OSVRT NA TALLINNSKI PRIRUČNIK O MEĐUNARODNOM PRAVU PRIMJENJIVOM NA KIBERNETIČKO RATOVANJE

Pregledni znanstveni rad

UDK 355.4
004.056
004.7
341.3

Primljeno: 3. travnja 2017.

Ratimir Prpić*

U ovome članku autor daje osvrt na osnovne postavke Tallinnskog priručnika o međunarodnom pravu primjenjivom na kibernetičko ratovanje. Prvi dio bavi se njegovim donošenjem, strukturom, pravnim obuhvatom te zabranom uporabe sile i pravom na samoobranu. Zatim se prikazuju temeljne odlike usvojenih pravila i pratećih komentara. U nastavku autor govori o autoritetu i općem značaju tog Priručnika. U završnom dijelu iznosi se ocjena njegove trenutačne uspješnosti te se ukratko sažimaju najvažnije spoznaje i činjenice prethodno iznesene u odgovarajućim analitičkim poglavljima članka.

Ključne riječi: kibernetičko ratovanje, *lex lata*, međunarodni priručnik, uporaba sile

1. UVOD

Dinamika i sveobuhvatnost tehnološkog razvoja osobito dolazi do izražaja na području komunikacijske i informacijske tehnologije, kojima su današnja moderna društva duboko prožeta.[1] Kibernetički prostor jedno je od određujućih obilježja suvremenog života i ključno područje djelovanja svjetskog gospodarstva, a rastom njegove važnosti jača i svijest o potrebi zajedničkog djelovanja radi jačanja sigurnosti u tome prostoru.[2] Zato mnoge zemlje imaju donesene i detaljno razrađene nacionalne strategije i formirane sustave kibernetičke sigurnosti.[3] Moderna su društva postala ovisna o računalima, no ta se „digitalna revolucija" ne odnosi samo na civilnu infrastrukturu, poput kućanstava, korporacija ili sveučilišta koja koriste kibernetički prostor, nego i na oružane snage.[4] Stoga kibernetička obrana postaje sve važniji dio nacionalnih i međunarodnih strategija

* Ratimir Prpić, dip.iur., polaznik poslijediplomskog doktorskog studija na Pravnom fakultetu Sveučilišta u Zagrebu

[1] Nacionalna strategija kibernetičke sigurnosti, str. 2 (tekst Odluke o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za njezinu provedbu u: „Narodne novine", broj: 108/2015).

[2] Vuković, H., *Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj*, u: National Security and the Future, vol. 13, br. 2, str. 12-13.

[3] V. Lewis, J., A., Timlin, K., *Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization*, 2011.

[4] Roscini, M., *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, str. 6.

obrane.[5] Nadalje, iz postojećih se procjena pravnih stručnjaka zaključuje da kibernetičko ratovanje postaje nova bitna tema u raspravama o daljnjem razvoju pozitivnog međunarodnog prava i međunarodne sigurnosti.[6] Neki autori ugroze u kibernetičkom prostoru dijele na četiri kategorije, i to: I.) kibernetički kriminal, II.) kibernetičku špijunažu, III.) kibernetički terorizam i IV.) kibernetičko ratovanje.[7] U takvim se okolnostima na poticaj jedne višenacionalne ustanove, ustrojene u okvirima Organizacije Sjevernoatlantskog ugovora (u daljnjem tekstu: NATO), okupila skupina stručnjaka i nakon višegodišnjeg rada izradila moderan međunarodni dokument u obliku priručnika koji identificira pravila mjerodavna za kibernetičko ratovanje.[8] Svrha je ovoga članka iznijeti osvrt na osnovne postavke tog rada.[9] U prvom dijelu upoznajemo čitatelje s donošenjem i s osnovnom strukturom navedenog priručnika. Zatim se bavimo njegovim pravnim obuhvatom, što ilustriramo iznošenjem ključnih pravila o zabrani uporabe sile. Nadalje, prikazujemo temeljne odlike usvojenih pravila i njihovih komentara. Rad nastavljamo govoreći o autoritetu i općem značaju priručnika kao sredstva za bolje razumijevanje primjene međunarodnog prava oružanih sukoba u kibernetičkom prostoru. U završnom dijelu iznosimo ocjenu njegove trenutačne uspješnosti te ukratko sažimamo najvažnije spoznaje do kojih smo došli istraživanjem provedenim u svrhu izrade ovoga članka. Napominjemo da materiji kibernetičkog ratovanja pristupamo veoma konzervativno. Naime, s obzirom na to da bi analiza svih postavaka priručnika uvelike premašila svrhu i cilj ovog rada, svoje izučavanje ograničavamo na opću razinu njihove kvalitativne komponente, no uz istodobni komentar i analizu pojedinih ključnih dijelova/pravila priručnika kako bismo ga oživotvorili i približili čitateljima te im omogućili lakše praćenje ovog članka.

[5] Prema dostupnim podacima 33 države uključile su kibernetičko ratovanje u svoje vojno planiranje i organizaciju. Ono što je zajedničko tim vojnim doktrinama jest da uključuju raspoložive kibernetičke kapacitete za potrebe operativnog izviđanja, dobivanja informacija i ometanja ključne mrežne infrastrukture. V. Lewis, Timlin, *op. cit.* (bilj. 3), str. 3.

[6] *Ibid*, str. 4.

[7] Vuković, *op. cit.* (bilj. 2), str. str. 17.

[8] Glede prijevoda pojma *cyber* kao *kibernetika* dajemo nekoliko napomena. Pojam *kibernetika* uveden je u pravni poredak Republike Hrvatske ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu (engl. *Budapest Convention on Cybercrime*), slijedom čega se uvriježilo koristiti pojam *kibernetički* u obliku pridjeva za nešto što uključuje računala, a osobito internet, koristi ih ili je povezano s njima. To je službeno obrazloženje tog pojma sadržano u uvodnom dijelu Odluke Vlade Republike Hrvatske o donošenju nacionalne strategije kibernetičke sigurnosti (v. *supra*, bilj. 1). S obzirom na takvu normativnu podlogu u hrvatskom zakonodavstvu u ovome radu pojam *kibernetičko ratovanje* koristimo u prijevodu izraza na engleskom jeziku *cyber warfare*. Postoje i drugačija mišljenja. Neki autori smatraju da za pojam *cyber* trenutačno ne postoji odgovarajući prijevod na hrvatski jezik i ističu da je prilikom prijevoda Budimpeštanske konvencije o kibernetičkom kriminalu učinjena terminološka zbrka jer riječ *kibernetika* nije istoznačnica riječi *cyber* (opširnije v. Vuković, *op. cit.* (bilj. 2), str. 15-16).

[9] Uvodni dio Tallinnskog priručnika sadrži naznaku da se pojam „kibernetičko ratovanje“ koristi u opisnom smislu, stoga ćemo ga tako koristiti i u ovome radu.

2. POČETNE POSTAVKE O DONOŠENJU TALLINNSKOG PRIRUČNIKA I NJEGOVOJ OSNOVNOJ STRUKTURI

Svjedoci smo sve intenzivnije militarizacije virtualnog prostora, kako je to ukratko objašnjeno u uvodnom dijelu.[10] Toga je svjestan i NATO-ov Centar izvrsnosti za suradnju u obrani od kibernetičkih napada (u daljnjem tekstu: NATO-ov Centar izvrsnosti) iz Tallinna i stoga je okupio niz pravnih praktičara, znanstvenika i tehničkih stručnjaka u radno tijelo pod nazivom Međunarodna skupina stručnjaka (u daljnjem tekstu: Međunarodna skupina) radi izrade priručnika o međunarodnom pravu primjenjivom na kibernetičko ratovanje.[11] Njihov je zadatak bio ispitivanje načina na koji se postojeće norme međunarodnog prava primjenjuju na kibernetičko ratovanje kao novu formu ratovanja i istodobno razjašnjavanje nekih od složenih pravnih pitanja koja se odnose na kibernetičke operacije.[12] Nije sporno da je glavna svrha pravila međunarodnog prava kojima se reguliraju klasični oružani sukobi humanizacija rata i drugih oblika oružanih sukoba.[13] Tallinnska razmatranja imaju isti cilj, s time da su ti napori usmjereni na polje oružanih sukoba s kibernetičkim obilježjem.[14] Rezultat takva zajedničkog trogodišnjeg rada članova Međunarodne skupine, u suradnji s ostalim sudionicima, jest donošenje opsežnog međunarodnopravnog priručnika potpunog naziva *Tallinnski priručnik o međunarodnom pravu primjenjivom na kibernetičko ratovanje* (u daljnjem tekstu: Priručnik), izdanog u travnju 2013.[15] Smatramo prikladnim da u početnom dijelu ovoga članka ponešto kažemo o sastavu Međunarodne skupine i upozorimo na neke njezine probleme.

Sudjelovanje u Međunarodnoj skupini imalo je isključivo osobno svojstvo. To znači da pojedini stavovi članova ni na koji način ne odražavaju službene politike institucija iz kojih dolaze. Kriteriji za njihovo sudjelovanje temeljili su se na njihovim vještinama na području relevantnog prava te na njihovim sposobnostima za analizu osjetljivosti kibernetičkog

[10] Ova je tvrdnja posebno vidljiva na primjeru kibernetičkih operacija usmjerenih na Estoniju 2007. i Gruziju 2008. te prilikom napada računalnim virusom na iranska nuklearna postrojenja 2010. V. npr. Lawor, Russell, A., *Cyber Blockades*, Washington, 2014, str. 131 i *SIPRI Yearbook 2011: Armaments, Disarmament and International Security*, Oxford, 2011, str. 384.

[11] NATO-ov Centar izvrsnosti (engl. *NATO Cooperative Cyber Defence Centre of Excellence*) nije dio zapovjedne strukture NATO-a niti je od njega financiran. Dio je šireg okvira koji podupire NATO-ove dogovore i ciljeve. Države koje ga (materijalno) podupiru jesu: Estonija, Njemačka, Mađarska, Italija, Latvija, Litva, Nizozemska, Poljska, Slovačka, Španjolska i Sjedinjene Američke Države; službene stranice: https://ccdcoe.org/research.html (pristup: 26. siječnja 2016.).

[12] Postoje i druge organizacije koje se bave kibernetičkim prijetnjama, primjerice *International Multilateral Partnership Against Cyber Threats* (IMPACT).

[13] Andrassy, J., Bakotić, B., Seršić, M., Vukas, B., *Međunarodno pravo 3*, Zagreb, 2006, str. 125.

[14] Doprinos tim djelatnostima dali su i promatrači iz ukupno tri organizacije, i to: NATO-ovo Savezničko zapovjedništvo za transformaciju, Kibernetičko zapovjedništvo SAD-a i Međunarodni odbor Crvenog križa. Njihov je rad bio ograničen isključivo na sudjelovanje u raspravama i izradi nacrta pravila, jer predstavnici tih organizacija nisu imali pravo glasa pri odlučivanju o (ne)usvajanju predloženih (konačnih) pravila. U procesu izrade nacrta mnoge su države iskoristile priliku da na neformalan, neslužbeni način daju svoje mišljenje o predloženom tekstu pravila (v. Gill, T., D., Greib, R., Heinsch, R., McCormack, T., Paulussen, C., Dorsey, J., *Yearbook of International Humanitarian Law 2012*, vol. 15, 2013, str. 4.).

[15] engl. *Tallinn Manual on the International Law Apalicable to Cyber Warfare*. Tekst Priručnika dostupan je na: http://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (pristup: 25. veljače 2016.).

konteksta u kojem bi takvo pravo bilo primijenjeno.[16] Takav odabir rezultirao je nastankom višenacionalne skupine stručnjaka, od kojih je većina imala iskustvo na području međunarodnog prava (kibernetičke) sigurnosti.[17] Nasuprot navedenom upozoravamo da učenjaci s područja filozofije nisu bili uključeni u taj projekt.[18] Autor tu činjenicu negativno cijeni i smatra da je time propuštena prilika za jačanje moralne komponente usvojenih pravila. Smatramo da su dodatne rasprave o predloženim tekstovima pravila, i to s gledišta (i u kontekstu) vojne etike, mogle sadržajno obogatiti i poboljšati njihovu kvalitetu. Već je na prvi pogled uočljivo da je sastav Međunarodne skupine bio (pretežito) ograničen na predstavnike zemalja članica NATO-a zainteresiranih za tu materiju. To znači da, iako su sudionici bili pripadnici različitih nacija, nije bilo pokušaja da se osigura ujednačena geografska raspodjela.[19] Dakle stvaraoci toga međunarodnog dokumenta nisu predstavljali odraz svih svjetskih pravnih kultura, nego su dolazili iz (pretežito) zapadnih zemalja.[20] Mišljenja smo da to donekle utječe na autoritet Priručnika, o čemu govorimo u zasebnom poglavlju ovoga rada (v. *infra,* poglavlje 6, odjeljak 1).

Prije nego što se upustimo u analizu osnovnih postavaka Priručnika, reći ćemo ponešto o njegovoj strukturi. Glavnom sadržaju Priručnika prethodi popis svih članova Međunarodne skupine i ostalih sudionika, zatim detaljan popis korištenih pravnih izvora te uvodni dio koji se sastoji od nekoliko kratkih poglavlja i sadrži napomene koje su autoru ovoga članka bile osobito korisne. Uvodni dio smatramo nezaobilaznim štivom i preporučujemo ga svakome tko planira proučavati Tallinnski priručnik. Uvod opisuje i predstavlja Priručnik te naglašava područje njegove primjene.[21] Naime kako je Međunarodna skupina ograničila svoju raspravu na uporabu sile i oružani sukob, kibernetičke aktivnosti koje ne dosežu taj stupanj nisu predmet razmatranja, jer se skupina fokusirala na kibernetičke operacije *stricto sensu*.[22] Uvod ističe da pravila mjerodavna za kinetičke operacije (uključivši i tradicionalne operacije elektroničkog ratovanja, poput elektroničkog ometanja) nisu obuhvaćena i objašnjava da je *ratio* takva isključenja u tome što su te teme već dobro proučene i shvaćene u tradicionalnim pravilima prava oružanog sukoba.[23] Smatramo da se tim pristupom ignorira međusobno preklapanje dvije teme od velikog značaja za vojne službe, i to elektroničko ratovanje s jedne strane te kapaciteti kibernetičkog ratovanja s druge. S tim se mišljenjem slažu i drugi autori.[24] Nakon uvoda slijedi glavni sadržaj Priručnika, koji se dijeli na dva dijela, i to dio I., koji razmatra pitanja međunarodnog prava kibernetičke sigurnosti, i dio II., koji razmatra pitanja prava kibernetičkog oružanog sukoba. Ti su dijelovi podijeljeni na

[16] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 4.
[17] *Ibid*, str. 11.
[18] Henschke, A., Strawser, B., J., *Binary Bullets: The Ethics of Cyberwarfare*, Oxford, 2016, str. 17-18.
[19] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 4.
[20] *Ibid*, str. 11.
[21] engl. cyber to cyber operations.
[22] McGhee, E., J., *The Schmitt Analaysis, Tallinn Manual and US Cyber Policy*, u: Journal of Law & Cyber Warfare, vol. 2, izd. 1, 2013, str. 84.
[23] *Ibid*.
[24] V. npr. *ibid*.

poglavlja i odjeljke, svaki odjeljak sadrži pravila, čiji ukupan broj iznosi 95. Najveći broj pravila (njih 45) nalazimo u četvrtom poglavlju, koje se bavi pitanjima postupanja u neprijateljstvima.[25]

Početno pravilo odnosi se na suverenost u kibernetičkom prostoru i prema njemu je država ovlaštena izvršavati kontrolu nad kibernetičkom infrastrukturom i aktivnostima unutar svojeg suverenog teritorija (pravilo 1). U komentarima koji obrazlažu to pravilo objašnjava se da nijedna država ne može tvrditi da ima suverenost nad kibernetičkim prostorom *per se*, no da države mogu izvršavati suverene ovlasti nad kibernetičkom infrastrukturom koja se nalazi na njihovu području, uključujući djelatnosti povezane s tom infrastrukturom.[26] Pozitivno cijenimo smještaj te teme u početni dio Priručnika jer je smatramo bitnom za primjenu ostalih pozitivnih međunarodnopravnih instituta mjerodavnih za kibernetičko ratovanje. U pojašnjenju te tvrdnje upućujemo na stavove autora, prema kojima je u ratovanju jedno od prvih pitanja koja moraju biti riješena pitanje gdje nacije imaju svoju nadležnost, gdje je mogu izvršavati te kada se očekuje da imaju kontrolu nad djelatnostima koje poduzimaju bilo same bilo posredovanjem svojih agenata.[27] Smatramo da su odgovori na ta pitanja određeni suvremenim shvaćanjima koncepata nacionalne suverenosti, pravne nadležnosti i državne kontrole.[28] S tim se mišljenjem slažu i drugi autori.[29] Priručnik ispituje te koncepte u kontekstu kibernetičkog ratovanja, no međunarodni karakter i obuhvat kibernetičkog prostora dodatno komplicira svako od njih, na što prateći komentari prvog pravila jasno upućuju i time postupno uvode čitatelje u glavne teme tog rada. Suverenost je ključni pojam ne samo u kontekstu razmatranja kibernetičkih operacija nego i kibernetičke infrastrukture. Razlog tome leži u činjenici da je takva infrastruktura podložna kontroli države na čijem se području nalazi i istodobno obuhvaćena zaštitom u okrilju njezine suverenosti (neovisno o tom nalazi li se u vlasništvu države ili privatnom vlasništvu).[30] Zato nesigurnost u pogledu shvaćanja što predstavlja povredu suvereniteta u kibernetičkom prostoru dolazi do izražaja u cijelom nizu životnih situacija, poput kibernetičke špijunaže, okolnosti kada

[25] U dijelu I. poglavlje prvo razmatra pitanje država i kibernetičkog prostora, uključujući suverenost, sudsku nadležnost i kontrolu te državnu odgovornost; poglavlje drugo razmatra uporabu sile (uključujući njezinu zabranu) i pravo samoobrane. U dijelu II. poglavlje treće razmatra općenita pitanja prava oružanog sukoba; poglavlje četvrto razmatra pitanja postupanja u neprijateljstvima; poglavlje peto razmatra pitanja stanovitih osoba, objekata i aktivnosti; poglavlje šesto bavi se okupacijom; poglavlje sedmo bavi se neutralnošću.

[26] Štoviše, pojedini autori upozoravaju da iz suvereniteta države proizlazi i njezina ovlast da u cijelosti ili djelomično ograniči pristup internetu istodobno ne dovodeći u pitanje mjerodavno međunarodno pravo (poput humanitarnog prava ili međunarodnog telekomunikacijskog prava). V. Jones, A., Kovacich, G., L., *Global Information Warfare: The New Digital Battlefield*, izd. 2, New York, 2015, str. 303.

[27] Chapple, M., Seidl, D., Cyberwarfare: Information Operations in a Connected World, Burlington, 2014, str. 62.

[28] Priručnik priznaje postojanje svojevrsne „izvanteritorijalne" strane kibernetičke tehnologije te (u smislu suverenih prava država) u pratećem komentaru pravila 1 navodi: „*Sama činjenica da je kibernetička infrastruktura smještena u danoj državi povezana s globalnim telekomunikacijskim mrežama ne može biti tumačena kao odricanje od suverenih prava nad tom infrastrukturom.*" V. Gehmann, U., Reiche, M., *Real Virtuality: About the Destruction and Multiplication of World*, Bielefeld, 2014, str. 389.

[29] Chapple, Seidl, *op. cit.* (bilj. 27), str. 62.

[30] *Ibid*.

mrežna računalna operacija predstavlja povredu suvereniteta druge države itd.[31] Detaljnije upuštanje u razmatranje navedene problematike uvelike bi premašilo opseg ovoga rada, stoga tek završno navodimo da se radi o otvorenim, složenim i sve važnijim pitanjima, koja zaslužuju daljnju pozornost i rasprave, to više što su nacionalne granice znatno manje vidljive kada se radi o uporabi i djelovanju međunarodnih računalnih mreža i sustava elektroničkih komunikacija.[32]

3. OBUHVAT PRIRUČNIKA

Ovo poglavlje otvaramo riječima glavnog urednika Priručnika Michaela Schmitta, prema kojem je njegova svrha da (poput udžbenika) pruži pravnu pomoć raznim (pravnim) savjetnicima, vladama i vojskama. Htjelo se stvoriti doktrinarni rad koji bi bio od koristi državama u formiranju vlastitih stajališta i njihovu djelovanju u kibernetičkom prostoru. Nisu se davale preporuke niti definirala najbolja praksa, nije se ulazilo u političke sfere.[33] Slijedom tih riječi zaključujemo da Priručnik želi pružiti analizu pozitivnog međunarodnog prava radi pružanja smjernica državama u provođenju njihovih tuzemnih i međunarodnih politika u kibernetičkom prostoru u kontekstu *jus ad bellum* i *jus in bello*.[34] Naime smatralo se da će njegovi korisnici morati uvažiti oboje radi odgovarajuće procjene kibernetičkih situacija.[35] Aktivnosti ispod te razine (poput kibernetičkog kriminala) nisu predmet interesa, kao ni teme iz područja međunarodnog telekomunikacijskog prava, pitanja kaznene odgovornosti pojedinca i sl. Priručnik objašnjava obuhvat primjenjivosti postojećih norma međunarodnog prava mjerodavnih za pitanja uporabe sile prije i tijekom oružanog sukoba, pri čemu se na više mjesta navodi da se on ne smatra potvrdom mjerodavnog međunarodnog prava.[36] Prije nego što se pristupilo tim zadacima, bilo je potrebno razriješiti dvojbu je li za potrebe normiranja kibernetičkog ratovanja potrebno stvoriti posve novo (ugovorno) pravo ili se ista svrha mogla ostvariti proširenjem postojećih pravila i principa međunarodnog prava.[37] Međunarodna skupina jednoglasno se složila s drugim stajalištem, prema kojem se postojeća pravila i principi nedvojbeno primjenjuju i na kibernetičko ratovanje.[38] Stoga pravila sadržana u Priručniku odražavaju gledište o primjenjivosti *lex lata* (odnosno prava koje je trenutačno mjerodavno za kibernetički sukob). Dobar je primjer navedenoga

[31] Friis, K., Ringsmose, J., *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*, Routledge, 2016, str. 155.
[32] Chapple, Seidl, *op. cit.* (bilj. 27), str. 62.
[33] Gladyshev, P., Marrington, A., Baggili, I., *Digital Forensics and Cyber Crime: Fifth International Conference, Revised Selected Papers*, Moskva, 2014, str. 131.
[34] Opširnije o pravilima Priručnika u kontekstu *jus ad bellum* i *jus in bello* v. npr. *ibid*, str. 137-139.
[35] Veliki problem u operacijama s kibernetičkim obilježjem jest učinkovito utvrđivanje izvora podrijetla napada. Takva neizvjesnost može dovesti do međusobnih optužaba i napetosti između država te ugroziti međunarodni mir i sigurnost, čije je očuvanje jedan od glavnih ciljeva organizacije Ujedinjenih naroda. V. Andrassy, J., Bakotić, B., Lapaš, D., Seršić, M., Vukas, B., *Međunarodno pravo 2*, Zagreb, 2012, str. 125.
[36] Te norme proizlaze iz međunarodnog prava oružanih sukoba kao skupa pravila koja uređuju odnose među subjektima međunarodnog prava za vrijeme oružanog sukoba i u vezi s njim. V. Andrassy, Bakotić, Seršić, Vukas, *op. cit.* (bilj. 13), str. 124.
[37] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 130.
[38] *Ibid*, str. 134-135.

pravilo prema kojemu su kibernetičke operacije koje su izvršene u sklopu oružanog sukoba podložne pravu oružanih sukoba (pravilo 20), kao i u danoj definiciji kibernetičkog napada/agresije, koju poslije opširnije razmatramo (v. *infra,* poglavlje 5, odjeljak 3), a čiji temelji leže u definiciji pojma napad sadržanoj u Dopunskom protokolu Ženevskim konvencijama od 12. kolovoza 1949. o zaštiti žrtava međunarodnih oružanih sukoba iz 1977. (u daljnjem tekstu: Protokol I.).[39]

Priručnik ne odražava sveobuhvatne odnose u kibernetičkom prostoru, jer je njegovo težište na primjeni međunarodnog prava u kontekstu kibernetičkog ratovanja, odnosno kibernetičkih operacija koje se smatraju najozbiljnijima. To znači da predmet pravnog normiranja nije usmjeren na cjelokupnu materiju međunarodnog prava kibernetičke sigurnosti, nego na (značajan) segment iste. Spomenuli smo važnost digitalnog prostora kao jednog od određujućih obilježja suvremenog života i ključnog područja djelovanja svjetskog gospodarstva. Stoga nam se na prvi pogled čini održivom teza da ispitivanje promjena u kibernetičkoj sigurnosti (koje utječu na privatnu sferu, poslovnu ekonomiju i građansko društvo) ima primat u odnosu na izučavanje pravila i principa međunarodnog prava koji se odnose na uporabu sile ili oružani sukob, drugim riječima, da za prosječnu osobu kibernetički kriminal ima veću životnu važnost nego „visoka politika" međunarodnih odnosa.[40] Stvarnost međutim demantira te tvrdnje i pokazuje da su vlade zemalja spremne iskoristiti prednost prilika koje im pruža kibernetička tehnologija čak i kada bi takve operacije mogle predstavljati zabranjenu upotrebu sile u međunarodnom pravu.[41] Pojedini autori smatraju da, iako je kibernetičko ratovanje podložno ustanovljenim pravilima i principima unutar ambicija međunarodnog prava, prijenos tih pravila i principa (stvorenih i naknadno dograđivanih za fizički svijet) u kibernetički svijet predstavlja stanovite teškoće te da se neka od tih pitanja mogu riješiti samo jednoglasjem međunarodne zajednice i donosioca međunarodnih norma.[42] Istodobno moramo uvažiti činjenicu da najveći broj kibernetičkih operacija usmjerenih prema državama (ili subjektima na njezinu području) neće dosegnuti nivo uporabe sile prema *jus ad bellum* ili oružani sukob prema *jus in bello*.[43] Stoga je na inicijativu NATO-ova Centra izvrsnosti pokrenut projekt koji je rezultirao donošenjem novog priručnika, u kojem se razmatraju mogućnosti odgovora država na kibernetičke operacije ispod praga oružanog napada i uporabe sile.[44] I prije dovršetka tog projekta neki su autori iznosili stav da će ta dva

[39] Podredno spomenimo da ovo nije prvi međunarodni dokument koji se bavi kodifikacijom i pitanjima primjene međunarodnog prava na kibernetički prostor. Tako je u veljači 2011. objavljeno prvo zajedničko rusko-američko izvješće koje se usredotočuje na zaštitu kritične infrastrukture u kibernetičkom prostoru pomoću sredstava međunarodnog humanitarnog prava (engl. *Working towards Rules Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*). Cilj te rusko-američke bilaterale bilo je istražiti kako se humanitarni principi, sadržani u ženevskim i haškim konvencijama o ratu, mogu proširiti na način da reguliraju rat u kibernetičkom prostoru. Opširnije o dosadašnjim kodifikacijama međunarodnog prava u kibernetičkom prostoru v. npr. *ibid*, str. 141.

[40] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 5.

[41] V. Lawor, *op. cit.* (bilj. 10), str. 131.

[42] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 141.

[43] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 4.

[44] Tzv. Talinnski priručnik 2.0. Opširnije v. npr. na: http://securityaffairs.co/wordpress/56004/cyber-warfare-2/nato-tallinn-manual-2-0.html (pristup: 29. ožujka 2017.).

priručnika na koherentan način obuhvatiti potpuni raspon međunarodnog prava kibernetičke sigurnosti.[45] S tim se mišljenjem slažemo te, poput tih autora, upozoravamo da je sve do donošenja takva novog dokumenta postojala stvarna opasnost promatranja svih kibernetičkih operacija (uključujući i one koje su ispod spomenutog praga oružanog napada i uporabe sile) isključivo kroz sferu Tallinnskog priručnika iz 2013., a to je iz navedenih razloga u cijelosti neprikladno.[46]

Neki autori postavljaju pitanje o mogućoj kvalifikaciji Priručnika kao „pomoćnog sredstva utvrđivanja pravila" u smislu članka 38. stavak 1.d Statuta Međunarodnog suda.[47] Pritom se polazi od stajališta da on predstavlja objavu onoga o čemu su se donosioci usuglasili u smislu pravila i principa međunarodnog prava primjenjivih na kibernetičko ratovanje.[48] Nadalje, upozoravamo da većina pravila Priručnika proizlazi iz običajnog međunarodnog prava, koje se danas smatra važnim izvorom prava oružanih sukoba.[49] Pri tome se polazilo od savjetodavnog mišljenja Međunarodnog suda o legalnosti nuklearnog oružja da haška pravila (1907.) odražavaju međunarodno običajno pravo te da većina odredaba ženevskih normiranja (1949.) ima isti status.[50] Donosioci Priručnika nastojali su demonstrirati kako postojeća međunarodna legislacija, koja se odnosi na domene zraka, mora, kopna i svemira, može biti vodič u tzv. „petoj domeni" kibernetičkih aktivnosti.[51] Primjer je navedenoga pravilo prema kojemu je zabranjeno upotrijebiti mine iznenađenja povezane sa stanovitim objektima naznačenima u pravu oružanih sukoba (pravilo 44). Naime u komentaru toga pravila naznačeno je da ono potječe iz Protokola o zabrani ili ograničenju uporabe mina, mina iznenađenja ili drugih naprava (1980.) te da odražava običajno međunarodno pravo. S druge strane Priručnik upozorava na ona međunarodna pravila koja nisu utemeljena na običaju i koja su u svojoj primjeni ograničena na stranke međunarodnih ugovora iz kojih potječu. Primjer nalazimo u pravilu prema kojemu je državama strankama Protokola I. zabranjena uporaba kibernetičkih metoda ili sredstava ratovanja koja su namijenjena ili za koje se očekuje da prouzrokuju široko rasprostranjene, dugoročne i ozbiljne štete prirodnom okolišu (pravilo 83b). Nisu svi suglasni s takvim metodološkim principom. Neki autori uspoređuju taj proces s pristupom brutalne sile i ističu da su se članovi Međunarodne skupine poslužili pravilima postojećeg prava kinetičkog ratovanja i jedno po jedno od tih pravila pokušali prisiliti na primjenu u kibernetičkoj domeni, čak i u slučajevima kada se to pokazalo problematičnim.[52] Ti autori istodobno smatraju da je kibernetičko ratovanje drugačije od

[45] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 4.
[46] V. npr. *ibid*, str. 1.
[47] *Ibid*, str. 11.
[48] *Ibid*.
[49] Opširnije o izvorima prava oružanih sukoba vidi npr. Andrassy, Bakotić, Seršić, Vukas, *op. cit.* (bilj. 13), str. 125-132.
[50] Legality of the Use by a State of Nuclear Weapons in Armed Conflict (*Advisory Opinion*), *International Court of Justice, Reports of Judgements, Advisory Opinions and Orders* (dalje: ICJ Reports), 1996.
[51] Henschke, Strawser, *op. cit.* (bilj. 18), str. 17.
[52] Richet, J., L., Cybersecurity Policies and Strategies for Cyberwarfare Prevention, 2015, str. 19.

kinetičkog ratovanja, zbog čega je potreban drugačiji način pristupa, i zauzimaju se za tzv. stupnjevit pristup.[53]

Navedene tvrdnje iz ovoga poglavlja ilustrirat ćemo čitateljima u nastavku ovoga članka kratkim prikazom i analizom ključnih pravila o zabrani uporabe sile i pravila o samoobrani, sadržanih u poglavlju II. Priručnika. Istodobno završno zaključujemo da je Međunarodna skupina samo identificirala moguće ponašanje država u kibernetičkom području, interpretirala primjenjiva pravila međunarodnog prava i pružila rješenja utemeljena na metodološkim procedurama.[54] Autor takva ograničenja u obuhvatu Priručnika negativno cijeni. Naime postoji stalna potreba razvoja međunarodnog prava radi davanja odgovarajućeg odgovora na izmijenjene prilike međunarodnog života.[55] Donosioci Priručnika takvoj potrebi nisu udovoljili i smatramo da su time propustili priliku davanja vlastitog doprinosa progresivnom razvoju i kvalitativnom obogaćenju te grane prava. Pojedini autori upozoravaju da to što je u procesu izrade korištena metoda interpretacije znači da dobiveni rezultati rada mogu biti predmet raznih osporavanja, kao i da države te rezultate mogu odbiti pozivajući se na svoje koncepcije razumijevanja prava, odnosno koristeći se argumentom da su postignuti rezultati suprotni njihovim tuzemnim ili međunarodnim interesima.[56]

4. UPORABA SILE I SAMOOBRANA

Poglavlje II. Priručnika bavi se uporabom sile. Već je na prvi pogled uočljivo da su mnoga pravila iz tog poglavlja *mutatis mutandis* preslika odredaba koje nalazimo u međunarodnim konvencijama. Tako pravilo 13 (Samoobrana protiv oružanog napada), pravilo 16 (Kolektivna samoobrana) i pravilo 17 (Obavještavanje o poduzetim mjerama samoobrane) uključuju pozivanje na članak 51. Povelje UN-a, dok se pravilo 18 (Vijeće sigurnosti Ujedinjenih naroda) i pravilo 19 (Regionalne organizacije) odnosi na članke 39, 41, 42 i 52 Povelje UN-a.[57] U raspravama o poglavlju II. članovi Međunarodne skupine polazili su od spomenutog savjetodavnog mišljenja Međunarodnog suda o legalnosti nuklearnog oružja, prema kojem se članak 2. stavak 4. Povelje UN-a (koji se odnosi na uporabu sile) i čl. 51. Povelje UN-a (koji se odnosi na uporabu samoobrane) primjenjuju na bilo koju uporabu sile, bez obzira na to koje je oružje upotrijebljeno.[58] U skladu s ranijim razmatranjima u prethodnom poglavlju ovoga rada, primjenom teleološke metode tumačenja, a istodobno vodeći se kriterijem logike i razuma, zaključujemo da se postojeća pravila i standardi međunarodnog prava primjenjuju u pitanjima uporabe sile u kibernetičkom ratovanju. Stoga se slažemo s autorima koji smatraju da kibernetičke operacije potpadaju pod naum i svrhu težnja sadržanih u spomenutom stajalištu

[53] *Ibid*.
[54] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 12.
[55] Andrassy, J., Bakotić, B., Seršić, M., Vukas, B., Međunarodno *pravo 1,* 2. izd., Zagreb, 2010, str. 39-41.
[56] V. npr. Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 12.
[57] Lovelace, D., C., *Terrorism: Commentary on Security Documents*, vol. 140, Oxford, str. 131.
[58] ICJ Reports 1996, *op. cit.* (bilj. 50), st. 39.

Međunarodnog suda.[59] Nadalje, s obzirom na to da Povelja UN-a daje opće standarde za uporabu sile, ona se time ustanovljuje kao važan instrument u analizi materije kibernetičkog ratovanja. U pogledu suvremenih trendova smatramo prikladnim ovom prilikom uputiti na mišljenja uglednih autora koji upozoravaju da, iako smo daleko od remilitarizacije sustava vrijednosti, moramo pažljivo pratiti pokušaje momentalnih „moćnika" da se na razne načine dovede do pravnog proširenja mogućnosti uporabe sile.[60]

U međunarodnoj zajednici postoji suglasje da kibernetička operacija može doseći status oružanog napada.[61] Prema Priručniku nezakonita je ona kibernetička operacija koja predstavlja prijetnju ili uporabu sile usmjerene protiv teritorijalne cjelovitosti ili političke nezavisnosti bilo koje zemlje, ili koja je na bilo koji drugi način nespojiva s ciljevima Ujedinjenih naroda (pravilo 10). U tom kontekstu definiranje sile pokazuje se ključnim. Naime prema stajalištu članova Međunarodne skupine kibernetički napadi koji imaju isti učinak kao i oružani napad trebaju biti kvalificirani kao uporaba sile, uz upozorenje da procjena kibernetičkih operacija nije lak zadatak, odnosno da je potrebno iznaći odgovarajuće sredstvo procjene kibernetičkih operacija u kontekstu uporabe sile.[62] Kako bi se utvrdilo predstavlja li kibernetička operacija uporabu sile i oružani napad, Priručnik se poziva na različita pravila i kriterije.[63] Tako kibernetička operacija predstavlja uporabu sile kada je njezin opseg i učinak usporediv s nekibernetičkim operacijama koje dosežu nivo uporabe sile (pravilo 11). Komentar tog pravila sadrži (neobvezujuću) listu od osam faktora za procjenu sile, i to: njezina ozbiljnost, neposrednost, izravnost, intenzitet napada, mjerljivost učinaka, vojni karakter, uključenost države i pravna utemeljenost.[64] Smatra se da je zabranjena svaka sila koja uzrokuje štetne učinke u obliku smrti ili ozljede i/ili fizičku štetu i koja je jednaka onoj koja nastaje kao posljedica uporabe vojne sile.[65] Polazeći od shvaćanja Međunarodnog suda iznesenih u predmetu *Nicaragua*, Priručnik uvodi svojevsrni *de minimis* prag za procjenu opsega i učinka kibernetičke operacije i navodi da bi ozbiljna uporaba sile predstavljala oružani napad (koji ima za posljedicu aktiviranje prava na samoobranu), dok s druge strane svaka manje ozbiljna uporaba sile ne bi imala karakter oružanog napada, ali bi predstavljala povredu članka 2. stavka 4. Povelje UN-a.[66] Autor takvo općenito određenje praga procjene negativno cijeni. Smatramo da bez taksativno navedenih i detaljno objašnjenih (obvezujućih) kriterija za mjerenje stupnja ozbiljnosti pojedine uporabe sile granice procjene ostaju prilično široke

[59] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 137.
[60] Seršić, M., *Agresija, samoobrana i anticipatorna samoobrana*, Zbornik Pravnog fakulteta u Zagrebu, *vol.* 57, br. 2, 2007, str. 287.
[61] Lehto, M., Neittaanmäki, P., *Cyber Security: Analytics, Technology and Automation*, Springer, 2015, str. 92.
[62] Chapple, Seidl, *op. cit.* (bilj. 27), str. 67.
[63] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 137.
[64] Priručnik raspravlja i o drugim faktorima koji mogu biti uzeti u obzir prilikom razmatranja kibernetičkih operacija kao nezakonite uporabe sile. Tako se u odnosu na kriterij ozbiljnosti navodi da, što je posljedica ozbiljnija (po ključne nacionalne interese), to će više pridonijeti kvalifikaciji kibernetičke operacije kao uporabe sile. Ujedno, u tom će slučaju obuhvat, trajanje i intenzitet posljedice biti od ključne važnosti. V. Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 22.
[65] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 22.
[66] *Ibid*, str. 23. Pojam oružanog napada (agresije) bio je u središtu razmatranja Međunarodnog suda u presudi u slučaju *Nicaragua* 1986. V. ICJ Reports 1986 i Seršić, *op. cit.* (bilj. 60), str. 274-282.

i nejasne. S tim se mišljenjem slažu i drugi autori.[67] Nadalje, prema Priručniku kibernetička operacija ili prijetnja kibernetičkom operacijom predstavlja nezakonitu prijetnju silom kada bi aktivnost kojom se prijeti, pod pretpostavkom njezina izvršenja, bila nezakonita uporaba sile (pravilo 12). Srž je prijetnje u prisili. Prijetnja može biti izražena na različite načine (riječima, konkludentnim radnjama i dr.), stoga autor smatra da procjena stupnja njezine ozbiljnosti ovisi o konkretnim i specifičnim okolnostima slučaja.[68] Dakle kao i kod procjene ozbiljnosti uporabe sile i u ovom slučaju granica za procjenu ostaje široka i nejasna uslijed nedostataka kriterija za mjerenje stupnja ozbiljnosti prijetnje.

Ukoliko dođe do uporabe sile, Priručnik se poziva na pravilo prema kojem država koja je meta kibernetičke operacije (koja doseže nivo oružanog napada) može iskoristiti svoje prirodno pravo na samoobranu, a predstavlja li kibernetička operacija oružani napad, ovisi o njezinu opsegu i učincima (pravilo 13). Prema citiranom pravilu to znači da država ima pravo obraniti se u slučaju da je objekt kibernetičke operacije koja po svojem opsegu i učinku predstavlja oružani napad.[69] Samoobrana je dopuštena samo kao odgovor na kibernetičku operaciju koja se izjednačava s oružanim napadom. No kako ni Sud ni Priručnik precizno ne navode kriterije za mjerenje stupnja ozbiljnosti takva napada, ostaje otvorenim pitanje kada je samoobrana dopuštena.[70] To više što i prema samom tekstu Priručnika država ne može uporabiti silu u odgovoru na silu koja je ispod praga oružanog napada.[71] Upravo se stoga od slučaja do slučaja procjenjuje radi li se oružanoj operaciji dovoljne ozbiljnosti da se može smatrati oružanim napadom od kojega je dopuštena samoobrana, uslijed čega jedan te isti incident može, ali i ne mora, biti kvalificiran oružanim napadom.[72] Daljnja analiza spomenutih pitanja premašila bi svrhu ovoga članka, stoga završno upozoravamo na postojanje cijelog niza nejasnoća o uporabi sile kao oružanom napadu u kontekstu kibernetičkih operacija, koje ostaju otvorene za daljnju raspravu, poput kibernetičkih operacija poduzetih izvan krugova vladinih vojnih organizacija (npr. od civilnih ugovaratelja, plaćenika, pojedinaca, organiziranih grupa), kvalifikacije kibernetičkog napada koji ne uzrokuje izravnu fizičku štetu (npr. napad na državne financijske institucije) itd.[73]

---

[67] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 23.

[68] Priručnik u svrhu ilustracije daje primjer države koja (u ozračju napetosti s drugom državom) agresivno razvija kibernetičke kapacitete i nadalje objašnjava da takva situacija sama po sebi neće predstavljati nezakonitu prijetnju silom. O nezakonitoj uporabi bit će riječ tek u slučaju objave da će takve novostečene kibernetičke sposobnosti biti uporabljene upravo u tu svrhu.

[69] Opširnije o konceptu samoobrane u međunarodnom pravu v. Seršić, *op. cit.* (bilj. 60), str. 271-290.

[70] Ako dođe do uporabe sile, Priručnik navodi pojedine situacije i objašnjava hoće li se one smatrati uporabom sile. Npr. nerazornu kibernetičku psihološku operaciju, koja se poduzima isključivo radi potkopavanja povjerenja u vladu ili ekonomiju, ne smatra uporabom sile. S druge strane niz kibernetičkih incidenata koji su pojedinačno ispod praga oružanog napada, ali su počinjeni od strane istog subjekta i pokazuju stanoviti obrazac, može kumulirano biti kvalificiran kao oružani napad kojim se aktivira pravo na samoobranu. V. Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 30.

[71] *Ibid*.

[72] Seršić, *op. cit.* (bilj. 60), str. 271-290.

[73] Neki autori upućuju na mogućnost kvalificiranja kibernetičke operacije kao uporabe sile pod pretpostavkom da ona ozbiljno utječe na ključnu državnu infrastrukturu, što dokazuju primjerom

5. PRAVILA I KOMENTARI TALLINNSKOG PRIRUČNIKA

Uvodni dio otkriva kako je proveden proces utvrđivanja pravila prilikom izrade Priručnika i navodi da ona odražavaju postignuto suglasje između članova Međunarodne skupine glede primjenjivosti *lex lata*.[74] Ne iznosi se *lex ferenda*. Članovi Međunarodne skupine bili su suglasni da pravila Priručnika predstavljaju presliku običajnog međunarodnog prava (osim ako izričito nije drugačije navedeno),[75] pri čemu su pojedini članovi povremeno upućivali na potrebu primjene različitih standarda identifikacije (strožih ili liberalnijih) u odnosu na one koji su u konačnici dogovoreni.[76] To znači da ona sadržajno predstavljaju odraz pravila međunarodnog prava primjenjivih na materiju kibernetičkog ratovanja, što smo pokazali na primjeru pravila koja reguliraju uporabu sile, a bit će vidljivo i iz analize pravila o definiciji kibernetičkog napada.[77] Prema nekima razvoj norma za ponašanje država u kibernetičkom prostoru kao takav ne čini postojeće međunarodne norme zastarjelima.[78] Istodobno ponovno upućujemo na savjetodavno mišljenje Međunarodnog suda o legalnosti nuklearnog oružja, koji smatra da se *jus ad bellum* primjenjuje na bilo koju uporabu sile neovisno o tome koje se oružje koristi te da je oružani sukob, čim postoji, reguliran pravilima međunarodnog humanitarnog prava.[79] Pri stvaranju pravila osobito se pazilo i na terminologiju.[80] To je vidljivo iz primjera pravila kojim se „kibernetička sredstva ratovanja" definiraju kao kibernetička oružja i njihovi pridruženi kibernetički sistemi (pravilo 41a). Unatoč svemu Priručnik ne polaže pravo da bude nacrt za norme neke buduće konvencije o uporabi sile u kibernetičkom prostoru.[81] On samo predlaže stanovita pravila koja bi trebala biti korištena u donošenju odluka u složenim pitanjima kibernetičkog sukoba i u tom smislu, kako smo objasnili, ne unosi neke naročite novine u pozitivno međunarodno pravo.[82] Smatramo da prava vrijednost tih pravila proizlazi iz njihove praktičnosti, što znači da ona mogu poslužiti

manipulacije podataka o državnoj ekonomiji koja ima ozbiljne negativne posljedice na državnu ekonomsku i političku dobrobit. V. Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 22.

[74] Str. 5 uvoda Priručnika.

[75] Uvod Priručnika spominje pravilo 38, koje je gotovo identično tekstu članka 52. stavka 2. Protokola I. U komentaru tog pravila dodatno se navodi stajalište članova Međunarodne skupine, prema kojem takva ugovorna odredba predstavlja pouzdanu i točnu potvrdu običajnog međunarodnog prava.

[76] Jednoglasnost potrebna za usvajanje teksta pravila odnosila se samo na članove Međunarodne skupine, ali ne i na promatrače, unatoč njihovu aktivnom sudjelovanju u svim raspravama pri izradi sadržaja Priručnika (v. *supra*, bilj. 14).

[77] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 131.

[78] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 9-10. S druge strane postavlja se pitanje dometa do kojeg postojeća pravna norma može na odgovarajući način biti primijenjena na nove tehnologije, metode, sredstva ratovanja i strateške okolnosti. Ta se tematika dijeli na dva međusobno različita, ali bitno povezana pitanja, odnosno primjenjuje li se pojedinačno pravilo u novom kontekstu te, ako se primjenjuje, na koji način. To su temeljna pitanja kojima se mnogi autori (poput autora Tallinnskog priručnika) bave. V. Boothby, H., W., *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors*, 2014, str. 9.

[79] ICJ Reports 1996, *op. cit.* (bilj. 50), st. 39.

[80] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 132. Npr. predgovor prvog poglavlja sadrži objašnjenje pojma „kibernetičke operacije" i navodi da se taj pojam odnosi na uporabu kibernetičkih kapaciteta s primarnom svrhom ostvarenja ciljeva u kibernetičkom prostoru.

[81] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 11.

[82] McGhee, *op. cit.* (bilj. 22), str. 24.

državama kao prikladni alat u oblikovanju njihova ponašanja u kibernetičkom prostoru i u pitanjima koja su s njim povezana. S navedenim se slažu i drugi autori.[83] S obzirom na to da je Priručnik sačinjen radi opisa *lex lata* u odnosu na kibernetičko ratovanje, njegova se pravila fokusiraju samo na one kibernetičke operacije koje se smatraju najrazornijima, odnosno odražavaju spomenuti *jus ad bellum* i *jus in bello* (no ne beziznimno, jer su neka pravila posvećena i drugim pitanjima, poput suvereniteta o kojem smo govorili u početnom dijelu ovoga rada, zatim sudbene nadležnosti, imuniteta, odgovornosti država, protumjera i dr.).

Komentari imaju ključnu ulogu u ostvarenju prethodno navedenih funkcija time što upozoravaju na sva bitna pitanja interpretacije i primjene tih pravila. Komentari objašnjavaju pravilo dovodeći ga u svezu s izvorom međunarodnog prava na kojem se ono temelji i pokazuju kako je Međunarodna skupina došla do zaključka da se odnosno pravilo može primijeniti u materiji kojom se Priručnik bavi.[84] Dakle njihova je svrha utvrditi pravni temelj samog pravila te objasniti njegove normativne implikacije, uz istodobno upućivanje na praktični domašaj (u kibernetičkom kontekstu).[85] Kako se Priručnik odnosi na pitanja međunarodnoga i nemeđunarodnoga oružanog sukoba, komentari sadrže naznaku kada je koje od sadržanih pravila primjenjivo na obje navedene kategorije. Primjer nalazimo u pravilu prema kojemu su dopuštene kibernetičke operacije koje se kvalificiraju kao lukavstvo (pravilo 61), a čiji komentar navodi da je takvo lukavstvo dopušteno u objema navedenim kategorijama oružanog sukoba. Slažemo se s mišljenjem autora koji smatraju da važnost komentara proizlazi iz toga što oni otkrivaju pitanja (u svezi s pravilima Priručnika na koja se odnose) glede kojih je postojalo suglasje stručnjaka Međunarodne skupine, kao i pitanja glede kojih takvo suglasje nije postojalo, odnosno gdje su postojala većinska i manjinska mišljenja u skupini.[86] Prema tome svatko tko želi otkriti teme koje su bile predmet nesuglasja treba izvršiti uvid u prateće komentare u kojima se čitateljima otkrivaju mnoge korisne informacije, poput prijedloga pravila, njihovih razloga i značenja te (važnija) pitanja o kojima u konačnici nije postignuta suglasnost.[87] Tako je primjerice u komentaru pravila o dopuštenosti lukavstva naznačeno da je Međunarodna skupina bila podijeljena u mišljenju o zakonitosti maskiranja računala ili računalne mreže radi prikrivanja unutar civilnog sustava na način koji ne predstavlja perfidiju. Na značaj statusa komentara upućuje i uvodni dio Priručnika, koji naglašava bitno nastojanje njegovih donosilaca da se (za potrebe daljnjeg razmatranja od strane korisnika) u komentare uključe sva (značajnija) iznesena stajališta, a sve s obzirom na nerazvijenost ugovorne primjene i prakse država u kontekstu kibernetičkog ratovanja u međunarodnom pravu.[88] Navedene tvrdnje oživotvorit ćemo čitateljima u nastavku ovoga

[83] V. npr. Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 12.
[84] Boothby, *op. cit.* (bilj. 78), str. 74.
[85] Međunarodna se skupina u komentarima često pozivala na sadržaj vojnih priručnika iz SAD-a, Kanade, Njemačke i Velike Britanije.
[86] Boothby, *op. cit.* (bilj. 78), str. 74.
[87] *Ibid*.
[88] Str. 6 uvoda Priručnika.

poglavlja iznošenjem bitnih postavaka pravila Priručnika glede definicije kibernetičkog napada (agresije).

Priručnik definira kibernetički napad (agresiju) kao kibernetičku operaciju poduzetu u napadu ili obrani za koju je razumno očekivati da će prouzročiti ozljedu ili smrt osoba, odnosno štetu ili uništenje objekata (pravilo 30). Temelj toga pravila leži u definiciji pojma napad iz članka 49. stavka 1. Protokola I., koja glasi: „"Napad" znači djela nasilja protiv protivnika poduzeta u napadu ili obrani." Početni nam komentari otkrivaju da je za potrebe definiranja kibernetičkog napada upućivanje na pojam „djela nasilja" iz citiranog članka potrebno provesti na način da se time istodobno ne ograničava opseg napada na aktivnosti kojima se oslobađa isključivo kinetička snaga.[89] Takvo stajalište Međunarodna skupina temelji na postojećim shvaćanjima prava oružanih sukoba, što dokazuje primjerom biološkog i kemijskog napada, koji (obično) ne rezultiraju kinetičkim učinkom, ali istodobno nema dvojbe da takva djela predstavljaju oružani napad u međunarodnopravnom smislu.[90] Druga bitna značajka na koju nas komentari upućuju odnosi se na problematiku visine praga posljedične štete, temeljem kojega se određuje potpada li doista kibernetička operacija pod definiciju kibernetičkog napada iz Priručnika. Drugim riječima, fokus na pitanje što sačinjava kibernetički napad uvelike je usmjeren na posljedice kibernetičkih operacija.[91] I mnogi autori smatraju da je precizno utvrđenje posljedica kibernetičkih operacija središnja komponenta definicije kibernetičkog napada.[92] Priručnik navodi da napad u kibernetičkom prostoru mora rezultirati ozljedom, smrću, štetom ili uništenjem da bi se mogao kvalificirati kao oružani napad prema međunarodnom pravu.[93] Analiza je primarno usmjerena na nasilne posljedice takva napada.[94] Dakle u svojim raspravama Međunarodna skupina polazi od stajališta prema kojem o posljedičnoj šteti koja proizlazi iz kibernetičke operacije ovisi moguća kvalifikacija te aktivnosti kao napada. Ta naizgled jednostavna početna postavka ima cijeli niz teškoća u svojoj praktičnoj primjeni i upravo je zbog toga Međunarodna skupina najveći dio svojih komentara tog pravila posvetila spomenutoj problematici; primjerice kako kvalificirati prag štete koja se sastoji u ometanju funkcionalnosti objekta; što ako cilj napada nije ni svjestan da je napadnut; doseže li traženi prag napada šteta koja se može otkloniti reinstalacijom operativnog sustava; kakve su pravne postavke ako šteta ne nastane uslijed uspješnog korištenja sredstava kibernetičke obrane itd. Detaljna analiza navedene problematike prelazila bi ambicije ovoga članka, no u svrhu ilustracije niza kritika kojima su rješenja Priručnika izložena spomenut ćemo mišljenja pojedinih autora koji smatraju da je izložena definicija prejednostavna i da ne obuhvaća složene nijanse

[89] Norris, M., J., *The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of „Attack" in the Digital Battlespace*, u: Inquiries Journal, vol. 5, br. 10, str. 1.
[90] Opširnije o konceptu pojma oružanog napada u međunarodnom pravu v. Seršić, *op. cit.* (bilj. 60), str. 274-282.
[91] Norris, *op. cit.* (bilj. 89), str. 1.
[92] *Ibid*, str. 3.
[93] Lawor, *op. cit.* (bilj. 10), str. 8.
[94] Collin, A., *Direct Participation in Hostilities from Cyberspace*, u: Virginia Journal of International Law, vol. 54, br. 1, str. 183.

kibernetičkog ratovanja.[95] Slažemo se s tim mišljenjem. Naime, kako i sam Priručnik navodi, spektar kibernetičkih napada širok je zbog same prirode kibernetičkog prostora, koja pruža mogućnosti za cijeli niz djelatnosti s različitim kinetičkim i nekinetičkim posljedicama, čiji se učinci kreću od posve bezopasnih do (veoma) razornih. Iz istog razloga pozitivno cijenimo mišljenja prema kojima u današnjem digitalnom društvu takva definicija nužno mora uzeti u obzir i moguće učinke manipulacije podacima i izmjene raznih mrežnih standarda rada, sve radi uzrokovanja virtualnih uništenja ili poremećaja.[96] Iz takvih razmišljanja proizlaze pojedini prijedlozi da se definicija proširi na način da se u nju uključi i pojam neutralizacije.[97] S obzirom na to da vojna prednost proizlazi iz pukog onesposobljavanja predmeta (vojnog cilja), neovisno o načinu do kojega je do toga došlo (uništenjem, oštećenjem ili na drugi način), takvo proširenje definicije smatramo odgovarajućim.[98] S obzirom na to da neutralizacija nije novi koncept u međunarodnom pravu, štoviše, nalazimo ga u definiciji vojnih ciljeva u članku 52. stavku 2. Protokola I., ostaje nejasno potpuno ignoriranje tog pojma od strane Međunarodne skupine pri izradi definicije kibernetičkog napada, kao i u njezinim popratnim komentarima.

6. AUTORITET I OPĆI ZNAČAJ TALLINNSKOG PRIRUČNIKA

Autoritet Tallinnskog priručnika najbolje je sažeo njegov glavni urednik riječima da taj Priručnik nije službeni dokument, nego rad skupine neovisnih stručnjaka, koji su pri njegovoj izradi sudjelovali isključivo u svojem osobnom svojstvu. Neovisno o znanju i dugogodišnjem iskustvu članova Međunarodne skupine ostaje činjenica da Tallinnski priručnik nije međunarodno obvezujući dokument, nego tekst obuhvaćen pod pojmom „međunarodni priručnik".[99] Za proces nastanka takvih radova karakteristično je da započinje okupljanjem grupe iskusnih pojedinaca, najčešće znanstvenika i praktičara, na inicijativu određenog tijela, radi rješavanja stanovitih problema koji proizlaze iz zadane teme izučavanja.[100] Iz prvog dijela ovoga članka vidljivo je da se u tom smislu ovaj Priručnik ne razlikuje od drugih istovrsnih priručnika te se kao primjer često upućuje na poznati Sanremski priručnik.[101] Dakle treba ga karakterizirati ni manje ni više nego kao

[95] Stavridis, J., G., *Incoming: What Is a Cyber Attack?*, u: Signal Magazine, 1. siječanj 2015., str. 1.
[96] *Ibid*.
[97] Takva definicija glasila bi: „Kibernetički je napad kibernetička operacija poduzeta u napadu ili obrani za koju je razumno očekivati da će prouzročiti ozljedu ili smrt osoba, odnosno štetu, uništenje ili neutralizaciju objekata." V. Norris, *op. cit.* (bilj. 89), str. 1. Predlažu se i druge definicije, npr. „Kibernetički je napad namjerna projekcija kibernetičke sile koja rezultira kinetičkim ili nekinetičkim posljedicama koje prijete nacionalnoj sigurnosti ili je na drugi način destabiliziraju, štete ekonomskim interesima, stvaraju političku ili kulturnu nestabilnost ili štete pojedincima, napravama ili sustavima." V. *ibid*, str. 2.
[98] U tom slučaju dodatni izazov postaje jasno formuliranje sadržaja pojma neutralizacija kako bi se izbjegla preširoka definicija „kibernetičkog napada", koja bi mogla obuhvatiti puku neugodnost i ometanje. V. npr. Norris, *op. cit.* (bilj. 89), str. 2-3.
[99] Neki autori smatraju da se pojam „međunarodni priručnik" odnosi na bilo koji tekst koji se obično sastoji od izjava pravnog karaktera ili pravne regulacije, a objavljuje se s pridruženim komentarima koji ga objašnjavaju, i čiji dijelovi ili cjelina sadržavaju suglasna gledišta stručnjaka koji su pripremili tekst ili one dijelove o kojima je postignuta suglasnost. V. Boothby, *op. cit.* (bilj. 78), str. 66.
[100] Opširnije o donesenim međunarodnim priručnicima i njihovim donosiocima v. npr. *ibid*.
[101] Puni naziv: Sanremski priručnik o međunarodnom pravu primjenjivom na oružane sukobe na moru (engl. *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*).

konsenzus akademskog rada skupine međunarodnih stručnjaka koji su posvetili tri godine identifikaciji postojećeg prava primjenjivog na kibernetičko ratovanje.[102] Rezultat je nastanak svojevrsnog alata koji državama može poslužiti u oblikovanju njihova ponašanja u kibernetičkom prostoru. No autoritet ovoga rada donekle je doveden u pitanje uslijed problematike geografske neujednačenosti u kontekstu sastava Međunarodne skupine. U početnom dijelu ovoga članka spomenuli smo da je većina članova dolazila iz zemalja članica NATO-a. Tako Talinska razmatranja izostavljaju predstavnike Kine, Rusije i drugih nacija i kultura za koje se moglo smatrati da imaju značajan interes u raspravljanju o naglašavanju hermeneutičkih principa, kao i rezultata pokušaja ekstrapoliranja postojećeg međunarodnog prava na kibernetičku domenu.[103] Unatoč navedenome smatramo da ipak postoji razumno očekivanje da taj dokument, ili barem njegovi pojedini dijelovi, steknu opće odobrenje i tih zemalja te s tom svrhom podsjećamo čitatelje ovoga članka na stajalište onih autora koji ističu da glavni doktrinarni radovi iz područja međunarodnog prava ionako pretežito dolaze iz (kolokvijalno govoreći) zapadnih/sjevernih zemalja, posebno iz manje skupine nekoliko tih zemalja gdje je razvoj i izgradnja međunarodnog prava dosegnula poprilično visok stupanj.[104] Zato smatramo da nema mjesta zaključku da Priručnik odražava isključivo europsko kontinentalno i anglosaksonsko pravo (u kontekstu podjele međunarodnog prava na opće i posebno (partikularno, npr. regionalno)), a da pravna shvaćanja ostalih zemalja i nacija nisu uzeta u obzir.

U pogledu njegova općeg značaja ovaj dokument cijenimo vrijednim doprinosom u produbljivanju i boljem razumijevanju primjene međunarodnog prava u kibernetičkom prostoru, a time i međunarodnog prava kibernetičke sigurnosti kao cjeline. S tim se mišljenjem slažu i drugi autori.[105] Analizirajući dostupnu građu za potrebe izrade ovoga rada, nismo našli dokaz za tvrdnju da je Priručnik stekao opće prihvaćanje, priznanje ili odobravanje. Samo će vrijeme pokazati hoće li i ovaj Priručnik biti uspješan kao spomenuti Sanremski priručnik. Slažemo se s mišljenjem pojedinih autora da je ovaj dokument dobra početna točka za daljnje analize i zaslužuje pohvalu jer daje doprinos boljem razumijevanju međunarodnog prava primjenjivog na kibernetičko ratovanje.[106] Spomenimo i da će Priručnik pridonijeti daljnjim pravnim razgovorima i razmatranjima time što će služiti kao temelj koji se daljnjim akademskim radom može nadograđivati.[107] U tom smislu dodatno cijenimo početni dio Priručnika, u kojem se razmatraju opća pitanja međunarodnog prava kibernetičke sigurnosti (sudska nadležnost, odgovornost država, opća zabrana uporabe sile i dr.). Bez sveobuhvatnog razumijevanja tih tema nema ni pravilne primjene ostalih norma mjerodavnih za kibernetičko ratovanje, što smo pokazali u kratkom osvrtu na pravilo o suverenosti. No spomenimo i da naše mišljenje ne dijele svi.

[102] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 4.
[103] Henschke, Strawser, *op. cit.* (bilj. 18), str. 17-18.
[104] V. npr. Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 11.
[105] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 131-132.
[106] Roscini, *op. cit.* (bilj. 4), str. 32.
[107] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 16.

Primjerice Rusija se trenutačno ne slaže s pozitivnom ocjenom i smatra da se radi o dokumentu koji ozakonjuje kibernetičko ratovanje.[108]

Donošenje ovog dokumenta može označiti svojevrsnu početnu točku procesa nastanka općeg dogovora o primjenjivosti i obuhvatu pravila i principa međunarodnog prava mjerodavnog za pitanja uporabe sile i ponašanja u neprijateljstvima u kibernetičkom prostoru, što bi države svakako trebale pozdraviti.[109] Smatramo da je u okolnostima rastuće važnosti komunikacijske i informacijske tehnologije bilo krajnje vrijeme da se objasni primjenjivost *jus ad bellum* i *jus in bello* na operacije u kibernetičkom prostoru. S tim se mišljenjem slažu i drugi autori.[110] S obzirom na izniman značaj tematike kibernetičkog ratovanja, a istodobno ne dovodeći u pitanje novi priručnik NATO-ova Centra izvrsnosti, u kojem se ispituju mogući odgovori država na kibernetičke operacije ispod praga oružanog napada i uporabe sile (v. *supra,* poglavlje 3, odjeljak 2), stajališta smo da je došlo vrijeme za donošenje suvremenog pravno obvezujućeg međunarodnog dokumenta (na razini konvencije) koji bi sveobuhvatno sabrao takva pravila. To bi ujedno bila odlična prilika za iznalaženje novih pravnih rješenja, ili barem prilika za početak ozbiljnije rasprave o cijelom nizu sve aktualnijih pitanja. S tim se mišljenjem slažu i drugi autori, a neki od njih predlažu da takav projekt bude proveden pod okriljem Ujedinjenih naroda.[111] Autor tu inicijativu smatra odgovarajućom iz razloga što su Ujedinjeni narodi organizacija stvorena upravo sa svrhom ostvarenja određenih zadatka za cijelu međunarodnu zajednicu te u čijem se okrilju stvara običajno međunarodno pravo.[112]

7. ZAKLJUČAK

Završavajući rad, Tallinnskom priručniku dajemo pozitivnu ocjenu unatoč cijelom nizu ograničenja na koja smo upozorili. Smatramo da njegova jedinstvenost proizlazi iz primjene *lex lata* na (relativno) novo tehnološko okružje jer je kibernetička tehnologija (kakvu danas poznajemo) novina u odnosu na tradicionalna pravila međunarodnoga prava. Kibernetički napadi (i svaka druga uporaba kibernetičke tehnologije u svrhu zlonamjernog iskorištavanja digitalnih prednosti) danas predstavljaju novi i stvarni oblik opasnosti za državu, društvo i pojedinca. U tim je okolnostima bilo nužno donijeti dokument koji bi državama pružio barem smjernice prilikom provođenja njihovih tuzemnih i međunarodnih interesa u kibernetičkom prostoru (i svim drugim mogućim oblicima korištenja kibernetičke tehnologije). Tallinnski priručnik želi pružiti upravo takvu analizu te pojasniti obuhvat primjenjivosti postojećih norma međunarodnog prava koje reguliraju uporabu sile prije oružanog sukoba i tijekom njega. Upitno je hoće li i u kojoj mjeri u budućnosti biti postignut konsenzus o nizu pitanja iz domene kibernetičkog ratovanja i drugih oblika operacija u kojima se koristi kibernetička tehnologija, zato

[108] V. npr. http://www.derechos.org/nizkor/espana/doc/cyberwar.html (pristup: 23. veljače 2016.).
[109] Gill, Greib, Heinsch, McCormack, Paulussen, Dorsey, *op. cit.* (bilj. 14), str. 16.
[110] *Ibid*, str. 17.
[111] Gladyshev, Marrington, Baggili, *op. cit.* (bilj. 33), str. 131-132.
[112] Andrassy, Bakotić, Lapaš, Seršić, Vukas, *op. cit.* (bilj. 35), str. 119 i 125.

napore poput ovog Priručnika, koji teže da daju jasnoću praksi koja se razvija, moramo pozdraviti. Kako smo spomenuli, u ovome trenutku ne nalazimo dokaz za održivost tvrdnje prema kojoj ovaj dokument polaže pravo da bude smatran nacrtom za norme neke buduće konvencije o ponašanju i (naročito) uporabi sile u kibernetičkom prostoru. Naime Tallinnska razmatranja nemaju imperativni, nego savjetodavni karakter. Ona ne nalažu, nego samo predlažu stanovita ponašanja u kontekstu *jus ad bellum* i *jus in bello* dajući time istodobno doprinos boljem razumijevanju međunarodnog prava kibernetičke sigurnosti u cjelini. Kako smo u prethodnom poglavlju naglasili, samo će vrijeme pokazati hoće li i u kojoj mjeri ovaj dokument biti uspješan. Autor ovoga rada i dalje smatra da Priručnik predstavlja dobru početnu točku za daljnje analize ponašanja pri provođenju neprijateljstava u kibernetičkom prostoru. Istodobno izražavamo nadu da će te analize u konačnici rezultirati donošenjem novog pravno obvezujućeg odgovarajućeg međunarodnog dokumenta neovisno o njegovu nazivu i formi. Završno ovom prilikom možemo samo ponovno izraziti žaljenje što u izradu Tallinnskog priručnika nije bio uključen širi krug subjekata kao odraz svih (ili barem glavnih) svjetskih pravnih kultura, no i nadalje ostajemo pri stajalištu da taj nedostatak nije presudan za pitanje njegova autoriteta i (pozitivnu) opću ocjenu njegova značaja kao dijela mozaika u procesu nastanka svojevrsnog cjelovitog međunarodnopravnog kibernetičkog oklopa.

Summary

OVERVIEW OF THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE

In this article, the author presents the basic features of the Tallinn Manual on the International Law Applicable to Cyber Warfare. The first part of the paper presents its general drafting process, structure, legal scope, prohibition of the use of force, and the right of self-defence, followed by a presentation of the main characteristics of the adopted rules and accompanying commentaries. The author continues the article with a discussion of the authority and overall meaning of the Manual. The final part contains a conclusion related to the Manual's success, combined with a summary of the basic facts and recapitulations as stated in the appropriate analytical chapters of the article.

Keywords: cybernetic warfare; lex lata; international manual; use of force

Ratimir Prpić, a student of postgraduate study at the Faculty of Law, University of Zagreb