Treći program
Broj 161–162, ZIMA–PROLEĆE 2014

Originalan naučni rad

341.3
343.533::004

COBISS.SR-ID 222304524

MLADEN MILOŠEVIĆ i NENAD PUTNIK*

PROBLEM PRAVNE (NE)REGULISANOSTI KONFLIKATA U KIBER PROSTORU

Članak je posvećen razmatranju problema pravne neregulisanosti konflikata u kiber prostoru. Autori raspravljaju o mogućim pravnim kvalifikacijama čina kiber ratovanja, ukazujući da se on ne može podvesti pod definiciju agresije usvojenu u rezoluciji Ujedinjenih nacija, ali da je ipak nedovoljno karakterisati ga kao krivično delo kažnjivo po odredbama nacionalnih zakonodavstava. U centralnom delu rada autori analiziraju nekoliko međunarodnih ugovornih režima: međunarodno ratno pravo, Sporazum o neširenju nuklearnog naoružanja, međunarodno kosmičko pravo, Sistem antarktičke povelje, Konvenciju Ujedinjenih nacija o pravu mora i ugovore o uzajamnoj pravnoj saradnji, kako bi utvrdili da li oni mogu služiti kao model za regulisanje međudržavnih konflikata u kiber prostoru.

Ključne reči: međunarodno ratno pravo, savremeno ratovanje, kiber ratovanje

Uvod

Nastanak kiber prostora predstavljao je svojevrsnu prekretnicu u sferi vojnih aktivnosti, ali i u poimanju korporativne, nacionalne, regionalne i globalne bezbednosti. Novi „prostor" pružio je velike mogućnosti za sprovođenje specijalnih propagandnih dejstava, ali i za izvođenje napada na protivničke informacione sisteme posredstvom računarskih mreža. Za ovaj novi vid konfrontacije u virtuelnom prostoru se u anglosaksonskom govornom području koristi pojam kiber ratovanje (engl. *cyber warfare*).

Kiber ratovanje jeste relativno nov i specifičan oblik društvenog konflikta, koji se vodi u specifičnom okruženju (kiber prostoru), specifičnim sredstvima (malicioznim kodovima i drugim softverskim alatima), sa specifičnim obeležjima i principima. Ovaj vid konflikta može se voditi samostalno ili kao podrška konvencionalnom, kinetičkom sukobu. Aktivnost kiber ratovanja ne mora biti ograničena samo na sferu vojnih aktivnosti.

* Univerzitet u Beogradu, Fakultet bezbednosti; e-mail: milosevic@fb.bg.ac.rs; nputnik@fb.bg.ac.rs

Individualni korisnici informaciono-komunikacionih tehnologija i politički (ideološki) motivisane društvene grupe koriste taktike i strategije kako bi tačno odredili mete napada u virtuelnom prostoru i postigli svoje ciljeve, na način koji nalikuje vojnim metodama. Prvobitno su teoretičari bili skloni da kiber ratovanje svrstaju u kategoriju „rata bez žrtava". Međutim, praksa je pokazala da napadi u virtuelnom prostoru, naoko neprimetni, mogu u realnom, fizičkom svetu rezultovati ljudskim žrtvama i materijalnim razaranjima. Zbog toga je kiber ratovanje danas u žiži interesovanja teoretičara i stručnjaka iz oblasti vojnih, pravnih, bezbednosnih i informatičkih nauka u svim državama zavisnim od informaciono-komunikacionih tehnologija.

Kiber ratovanje ne samo da preispituje određene konvencionalne pretpostavke o prirodi društvenih konflikata, već u isto vreme ilustruje i neke od skrivenih mogućnosti i paradoksalnih potencijala (socijalna fuzija i fisija) globalno umreženih tehnologija. Ono, takođe, pokreće mnoštvo pitanja vezanih za etičnost ofanzivnog kiber ratovanja i adekvatnost postojećih multilateralnih propisa i konvencija u koje bi se ovi novi modaliteti morali uklopiti. Naročito važan problem predstavlja nepostojanje opšte saglasnosti o međunarodnim sporazumima koji bi razjasnili pravni status država i nedržavnih aktera u kiber konfliktima. Zapravo, celokupno polje kiber prava još uvek je nedovoljno razvijeno.

Problem pravnog statusa kiber konflikata

Ako se u obzir uzmu katastrofalne posledice koje kiber napadi mogu izazvati, od vitalnog je značaja da države budu osposobljene da efikasno odbrane svoju kritičnu infrastrukturu od napada. Najefikasniji način za odbijanje kiber napada jeste upotreba slojevitog sistema odbrane, sastavljenog od mera aktivne i pasivne odbrane.[1] U praksi, međutim, države namerno biraju isključivo mere pasivne odbrane, iz straha da bi korišćenjem mera aktivne odbrane prekršile međunarodno ratno pravo.

Za aktivnosti koje nazivamo kiber ratovanjem, iako se one sprovode već više od deset godina, u međunarodnom ratnom pravu još uvek nije

[1] Mere aktivne odbrane su elektronske mere kontranapada koje su osmišljene tako da uzvrate napad računarskim sistemima sa kojih je napad potekao i da zatvore „kanal" napada. Eksperti u oblasti informaciono-komunikacionih tehnologija mogu paodesiti mere aktivne odbrane tako da automatski odgovore na napade protiv kritičnih sistema, ili ih mogu aktivirati manuelno. Mere pasivne odbrane su tradicionalne forme računarske bezbednosti koje se koriste za zaštitu računarskih mreža, kao što su: kontrola pristupa sistemu, kontrola pristupa podacima, projektovanje i dizajniranje bezbednog sistema i održavanje njegove funkacionalnosti, primena fizičkih i logičkih fajervol uređaja, korišćenje antivirusnih programa i sl.

pronađena adekvatna definicija. U ovom trenutku, dakle, ne postoji sveobuhvatni međunarodni sporazum koji bi regulisao kiber napade, tj. pružio neku pravnu definiciju čina kiber agresije (Mladenović, 2012).

U tom smislu, zvaničnici američke vojske, među kojima i šef Strateške komande Sjedinjenih država, general vazduhoplovstva Kevin Čilton (Kevin P. Chilton), već nekoliko godina najavljuju da će se međunarodno ratno pravo primeniti na ovu oblast (Schogol, 2009). Još uvek nije poznato da li su sa ovim stavom saglasne i druge države, naročito Ruska Federacija i Narodna Republika Kina.

Iz javno dostupnih izvora može se saznati da Rusija favorizuje međunarodne sporazume poput onih postignutih pregovorima o hemijskom naoružanju, i da je agitovala za takav pristup na brojnim skupovima proteklih godina, kao i u javnim izjavama visokih zvaničnika (Markoff & Kramer, 2009).

Sjedinjene Američke Države, pak, tvrde da sporazum nije neophodan. Umesto toga, one zagovaraju bolju saradnju međunarodnih agencija za sprovođenje zakona. Ukoliko ove agencije sarađuju tako da učine kiber prostor bezbednijim u pogledu kriminalnih aktivnosti, njihov rad će ga učiniti sigurnijim i u pogledu vojnih kampanja.

Zbog pravne neregulisanosti ove oblasti države su, u praksi, stavljene pred izbor da li će izjednačavati kiber napade sa tradicionalnim oružanim napadima i odgovarati na njih prema međunarodnom ratnom pravu, ili će kiber napade izjednačavati sa kriminalnim aktivnostima i odgovarati na njih u skladu sa domaćim krivičnim zakonima i međunarodnim konvencijama o kiber kriminalu. Stav koji preovladava među državama i pravnim ekspertima jeste da države moraju da tretiraju kiber napade kao kriminalna dela: 1) zbog nesigurnosti oko toga da li se kiber napad može smatrati oružanim napadom, i 2) zbog toga što međunarodno ratno pravo zahteva od država da pripišu oružani napad nekoj stranoj vladi ili njenim akterima pre nego što odgovore silom.

Kako bismo ispitali zasnovanost navedenih stavova, osvrnućemo se na pravne argumente za obe teze, imajući u vidu mogućnosti koje pruža oslanjanje na norme međunarodnog ratnog prava i nacionalnih krivičnih zakonodavstava (kao i međunarodnog krivičnog prava), i uporediti razloge koji govore u prilog jednoj ili drugoj.

Pri tome, ne treba zaboraviti da definisanje čina kao agresorskog ne isključuje krivičnu odgovornost pojedinca kome se takav akt može pripisati (država kao pravno lice nije subjekt krivične odgovornosti, te u krivičnopravnom smislu ne odgovara). Vođenje rata je zabranjeno normama najvažnijih akata međunarodnog prava. Države su ovlašćene da primenjuju mere individualne i kolektivne samoodbrane jedino u slučaju agresije od strane druge države (ili država). Agresija se, u skladu s prethodno rečenim,

na osnovu preporuka akata međunarodnog prava u nacionalnim zakonodavstvima smatra za krivično delo.

Dakle, ukoliko kiber napad tumačimo kao vid agresije, učinioci ovog akta bili bi podložni krivičnoj odgovornosti, a država kojoj bi se napad pripisao bila bi okarakterisana kao agresor po pravilima međunarodnog prava. No, osvrnimo se na kratak istorijat zabrane i inkriminisanja agresorskih akata.

Agresija je prvi put definisana kao krivično delo – zločin protiv mira u članu 6 Statuta Međunarodnog vojnog tribunala u Nirnbergu, kao: „planiranje, pripremanje, započinjanje ili vođenje agresorskog rata ili rata kojim se krše međunarodni ugovori, sporazumi ili garancije, ili učestvovanje u nekom zajedničkom planu ili zaveri za izvršenje ma kog od gore navedenih dela“ (Vučinić, 2013).

Za suđenje zbog krivičnog dela protiv mira bio je nadležan i Tokijski tribunal. Od tada, međutim, niko nije bio osuđen za zločin protiv mira.

Agresorski rat je bio zabranjen i pre suđenja u Nirnbergu, Brijan-Kelogovim paktom iz 1928. godine, mada njime nije bila uvedena potpuna zabrana svakog rata. To će se desiti tek usvajanjem Povelje Ujedinjenih nacija (UN), koja dopušta isključivo odbrambeni rat i prinudne mere samih UN. Sprečavanje sile u međudržavnim odnosima jedno je od osnovnih načela UN, a posebno se ovim pitanjima bave članovi 1, 2, 33 i 39 Povelje UN.

Ipak, ključni korak načinjen je usvajanjem Rezolucije Generalne skupštine Ujedinjenih nacija br. 3314 iz 1974. godine. Rezolucijom je data precizna definicija agresije, a navedeni su i konkretni akti koji se smatraju agresorskim po slovu rezolucije.

Rezolucija daje osnovni kriterijum za karakterisanje čina kao agresorskog, pošto eksplicitno podvlači da „prvootpočinjanje upotrebe oružane sile od jedne države protivno Povelji predstavlja *prima facie* dokaz izvršenja akta agresije“.

Član 3. Rezolucije navodi konkretne pojavne oblike izvršenja agresije, to jest definiše koji se oblici upotrebe sile smatraju agresorskim činom:

- invazija ili napad oružanih snaga jedne države na teritoriju druge države, ili svaka vojna okupacija, makar i privremena, koja proizađe iz takve invazije ili napada, ili aneksija teritorije ili dela teritorije druge države upotrebom sile;
- bombardovanje teritorije neke države od strane oružanih snaga druge države ili upotreba ma kog oružja od strane jedne države protiv teritorije druge države; blokada luka ili obala jedne države od strane oružanih snaga druge države;
- napad oružanih snaga jedne države na kopnene, pomorske ili vazduhoplovne snage, pomorsku ili vazdušnu flotu druge države;
- upotreba, od strane jedne države, oružanih snaga koje se s pristankom zemlje prijema nalaze na teritoriji ove poslednje, protivno uslovima predviđenim u spo-

razumu, odnosno ostajanje tih snaga na teritoriji zemlje prijema i posle isteka sporazuma;
- radnja jedne države koja svoju teritoriju stavi na raspolaganje drugoj državi da bi je ova iskoristila za izvršenje akta agresije protiv treće države;
- upućivanje od strane, odnosno u ime jedne države oružanih bandi, grupa, neregularnih vojnika ili najamnika, koji protiv druge države vrše akte oružane sile toliko ozbiljno da se izjednačuju sa gore pomenutim aktima, odnosno značajno učešće jedne države u tome.

Rezolucija podvlači da nikakvi razlozi bilo koje prirode ne mogu služiti kao opravdanje za agresiju, te da agresija povlači međunarodnu odgovornost, dok agresorski rat predstavlja zločin protiv međunarodnog mira, što podrazumeva i krivičnu odgovornost pojedinaca kojima bi se u skladu sa pravilima krivičnog prava moglo pripisati ostvarenje bića krivičnog dela zločina protiv mira (Kreća, 2012).

Na planu međunarodnog krivičnog prava preduzeti su dalji koraci ka inkriminisanju agresorskog čina i uvođenju nadležnosti međunarodnog krivičnog suda, ali su pisci Statuta Međunarodnog krivičnog tribunala ostavili mesta novoj nedoumici. Rimski statut Međunarodnog krivičnog suda predviđa da je ovaj sud odgovoran za te zločine, ali uslovno. To znači da će sud u praksi postati nadležan tek kada se Statut dopuni određivanjem pojma agresije i kada se utvrde i drugi uslovi pod kojima će sud biti nadležan za ovo krivično delo. Nije jasno zašto Sud nije prihvatio definiciju agresije iz Rezolucije 3314 UN (Stojanović, 2012). Pitanje je da li se ovo može tumačiti (ili barem iskoristiti) kao potez kojim se ide ka redefinisanju agresije na nivou međunarodnog prava, uz širenje njenog pojma i na druge, sada izostavljene akte.

U domaćem krivičnom zakonodavstvu zločin protiv mira predviđen je članom 386 Krivičnog zakonika. Ovo delo se u našem zakonodavstvu naziva „agresivan rat", a u stavovima 1 i 2 propisani su oblici ostvarenja njegovog bića, pri čemu stav 1 propisuje osnovni, a stav 2 kvalifikovani oblik (videti: Stojanović, 2012a). Radnja osnovnog i težeg oblika predstavlja čin podstrekavanja, ili ponašanja slična njemu koja se, ipak, ne mogu podvesti pod krivičnopravni pojam podstrekavanja (osnovni oblik – pozivanje i podsticanje, a teži – izdavanje naređenja za vođenje agresivnog rata), koji je izjednačen sa izvršenjem krivičnog dela. Zakonodavac je ovako postupio zbog prirode agresorskog čina i oružanih sukoba, jer ukoliko bi se propisalo kažnjavanje lica koja neposredno vrše radnju krivičnog dela, inkriminacija bi izgubila smisao i mogućnost primene. Uostalom, suština ovog krivičnog dela i jeste kažnjavanje nalogodavaca, lica koja imaju vlast i faktičku moć da pokrenu agresivan rat, a ne pojedinaca koji učestvuju kao puki izvršioci njihove volje, a čiji je broj potencijalno ogroman. Objektivno gledano, narediti agresivan rat je društveno

opasnije ponašanje od učestvovanja pripadnika oružanih snaga u vojnim operacijama.

Načini ostvarenja bića osnovnog oblika širi su od podstrekavanja i ne bi se mogli podvesti pod njega. Reč je, pre svega, o pozivanju na vođenje agresivnog rata. Razlog je, ponovo, jasan – čin pozivanja na agresiju dovoljno je društveno opasan da se može kazniti kao samostalno krivično delo, bez obzira da li je poziv upućen zatvorenom krugu lica (što je uslov za postojanje podstrekavanja) ili je ostvaren ka neodređenom i otvorenom krugu subjekata.

Posmatrajući navedene izvore prava, čini nam se nespornim da se kiber napadi ne mogu podvesti pod pojam agresije definisan Rezolucijom Generalne Skupštine UN. Svaki od navedenih oblika podrazumeva oružani napad, to jest upotrebu fizičke sile prema drugoj državi. Takođe, jasno je da Rezolucija kao aktera agresije vidi isključivo državu, a ne i nedržavne aktere (ovo je odavno zamerano tekstu rezolucije), poput pobunjeničkih grupa ili međunarodnih organizacija (mada bi širim tumačenjem akt međunarodne organizacije mogao da se okarakteriše kao agresija od strane više država prema jednoj državi), kao i drugih grupa ili individua. Posmatrajući osobine kiber ratovanja, pak, vidimo da su konkretni izvršioci uglavnom nevezani za konkretnu državu, ili je tu vezu gotovo nemoguće dokazati.

U literaturi se, međutim, uveliko raspravlja o ovom problemu i mogućim pravnim solucijama. NATO koordinacioni centar za kiber odbranu i podršku (NATO Cooperative Cyber Defense Centre of Excellence – CCDCOE) objavio je članak na ovu temu u novembru 2008. godine, pod nazivom „Kiber napadi na Gruziju: izvučene pravne pouke". U njemu autori razmatraju mogućnosti primene međunarodnog ratnog prava na kiber napade koji su se pojavili tokom rusko-gruzijskog konflikta avgusta 2008. godine. Autori navedenog članka smatraju da je u osnovi problema pitanje određenja sadržine i obima pojma kiber agresije. Šta bi pod ovim pojmom trebalo podrazumevati? Da li bi on obuhvatio sva, ili samo neka od sledećih tumačenja:

- kiber agresija podrazumeva napade na vladine, ključne državne ili civilne internet stranice ili mreže bez prateće vojne sile;
- kiber agresija se odnosi na napade usmerene protiv političkih neistomišljenika unutar države;
- kiber agresija označava napade na kritičnu infrastrukturu i mreže države;
- kiber agresija se može poistovetiti sa kiber špijunažom (Tikk et. al., 2008).

Da li neko od navedenih određenja adekvatno definiše čin kiber agresije, ili sva, ili pak nijedno? Da li definicija kiber agresije treba da sadrži odrednicu prema kojoj mora postojati odgovornost (protivničke) države za

izvršeni napad? Da li se pojmovi kiber agresije i kiber rata mogu sinonimno upotrebljavati?

Opšte uzev, korišćenje međunarodnog ratnog prava kao smernice za određivanje toga šta jeste, a šta nije kiber ratovanje skopčano je sa brojnim problemima. Prvo, međunarodno ratno pravo primenjuje se samo u slučaju otpočinjanja oružanog sukoba. Zatim, kiber incidenti koji odgovaraju oružanom napadu moraju biti takvi da ih je moguće pripisati konkretnoj državi. Dalje, postoji pitanje namere koja za cilj ima nanošenje štete. Da li je kiber incident izazvao povrede ili štete (monetarne, fizičke, ili virtuelne)? Zatim, u kom trenutku napadnuta država može legalno odgovoriti na kiber napad, itd.

Međunarodno ratno pravo sastavljeno je od dobro poznatih i prihvaćenih principa, ali primena tih principa na kiber napade očigledno predstavlja težak zadatak. Poteškoće nastaju iz činjenice da se međunarodno ratno pravo razvilo, većim delom, kao odgovor na „klasične" međudržavne ratove. Iz paradigme tradicionalnih oružanih sukoba relativno je jednostavno proceniti obim napada i otkriti identitet napadača. Međutim, tokom kiber napada, napadnutoj državi je teško da proceni obim napada, kao i da zaključi ko je za njega odgovoran (Putnik, 2009).

Drugi sporazumi bi možda mogli da obezbede bolji okvir za uspostavljanje pojmovnog određenja kiber agresije.

Jedan teorijski pokušaj u tom pravcu učinjen je u članku Skota Šeklforda (Scott Shackleford) iz 2009. godine, pod nazivom „Od nuklearnog do internet rata: uspostavljanje analogije sa kiber napadima u međunarodnom pravu" (Shackleford, 2009).

Šeklford nabraja nekoliko ugovornih režima koji mogu poslužiti u konstruisanju međunarodnog kiber sporazuma: Sporazum o neširenju nuklearnog naoružanja, međunarodno kosmičko pravo, Sistem antarktičke povelje, Konvencija Ujedinjenih nacija o pravu mora i ugovori o uzajamnoj pravnoj pomoći.

Ugovori o neširenju nuklearnog naoružanja. Ugovori o neširenju nuklearnog naoružanja nastali su sa ciljem da se širenje proizvodnje nuklearnog oružja spreči već u početnim fazama, tj. na stupnju nuklearnog reaktora. Nuklearni reaktori su poslednji put korišćeni u Iranu, nakon što je on odbio da u potpunosti sarađuje sa Međunarodnom agencijom za atomsku energiju (International Atomic Energy Agency – IAEA).

Ovi ugovori su delotvorni jer su komponente koje učestvuju u stvaranju nuklearnog uređaja strogo zabranjene i pažljivo nadgledane od strane IAEA, različitih vlada i njihovih agencija za praćenje aktivnosti širenja nuklearnog naoružanja.

Kada su u pitanju sredstva kiber ratovanja, stvari stoje drugačije. Celokupna tehnika koja je napadaču potrebna za izvršenje napada naveliko se

distribuira i može se nabaviti po veoma niskoj ceni. Zbog toga se sporazumi o nešrenju naoružanja ne mogu primeniti za sprečavanje država da razvijaju sposobnosti kiber ratovanja.

Zvaničnici SAD-a i Ruske Federacije skloni su preterivanju u izjavama po pitanju razmera i proporcionalnosti odgovora na kiber napade velikih razmera (Carr, 2010: 33)[2], a pored toga, nijedna strana nema jasnu politiku kojom bi se ta pitanja regulisala.

S pravom se može postaviti pitanje da li kiber napad može da se podigne na nivo nuklearnog napada. Sam po sebi, ne može, ali ako je dovoljno velikih razmera da uništava glavne mreže i stoga sistematski uništava bezbednosnih sistema nuklearnih elektrana, mogao bi imati razorne posledice, uključujući i gubitke života.[3]

Međunarodno kosmičko pravo i Sistem antarktičke povelje. Kiber prostor se često upoređuje sa svemirom pošto su i jedan i drugi neograničeni i neregulisani zakonom. Međunarodno kosmičko pravo ne zabranjuje korišćenje svemira kao platforme za testiranje oružja, osim nuklearnog. Upotreba ove vrste naoružanja zabranjena je međunarodnim ugovorom, kao što je zabranjeno i odlaganje takvog oružja na neko planetarno telo. Međutim, pravni vakuum između ove dve kategorije naoružanja još uvek nije regulisan.

Jedna od prepreka u primeni ove analogije na kiber ratovanje ogleda se u tome da mali broj nacija ima mogućnost, ili može očekivati da će biti u mogućnosti, da ratuje u svemiru. Sa druge strane, preko 120 nacija danas ima mogućnost vođenja rata u kiber prostoru.

Drugi problem predstavlja razlika u potencijalu pretnje kiber napada u poređenju sa lansiranjem nuklearnog oružja iz svemira. Nema takvog kiber napada koji može prouzrokovati štetu ekvivalentnu šteti izazvanoj nekim nuklearnim oružjem iako se, teoretski, upotreba ogromnog botneta koji uključuje milione zombi računara može, bar približno, smatrati internet ekvivalentom nuklearnog napada.

Alternativa zabrani određenog tipa oružja u nekom području jeste zabrana svakog oružja u datom području, po principu Antarktičke povelje iz 1959. godine. Prema ovom ugovornom režimu, Antarktik je van doma-

[2] Na primer: „Rusija zadržava pravo da koristi nuklearno oružje protiv sredstava i sila informacionog ratovanja a onda i protiv same zemlje agresora" (pukovnik V. I. Tsimbal, 1995); kiber ratovanje je „bliski susret treće vrste iza širenja naoružanja za masovno uništenje i upotrebe nuklearnog, biološkog i hemijskog oružja od strane terorista" (bivši direktor CIA-e John Deutch, 1996).

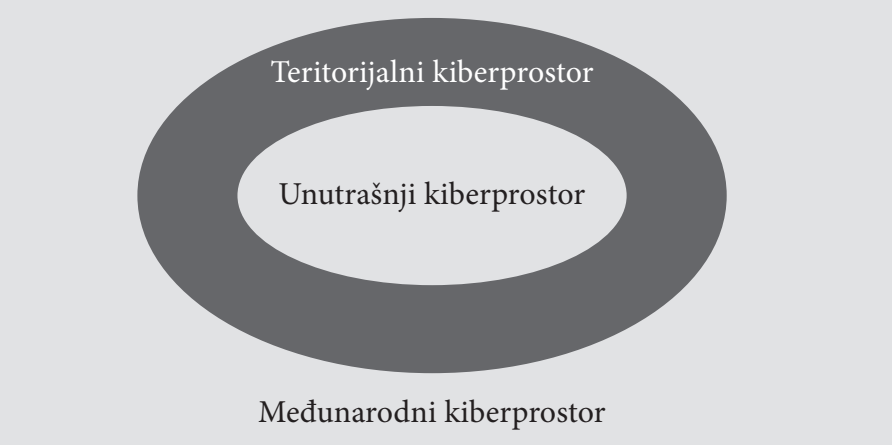
[3] Setimo se virusa *Stuxnet* koji je septembra 2010. godine zarazio računare iranske nuklearne elektrane Bušer. Virus je bio kreiran tako da je mogao da zaustavi rad elektrane i dovede do havarije velikih razmera.

šaja svih oblika vojnih aktivnosti od strane bilo koje nacije i koristi se samo u mirovne, prevashodno naučno-istraživačke svrhe.

Ipak, čini se da ni ovakav ugovorni režim ne može poslužiti kao model za regulisanje kiber ratovanja. Jedan od razloga jeste nemogućnost da se napravi razlika između informatičkog koda koji se koristi u mirovne svrhe i onog koji se koristi u maliciozne.

Drugi problem je u tome što kiber prostor nema vidljivih granica niti ima pouzdanih načina da se one veštački povuku (Carr, 2010).[4]

Konvencija Ujedinjenih nacija o pravu mora (The United Nations Convention on the Law of the Sea – UNCLOS). Pravo mora i međunarodnih voda određeno je Konvencijom Ujedinjenih nacija o pravu mora. U pitanju je sporazum koji je usvojila Treća konferencija Ujedinjenih nacija o pravu mora (UNCLOS III) i koji je stupio na snagu 1994. godine.[5] Mora i okeani su, kao i svemir, po svom prostranstvu slični kiber prostoru. Slikovito bi se to moglo prikazati na sledeći način:



Shema br. 1: Unutrašnji, teritorijalni i međunarodni kiber prostor

[4] Jedan od skorašnjih napada na Internet stranice vlada SAD i Južne Koreje potekao je sa servera na tlu SAD preko VPN konekcije sa serverom u Velikoj Britaniji. Server u Britaniji je bio kontrolisan od strane komandnih i kontrolnih servera stacioniranih na teritoriji drugih država sa kojih je napad i započet. Bezbednosna služba Južne Koreje, pak, bila je ubeđena da je napad iniciran iz Severne Koreje. Tu pogrešnu procenu podržala je celokupna štampa i jedan američki kongresmen. Kongresmen je zatražio od vojske SAD da uzvrati kiber napad Severnoj Koreji. Da je to učinjeno, odnosi u međunarodnoj zajednici bi danas verovatno bili mnogo zaoštreniji.

[5] Prva konferencija UN-a o pravu mora (UNCLOS I) održana je 1958. u Ženevi. UNCLOS I rezultirala je usvajanjem četiri konvencija. Iako je UNCLOS I smatrana uspešnom, ostavila je nekoliko bitnih pitanja nerešenim, pre svega širinu teritorijalnog mora. Druga konferencija UN-a o pravu mora (UNCLOS II) održana je 1960. Međutim, ova konferencija nije rezultirala niti jednim novim sporazumom. Opšte govoreći, zemlje u razvoju i zemlje trećeg sveta učestvovale su na ovoj konferenciji

Prema ovoj analogiji, unutrašnji kiber prostor bio bi područje u kome nacionalna država ima potpuni suverenitet. Pod teritorijalnim kiber prostorom podrazumevao bi se deo nacionalnog kiber prostora u koji se dopušta neograničen pristup. Međunarodni kiber prostor teže je definisati, ali bi se, prema analogiji sa UNCLOS-om, odnosio na ona područja koja nisu pod suverenitetom niti jedne nacije.

Međutim, problemi vezani za regulativu prava mora su se pojavili još tokom Treće konferencije, kada su SAD, Nemačka i Ujedinjeno Kraljevstvo osujetili pokušaje Ujedinjenih nacija da se uspostave standardi transfera tehnologije. Čini se da tehnologija stalno nudi izazove sporazumnom režimu, koji pokušava da reguliše njen razvoj – nagoveštavajući na taj način pravne poteškoće koje nastaju kao rezultat kiber ratovanja. Drugim rečima, ako transfer tehnologije ne bude regulisan Konvencijom Ujedinjenih nacija o pravu mora, neće biti nimalo lako napraviti sporazum o regulisanju problema kiber ratovanja prema njegovom modelu.

Sporazum o uzajamnoj pravnoj saradnji (Mutual legal assistance treaty – MLAT). Sporazumi o uzajamnoj pravnoj saradnji mogu poslužiti kao univerzalni model za sporazume o bilateralnoj saradnji među državama, kao što su udruženi napori za sprovođenje zakona, sporazumi o ekstradiciji itd. Izgleda da SAD trenutno zagovaraju ovaj pristup, dok Ruska Federacija preferira analogiju po kojoj se kiber prostor tretira kao oružje za masovno uništenje, i zabranu njegove upotrebe odgovarajućim sporazumnim režimom.

Rusi smatraju da problem kiber ratovanja treba da se reguliše prema modelu Sporazuma o hemijskom naoružanju, ili bilo kom drugom sporazumu o kontroli naoružanja, dok SAD zagovaraju sprovođenje međunarodnog prava u oblasti kiber kriminala i bolju saradnju među državama na tom polju. Mnogi kiber kriminalci uključeni su u kiber konflikte kao nedržavni akteri, haktivisti (populacija visokoobrazovanih, patriotski nastrojenih hakera koji se rado bore u ime svoje države na području kiber prostora), tako da bi ova strategija rezultirala dvostrukom dobiti – obezbeđivanjem interneta od kiber kriminala i kiber ratovanja.

U moskovskom žurnalu Vojna misao, pod nazivom „Vojna politika Ruske Federacije u oblasti Međunarodne informacione bezbednosti:

---

samo kao saveznici SAD-a i SSSR-a, bez značajnijeg vlastitog doprinosa. Treća konferencija UN o pravu mora sazvana je 1973. godine u Njujorku, i trajala je do 1982, uz učešće 160 država. Kako bi se sprečio pokušaj da određene grupe država dominiraju pregovorima, konferencija je donosila odluke konsenzusom, izbegavajući primenu sistema većine. Rezultat UNCLOS III je Konvencija o pravu mora. Konvencija je uvela novi institut u međunarodno pravo mora – isključivi državni pojas, koji je već postojao u običajnom međunarodnom pravu, ali nije bio do kraja definisan. Konvencijom je predviđeno osnivanje Međunarodne vlasti za morsko dno, ali i Međunarodnog suda za pravo mora.

regionalni aspekt", objavljen je jedan argument Rusije protiv stava SAD: „Međunarodni pravni akti koji regulišu odnose koji se javljaju u procesu suzbijanja kiber kriminala i kiber terorizma ne smeju da sadrže norme koje narušavaju tako bezuslovne principe međunarodnog prava kao što su neuplitanje u unutrašnje poslove drugih država i suverenitet potonjih. Štaviše, politički motivisani kiber napadi izvršeni po nalogu vladajućih struktura mogu se okvalifikovati kao vojni zločin sa svim predviđenim procedurama istrage i krivičnog gonjenja zločinaca. Pored toga, vojni kiber napadi mogu se posmatrati i kao predmet međunarodnog javnog prava. U ovom slučaju, trebalo bi da govorimo o uvođenju ograničenja na razvoj i upotrebu računara sa namerom da se izazovu negativni uticaji na entitete kiber prostora drugih država.

U svakom slučaju, vojna politika u oblasti međunarodne informacione bezbednosti, gde ova uključuje suprotstavljanje kiber terorizmu i kiber kriminalu, trebalo bi da bude usmerena ka uvođenju međunarodnih pravnih mehanizama koji bi omogućili sprečavanje nekontrolisane i tajne upotrebe kiber oružja od strane potencijalnih agresora protiv Ruske Federacije i njenih geopolitičkih saveznika." (Военная политика Российской Федерации в областимеждународной информационной безопасности: региональный аспект, 2007)

Rusija je formulisala svoju politiku u ovoj oblasti pre 2007. godine, i ona se do danas nije promenila. Dva su razloga uticala na njenu poziciju. Prvi razlog svakako je zaštita nacionalnog suvereniteta. Sa druge strane, ne bi trebalo prenebregnuti korist koju Ruska Federacija ima od nedržavnih aktera u kiber konfliktima. Dosadašnje iskustvo pokazalo je da haktivisti predstavljaju strateško sredstvo u ruskom kiber arsenalu.

Zanimljivo je da se Šeklford uopšte ne bavi međunarodnim ratnim pravom u pomenutom eseju, što samo pokazuje koliko se razlikuju mišljenja pravnih stručnjaka koji su fokusirani na ovu oblast. Umesto toga, on potcrtava tezu da je najbolji način za smanjenje obima kiber ratovanja formulisanje međunarodnog sporazuma koji bi se bavio isključivo kiber napadima pod pokroviteljstvom država u međunarodnom pravu. Ovakav sporazum bi podrazumevao formiranje stalnog tela za reagovanje u hitnim slučajevima, koje bi bilo slično već predloženom globalnom računarskom timu za reagovanje u kriznim situacijama. Šeklford smatra da bi SAD trebalo da odbace svoje protivljenje takvom režimu sporazuma: „Bez jedne takve organizacije, međunarodna zajednica će posrtati od slučaja do slučaja, brinući se da će narednog puta slučaj Estonije biti samo korak koji vodi ka mrežnom ratu v. 2.0. Kada kiber ratovanje dostigne stupanj nuklearnog rata, biće neophodan novi i drugačiji režim, koji će u sebi sadržati elemente postojećeg međunarodnog prava, osobito međunarodnog humanitarnog prava, jer će, u suprotnom, nacije biti izložene riziku od sistematskih

oštećenja infrastrukture, koja mogu ne samo onesposobiti društva, već vrlo verovatno i do temelja uzdrmati informaciono doba“ (Shackleford, 2009).

Zaključak

Nakon relativno iscrpnog prikaza teorijskih i doktrinarnih stavova i nedoumica, a u vezi sa mogućnostima primene odredaba međunarodnih ugovornih režima i drugih akata (poput Rezolucije UN), mislimo da se argumentovano može doneti zaključak o neadekvatnosti postojećeg međunarodnopravnog okvira za suprotstavljanje fenomenu kiber napada, ukoliko ove kvalifikujemo kao sredstvo ili način vršenja agresivnih radnji protiv određene države.

Savremeno doba donelo je informatizaciju mnogih važnih procesa, uključujući i one podvedene pod kritičnu infrastrukturu. Globalno povezane ekonomije zavisne su od informacionih tehnologija, i ugrožavanje informaciono regulisanih ili nadgledanih procesa potencijalno dovodi do tektonskih poremećaja u životima ljudi, funkcionisanju javnih službi, uživanju opštih dobara i privrednom razvoju.

Opasnosti koje donosi zloupotreba informacionih tehnologija u umreženom svetu prevazilaze okvire u kojima se razmišljalo u kontekstu konvencionalnih vojnih doktrina. Iako je upitno da li je do sada bilo slučajeva kiber napada koji bi poprimili odlike ratovanja, nedvosmisleno je jasno da mogućnosti za njihovo ostvarenje vise nad savremenim društvima poput Damoklovog mača.

U tom smislu, treba se zapitati da li pojedinim državama odgovara postojeće stanje zato što veruju da će pre biti akteri nego žrtve kiber napada. Pokušava li neko da se unapred zaštiti od odgovornosti, dozvoljavajući da kiber prostor ostane „prašuma“ u kojoj nema pravila i gde vlada samo zakon jačega? Da li je u pitanju nameran eksperiment sa nesagledivim posledicama, ili je međunarodna zajednica nesposobna da dođe do jedinstvenog i prihvatljivog rešenja, orijentisanog ka odricanju od zlonamernog korišćenja sveta ogromnih mogućnosti koje nudi nova dimenzija društvenog života? Bojimo se da ne zvuči realno opcija po kojoj dobronamerni akteri međunarodnih odnosa ne postižu saglasnost iz doktrinarnih, teorijskih ili pravnih razloga. Kiber napad može da zada jači i odsudniji udarac nego mnoga konvencionalna oružja, a mogućnosti manipulacije u umreženom svetu, uključujući psihološko ratovanje, dodatno „otvaraju oči“ o ulozi kakvu u budućim sukobima može imati kiber svet.

Otvoreno more i svemir regulisani su odredbama međunarodnog prava, ali smo svedoci činjenice da onaj koji nema faktičku mogućnost da ih koristi, nema koristi od proklamovanih prava. Ovde vidimo i da međunarodno pravo samo po sebi ne može da spreči zloupotrebe moćnih aktera

međunarodnih odnosa. Uostalom, to pokazuju i vojne intervencije vršene poslednjih godina dvadesetog veka, a protivno međunarodnom pravu. U ovom smislu gledano, kiber napade ne može da spreči nikakva odredba. Ipak, regulisanost oblasti omogućila bi nam da barem saznamo na čijoj je strani međunarodno pravo.

Literatura

Военная политика Российской Федерации в областимеждународной информационной безопасности: региональный аспект, *Военная мысль*, Но. 2/2007, Москва.

Vučinić, Z. (2013). *Međunarodno javno pravo*. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti, Čigoja štampa.

Carr, J. (2010). Inside Cyber Warfare, Sebastopol: O'Reilly Media.

Kreća, M. (2012). *Međunarodno javno pravo*. Beograd: Pravni fakultet, Centar za izdavaštvo i informisanje.

Markoff, J., A. Kramer (2009). U.S. and Russia Differ on a Treaty for Cyberspace, The New York Times. Tekst preuzet sa: http://www.nytimes.com/2009/06/28/world/28cyber.html

Mladenović, D. (2012). *Međunarodni aspekt sajber ratovanja*. Beograd: Medija centar „Odbrana".

Putnik, N. (2009). *Sajber prostor i bezbednosni izazovi*. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti.

Schogol, J. (2009). Official: No Options 'off the table' for U.S. Response to Cyber Attacks, Stars and Stripes. Tekst preuzet sa: http://www.stripes.com/news/official-no-options-off-the-table-for-u-s-response-to-cyber-attacks-1.91319

Shackleford, S. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law*, Vol 27, No 1, pp. 192–251.

Stojanović, Z. (2012). *Međunarodno krivično pravo*. 7. izdanje. Beograd: Pravna knjiga.

Stojanović, Z. (2012a). *Komentar Krivičnog zakonika*. 4. izmenjeno i dopunjeno izdanje. Beograd: Službeni glasnik.

Tikk, E. et. al. (2008). Cyber Attacks Against Georgia: Legal Lessons Identified, Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia. Tekst preuzet sa: http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

MLADEN MILOŠEVIĆ and NENAD PUTNIK

THE PROBLEM OF LEGAL (DE)REGULATION OF CYBERSPACE CONFLICTS

Summary

The article focuses on the analyses of the problem of legal regulation of cyberspace conflicts. The authors discuss about eventual legal qualifications of cyber warfare, underlining two main issues: first, the fact that cyber warfare cannot be considered as an act of the aggression according to the definition introduced by the UN Resolution; and, second, that it is widely considered that cyber warfare is more than an criminal act incriminated by national legislation. Having this in mind, the authors discuss about possibility of applying some of the established international treaty systems (International Law of War, International Space Law, Treaty on the Non-Proliferation of Nuclear Weapons, Antarctic Treaty System, United Nations Convention on the Law of the Sea, Mutual legal assistance treaties) as models for regulating cyberspace.

Key words: international humanitarian law and the law of war; contemporary warfare, cyber warfare