginkluotą jėgą) institutas. Klasikiniai identifikavimo kriterijai kibernetiniame „mūšio lauke" tampa nebetinkami, o iš esamos reguliavimo bazės labiausiai tam tiktų pritaikyti „nuolatinio kovotojo" bei „civilio, tiesiogiai naudojančio ginkluotą jėgą" koncepcijas. Tiesa, šios koncepcijos yra išvestinės iš skurdaus reguliavimo, tačiau jos suformuluoja svarbias gaires, leidžiančias spręsti tokių asmenų apsaugos klausimus.

Literatūra

1929 m. Convention relative to the Treatment of Prisoners of War. Geneva, 27 July 1929 [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=0BDEDDD046FDEBA9C12563CD002D69B1&action=openDocument>.

1949 m. rugpjūčio 12 d. Ženevos konvencija „Dėl elgesio su karo belaisviais". *Valstybės žinios*. 2000, Nr. 63-1907.

1949 m. rugpjūčio 12 d. Ženevos konvencija „Dėl sužeistųjų, sergančiųjų ir skęstančiųjų ginkluotųjų pajėgų narių jūrose padėties pagerinimo". *Valstybės žinios*. 2000, Nr. 63-1906.

1949 m. rugpjūčio 12 d. Ženevos konvencija „Dėl civilių apsaugos karo metu". *Valstybės žinios*. 2000, Nr. 63-1908.

1949 m. rugpjūčio 12 d. Ženevos konvencija dėl sužeistųjų ir ligonių padėties veikiančiose armijose pagerinimo. *Valstybės žinios*. 2000, Nr. 63-1905.

1949 m. Ženevos konvencijų papildomas protokolas dėl tarptautinių ginkluotų konfliktų aukų apsaugos (I protokolas). *Valstybės žinios*. 2000, Nr. 63-1909.

1949 m. Ženevos konvencijų papildomas protokolas dėl tarptautinių ginkluotų konfliktų aukų apsaugos (II protokolas). *Valstybės žinios*. 2000, Nr. 63-1910.

Anderson, N. Massive DDoS attacks target Estonia; Russia accused. *Arstechnica.com* [interaktyvus]. [žiūrėta 2013-07-01]. <http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/>.

Arimatsu, L. A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

(Draft) Articles on Responsibility of State for Internationally Wrongful Acts, UN Doc. A/RES/56/83 (12 Dec. 2001).

Cavelty, M. D. The Militarisation of Cyberspace: Why Less May Be Better. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

Commentary - Art. 2. Chapter I: General provisions [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?viewComments=LookUpCOMART&articleUNID=41229BA1D6F7E573C12563CD00519E4A>.

Dinstein, Y. *War Aggression and Self Defence*. 4th ed. Cambridge University Press, 2005.

Fanelli, R.; Conti, G. A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

Fuks, E. Išvada po susitikimo su prezidente: vargu ar apsiginsime nuo didesnės atakos. *delfi.lt* [interaktyvus]. [žiūrėta 2013-06-04]. <http://www.delfi.lt/news/daily/lithuania/isvada-po-susitikimo-su-prezidente-vargu-ar-apsiginsime-nuo-didesnes-atakos.d?id=61545466>.

Haddick, R. This Week at War: Lessons from Cyberwar I. *Foreign Policy* [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i>.

Hague Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899 [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=CD0F6C83F96FB459C12563CD002D66A1&action=openDocument>.

Hamdan v. Rumsfeld 126 S Ct 2749 (2006).

Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law. Melzer, N. (ed.). Geneva: International Committee of the Red Cross, 2009.

Įsteigta Kibernetinio saugumo taryba. Lietuvos Respublikos vidaus reikalų ministerija [interaktyvus]. [žiūrėta 2013-07-09]. <http://www.vrm.lt/go.php/lit/Isteigta-kibernetinio-saugumo-taryba-/830>.

Jungtinių Tautų Chartija. *Valstybės žinios*. 2002, Nr. 15-557.

Kushner, D. The Real Story of Stuxnet. *IEEE Spectrum* [interaktyvus]. [žiūrėta 2013-07-01]. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996.

Liles, S.; Dietz, J. E.; Rogers, M.; Larson, D. Applying Traditional Military Principles to Cyber Warfare. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

Melzer, N. *Cyber Warfare and International Law*. UNIDIR Books and Reports. Geneva: United Nations Institute for Disarmament Research, 2011.

Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*). Merits, Judgment. I.C.J. Reports 1986.

Moir, L. *The Law of Internal Armed Conflict*. Cambridge University Press, 2004.

Prescott, J. M. Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States? *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

Prosecutor v. Dusko Tadic, Appeals Chamber Judgement, IT-94-1-AR72, 27 February 2001.

Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995.

Prosecutor v. Haradijan, Trial Chamer Judgement, IT-04-84-T, 3 April 2008.

Prosecutor v. Limaj, Trial Chamber Judgement, IT-03-66-T, November 20, 2005.

Rabkin, J. A.; Rabkin, A. To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict. *Koret-Taube Task Force on National Security and Law* [interaktyvus]. [žiūrėta 2013-07-01]. <http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf>.

Rauscher, K. F.; Korotkov, A. *Working towards rules for governing cyber conflict. Rendering the Geneva and Hague Conventions in Cyberspace*. New York: EastWest Institute, 2011.

Schmitt, M. N. "Attack" as a Term of Art in International Law: The Cyber Operations Context. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

Schmitt, M. N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*. 1998−1999, 37: 885−938.

Tallinn Manual on the international Law Applicable to Cyber Warfare. Schmitt, M. N. (ed.). Cambridge University Press, 2013.

Traynor, I. Russia accused of unleashing cyberwar to disable Estonia. *The Guardian* [interaktyvus]. [žiūrėta 2013-07-01]. <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.

Watts, S. The Notion of Combatancy in Cyber Warfare Watts. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

Ziolkowski, K. *Ius ad bellum* in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force. *2012 4th International Conference on Cyber Conflict Proceedings*. Czosseck, C.; Ottis, R.; Ziolkowski, K. (eds.). Tallinn: NATO CCD COE Publications, 2012.

THE INFLUENCE OF USING CYBER TECHNOLOGIES IN ARMED CONFLICTS ON INTERNATIONAL HUMANITARIAN LAW

Justinas Žilinskas

Mykolas Romeris University, Lithuania

Summary. *Cyber warfare is becoming a new reality with new battles fought everyday on virtual battlefields. For a century and a half, International Humanitarian Law has been a sentry for victims of wars guaranteeing their legal protection from the calamities of war, trying hard to respond to Clausewitz's "chameleon of war". Cyber conflict marks new chameleon's colour together with the unmanned aerial vehicles, autonomic battle systems and other technologies deployed on battlefields. However, it would be greatly erroneous to claim that the International Humanitarian Law may not apply to the new phenomena just because it is caused by the advanced technology. Even if the Geneva Conventions of 1949 are already sixty years old, the International Humanitarian Law in itself has at minimum customary response*

mechanism, granting, in a spirit of Marten's clause, protection and authority of the principles of international law derived from established custom, from the principles of humanity and from dictates of public conscience (Protocol I).

Notwithstanding, some more complicated fundamental issues also have to be addressed: how the use of cybernetic weapons and means may affect the classic notion of armed conflict? How it can be interpreted in the light of new technologies, i.e. can we still rely on a classic understanding of weapon's kinetic effect as the main element, or shall we embrace effects-based "Schmitt's criteria". If it so happens, will it make an act without apparent damage to a person/property equal to military hostilities, required by the armed conflict notion and justify the real-life response to it. The effective or overall control tests were used for the attribution of non-state actor's activity to the state party of an armed conflict but these tests might not meet its purpose in the virtual battlefield of loose networks and open-source communities. If the concept of armed conflict is treated more flexibly, other changes (including issues of attribution) may follow, as well. Perhaps this is the way how the combatant institute will evolve. With classic combatant's criteria impossible to apply on virtual battlefields, one of the options would be to elaborate concepts of "constant combat function" and "direct participation in hostilities" more precisely, as well as to reconsider state's affiliation requirements.

Keywords: *armed conflict, cyber conflict, international humanitarian law, cyber weapon.*

Justinas Žilinskas, Mykolo Romerio universiteto Teisės fakulteto Tarptautinės ir Europos Sąjungos teisės instituto profesorius. Mokslinių tyrimų kryptys: tarptautinė humanitarinė teisė, naujieji ginkluotieji konfliktai, Tarptautinis baudžiamasis teismas.

Justinas Žilinskas, Mykolas Romeris University, Faculty of Law, Institute of International and European Union Law, Professor. Research interests: international humanitarian law, modern armed conflicts, International Criminal Court.