Pregledni rad
Primljen: 11. 7. 2017.
Revidirana verzija: 15. 11. 2017.
Prihvaćen: 6. 12. 2017.

UDK: 341.3
343.533::004
doi: 10.5937/nabepo22-14504

KIBER NAPADI I POVELJA UJEDINJENIH NACIJA

Katarina Jonev[1]

Sažetak: Kiber napadi predstavljaju nov, potencijalni oblik ratovanja i ne uklapaju se u tradicionalne međunarodne okvire koji regulišu upotrebu sile. Novijeg su datuma u odnosu na Povelju UN koja je stupila na snagu 1945. godine. Ipak, ni u 21. veku uticaj Ujedinjenih nacija, globalne međunarodne organizacije koja broji 193 države članice, nije opao, a države su i dalje glavni nosioci međunarodnog subjektiviteta. Da li je i kako moguće odgovoriti na nove bezbednosne izazove i da li Ujedinjene nacije imaju kapacitet da se suoče sa novim rizicima i pretnjama u kiber prostoru? U radu će biti predstavljena tumačenja pojedinih odredaba Povelje UN, pre svih člana 2(4) i člana 51, koja bi mogla biti upotrebljena u slučaju kiber napada.

Ključne reči: Ujedinjene nacije, kiber napadi, kiber bezbednost, Povelja UN, agresija.

Uvod

Kada su 1945. godine postavljeni temelji međunarodnih odnosa, nije se moglo ni pretpostaviti da će tehnologija dostići domete koje poznajemo danas. Sticanje znanja, dostupnost informacija, olakšana komunikacija i umreženost ekonomija, prednosti su koje nam je globalna mreža zvana Internet omogućila.

1 Doktorand na Fakultetu bezbednosti Univerziteta u Beogradu, jonev.katarina@gmail.com

Internet je, pored značajnih prednosti, doneo i bezbednosne pretnje, kako po pojedinca tako i po interese nacionalnih država. Naše sve veće vezivanje za mrežu nije praćeno naporima da se ona sačuva bezbednom. Savremeni informacioni sistemi su doneli mnoge pogodnosti kada je u pitanju poslovanje, zatim automatizaciju i lakše proizvodne procese u oblasti industrije, saobraćaja i drugih vidova kritične infrastrukture. Internet i IKT tehnologije postali su vitalni deo nacionalne infrastrukture i ključni pokretači društveno-ekonomskog rasta i razvoja država[2]. Od trenutka nastanka, nacionalne vlade i kompanije prihvatile su Internet kao potencijal za generisanje prihoda. U nekim zemljama Internet čini i do 8% bruto domaćeg proizvoda (BDP)[3].

Međutim, pored svih prednosti koje sa sobom nosi tehnološki napredak, postoje i mnoge opasnosti u vidu kiber rizika i pretnji. Internet, zajedno sa informacionom i komunikacionom tehnologijom koja ga podupire, postao je kritičan nacionalni resurs za države. Kiber prostor pruža nove mogućnosti, ali predstavlja i nove izazove za države, podjednako na unutrašnjem i spoljnopolitičkom planu, uključujući i nacionalnu odbranu. Globalno razumevanje fenomena kiber prostora treba da obuhvati političke, ekonomske, pravne, društvene i tehnološke aspekte koji će omogućiti razvoj operativnih mera zaštite svih učesnika globalne zajednice – država, međunarodnih organizacija, pojedinca, privatnog i javnog sektora. Kiber bezbednost predstavlja kamen temeljac informacionog društva. Pored pitanja izazova u pogledu sigurnosti i poverenja koji se odnose na nacionalnu bezbednost i zaštitu kritične infrastrukture i odbrane, kiber bezbednost paralelno treba da odgovori na bezbednosne zahteve građana.

Kiber prostor ujedno predstavlja i najsavremenije pitanje koje se tiče međunarodnog prava, međunarodnih odnosa i bezbednosti.

Ne bez osnova, preovlađuje gledište da će i dvadeset prvi vek biti opterećen oružanim sukobima, sa različitim povodima i ciljevima, većeg ili manjeg intenziteta. Sve veći broj država ima tendenciju da posmatra kiber napade kao oružje, što se dokazuje i kroz usvajanje kiber strategija na nacionalnim nivoima proteklih godina. Broj država koje su donele svoje kiber doktrine raste. Godine 2011. bivši predsednik SAD, najveće sile na svetu, Barak Obama je uz problem nuklearnog razoružanja i terorizma proglasio kiber pretnje za najbitnije s gledišta bezbednosnih nacionalnih interesa SAD, dok je digitalna infrastruktura priznata za glavni „strateški resurs". Sjedinjene Države su kiber supersila bez premca.

2 A. Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn, 2012, str. 18.
3 D. Dean et al., *The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy*, BCG Perspectives.

Međutim, poslednjih godina beleži se rast „kiber sila" koje se pojavljuju kao potencijalni rivali SAD[4]. Nacionalna odbrambena strategija SAD jasno je definisala kiber prostor kao novo područje vođenja vojnih operacija[5] u kojem se kiber oružje smatra podjednako važnim kao i konvencionalno i nuklearno oružje[6]. Ministarstvo odbrane SAD donelo je 2015. godine Strategiju nacionalne bezbednosti, kojom je naglašeno da se moraju ojačati kapaciteti SAD da se zaštite i osiguraju od kiber napada kao i neophodnost saradnje sa državama.[7] Kada je opravdano, Sjedinjene Države će reagovati na neprijateljske akte u kiber prostoru kao što bi reagovali na bilo koju drugu pretnju[8]. Bivši predsednik Barak Obama je identifikovao i dva najveća suparnika Sjedinjenim Državama u kiber prostoru – Narodnu republiku Kinu i Rusku Federaciju – nazvavši ih „agresivnim" igračima u svetu kiber špijunaže i upozorio da će ove dve države nastaviti da na nelegalan način kradu industrijske i tehnološke tajne Sjedinjenih Američkih Država[9]. Pored toga, postoji niz nedržavnih aktera (pre svega terorističke grupe) koji prete da steknu sredstva da pokrenu kiber napade.

Definisanje pitanja politike nacionalne bezbednosti i odbrane jedne države uslovljeno je geopolitičkom stvarnošću. Međutim, uprkos činjenici da je kiber bezbednost u vrhu liste najvećih pretnji po bezbednost u agendama nacionalnih država, na međunarodnom nivou još uvek ne postoji konvencija, ugovor ili deklaracija koja bi definisala problematiku kiber bezbednosti. Kiber operacije imaju potencijal da proizvedu društveni i ekonomski poremećaj bez izazivanja fizičke štete koju obično povezujemo sa tradicionalnim oružanim sukobima. Takođe su inherentno prekogranična, čime direktno osporavaju koncept teritorijalnosti. Ofanzivne napade mogu pokrenuti pojedinci ili grupe, mogu ih sponzorisani vlade država i nedržavni subjekti.

Ujedinjene nacije su najveća međunarodna organizacija, koja broji 193 države članice. I u 21. veku uticaj Ujedinjenih nacija, kao globalne međunarodne organizacije, nije opao, a države su i dalje glavni nosioci međunarodnog subjektiviteta. Države sve više postaju svesne da se u fazi povećanja opasnosti

4http://www.telegraph.co.uk/news/uknews/defence/8369520/Military-Balance-report-countries-creating-new-cyber-warfare-organisations.html /, pregledano 3. 4. 2017.
5 K. B. Alexander, Warfighting in Cyberspace, *Joint Forces Quarterly*, 31. jul 2007,
http://www.military.com/forums/0,15240,143898,00.htm.
6 K. B. Alexander, Warfighting in Cyberspace, *Joint Forces Quarterly*,
http://www.military.com/forums/0,15240,143898,00.htm/, pregledano 23. 8. 2017.
7 https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, pregledano 9. 9. 2017.
8 Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011, str. 2, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.
9 http://m.guardian.co.uk/technology/2013/feb/21/white-house-cyber-threat-russia-china/, pregledano 5. 2. 2017.

od ugrožavanja njihovog kiber prostora moraju naći odgovori na nove bezbednosne pretnje, ne samo kroz nacionalne strategije već i na međudržavnom nivou. Radna grupa za borbu protiv terorizma (*Counter-terrorist implementation task force*) pri Ujedinjenim nacijama, održala je mnogobrojne sastanke u Nemačkoj i SAD radi preduzimanja mera protiv sve veće pojave kiber napada.[10] Suočene kako sa tradicionalnim tako i netradicionalnim bezbednosnim izazovima, države su, kada deluju same, loše opremljene, zbog čega postoji potreba za zajedničkom strategijom i normama na međunarodnom nivou. Ujedinjene nacije su postavile kamen temeljac granama međunarodnog prava nakon Drugog svetskog rata Stoga im treba dati mogućnost da i u oblasti kiber bezbednosti daju svoj doprinos.

Kiber aktivnost može biti legitimna vojna aktivnost[11], ali još uvek ne postoji globalni dogovor o pravilima koja važe. Dok su pioniri u akademskim krugovima predložili kompleksnu listu indikativnih kriterijuma za razlikovanje oružane sile i ekonomske ili političke prinude u kiber domenu[12], drugi su istakli slabosti u ovim kriterijumima koji ilustruju, pre nego uklanjaju, nedostatak jasnoće u ovoj oblasti.[13] Međunarodna zajednica mora da prepozna ovaj izazov, nastajanje i strukturu i da kreira, u skladu sa situacijom, međunarodni odgovor uzimajući u obzir da kiber napadi nemaju geoprostorna ograničenja tradicionalne agresije.

Postavlja se pitanje: da li postojeći mehanizmi Organizacije ujedinjenih nacija mogu da odgovore na nove rizike i pretnje koje kiber napadi izazivaju?

1. Povelja Ujedinjenih nacija

Nagli porast upotrebe informaciono-komunikacione tehnologije u mnogobrojnim sferama, a pre svega u vojnoj oblasti, iznedrio je nove pretnje po bezbednost država. Efikasnost primene kiber napada zauzima sve značajnije mesto, kao i sama integracija vojnih doktrina koje definišu kiber bezbednost kao jedan od nacionalnih odbrambenih prioriteta. Kiber napadi pružaju ogromne mogućnosti, kako u vreme oružanih sukoba tako i u mirnodopsko vreme. U kiber prostoru ne postoje geografska ograničenja, što potencijalnim počiniocima ide u korist i pruža mogućnost delovanja sa bilo kog dela planete.

10 http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf.

11 A. Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 2012, str. 17.

12 *Ibid*, str. 17.

13 M. Roscini, World Wide Warfare – Jus ad bellum and the Use of Cyber Force, *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, str. 104.

Velika integracija računarskih mreža otvara i mogućnost da se iskoriste ranjivosti sistema.

Uprkos gotovo svakodnevnim kiber napadima različitih razmera, efekata i posledica, do danas nije zabeležen niti jedan slučaj kiber incidenta koji bi doveo do rasprave pred institucijama Ujedinjenih nacija, niti pred Savetom bezbednosti, kome su tvorci Povelje dodelili ulogu organa kome je poverena zaštita međunarodnog mira i bezbednosti. Države same razmatraju i traže smernice u okviru svojih nacionalnih zakona i strategija, kao i postojećih pristupa ovom delu međunarodnog prava, kako bi ocenile šta se smatra dozvoljenom aktivnošću u kiber prostoru i kako treba odgovarati na incidente.

Države sve više postaju svesne da se u fazi povećanja opasnosti od ugrožavanja njihovog kiber prostora moraju naći odgovori na nove bezbednosne pretnje, ne samo kroz nacionalne strategije već i na međudržavnom nivou. Suočene kako sa tradicionalnim tako i sa netradicionalnim bezbednosnim izazovima, države su, kada deluju same, loše opremljene zbog čega postoji potreba za zajedničkom strategijom i normama na međunarodnom nivou. Dok se države ne usaglase oko Konvencije o kiber bezbednosti, potrebno je ukazati da UN nisu apsolutno nemoćne kada su u pitanju kiber napadi i da se određeni postojeći mehanizmi mogu primeniti i kada je ovakva vrsta opasnosti u pitanju.

Povelja UN (1945) jeste multilateralni sporazum sa dvostrukom funkcijom: sadrži pravila o funkcionisanju i radu Organizacije i pravila o ponašanju država, odnosno njihovim pravima i obavezama. Skoro sve postojeće države ujedno su i članice OUN i time su dužne da se pridržavaju odredaba Povelje UN.

Član 1 Povelje u prvoj tački određuje svrhu Organizacije ujedinjenih nacija, a to je „održavanje međunarodnog mira i bezbednosti". Zabranjuje se pribegavanju bilo kojoj meri koja bi mogla da isprovocira vojni napad i dovede do izbijanja međunarodnog oružanog sukoba. Da bi kiber sukob imao prirodu ratovanja, neophodno je da ima karakter organizovane agresije jednog subjekta međunarodnog prava na drugi. To u načelu podrazumeva agresiju jedne države na drugu. Ne može se isključiti ni mogućnost upotrebe sile i od strane nedržavnih aktera, koja predstavlja pretnju međunarodnom miru i bezbednosti i zahteva da Savet bezbednosti razmotri, preduzme ili odobri mere kolektivne prisile[14] kao odgovor.

S obzirom na napredak savremene ratne tehnike, pravila ratovanja su morala da se prilagode. Digitalno doba je uvelo novu vrstu oružja – kiber oružje[15].

14 N. Melzer, *Cyberwarfare and International Law*, 2011, UNIDIR, str. 6, dostupno na: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

15 Kiber oružje je jedan od pojmova za koje međunarodna zajednica još uvek nije formirala definiciju. Zlonamerni kod ne može se sam po sebi smatrati „oružjem" samo po svojim svojstvima već i po ishodu za koji je dizajniran da proizvede. Drugim rečima, samo ako se utvrdi da zlonamerni kod poseduje kapacitet ofanzivnog naoružanja, i postoji namera da se upotrebi kao ofanzivan, može se smatrati „kiber – oružjem". M. Schmitt, Cy-

Dodatni protokol I iz 1977. godine jasno je u članu 36 propisao da nova oružja takođe potpadaju pod međunarodnu regulativu, čak i kada nisu eksplicitno definisana[16], čime se otvara mogućnost da se sankcionišu kiber napadi i korišćenje destruktivnih malvera (virusa, crva, trojanaca).

Tačan obim, sadržaj i domet Povelje UN predmet je stalnog tumačenja od strane država već decenijama. Međutim, same karakteristike kiber prostora svojom prirodom i specifičnostima zahtevaju posebna tumačenja u skladu s Poveljom, posebno s principima navedenim u članu 2, koji se odnosi na teritorijalnost, suverenitet država i nemešanja u unutrašnje stvari drugih država.

Jedan od osnovnih problema u vezi sa primenom Povelje UN jeste teškoća utvrđivanja i kategorizacije kiber incidenata[17]. Pretnje u kiber prostoru ne potiču samo od država već i od nedržavnih entiteta poput terorističkih grupa, ali i od pojedinaca i grupa koje zahvaljujući arhitekturi kiber prostora mogu sprovesti napad sa nepoznate lokacije, sačuvati svoj identitet i naneti štetu. Oni ne moraju nužno da izvrše napad u ime države, već im cilj može biti nelegalno sticanje finansijske dobiti, dolazak u posed industrijskih i državnih tajni posredstvom kiber špijunaže, slanje političkih, verskih i ideoloških poruka. Ujedno, nije uvek moguće utvrditi da li je napad bio izazvan namerno ili slučajno, odnosno da li su ga prouzrokovali ljudi, ili je rezultat kompjuterske greške ili rutinskog kvara u sistemu.

Kiber operacije nisu kinetičke po svojoj prirodi i upotreba kiber oružja ne može se smatrati „oružjem" u tradicionalnom smislu. Za razliku od upotrebe tradicionalne oružane sile, kiber napadi ne mogu dovesti do okupacije zemlje odnosno zauzimanja teritorije suverene države ili javnih dobra koje pripadaju državi kao što su gradovi, vojni objekti, industrijska postrojenja, aerodromi, naftna nalazišta i kritične infrastrukture. Ipak, ono što je specifično kod kiber napada jeste da imaju potencijal da ostvare efekat koje su vojske imale upotrebljavajući bombe i rakete, ali ovog puta praktično bez kolateralne štete. U meri u kojoj dovedu do povrede ili smrti lica, oštećenja ili uništenja imovine, kiber napadi zadovoljavaju kriterijum oružanog konflikta.

ber Operations and the Jus in Bello: Key Issues, *87 International Law Studies*, Naval War College, 2011; Charles Dunlap, Perspective for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly, Spring 2011, 81–99, 85.

16 Član 36: „U proučavanju, usavršavanju, nabavljanju, ili prihvatanju novog oružja, sredstva ili metoda ratovanja visoka strana ugovornica obavezna je da utvrdi da li će njegova primena u nekim ili svim uslovima da bude zabranjena ovim protokolom ili nekim drugim pravilom međunarodnog prava koji se primenjuje na visoku stranu ugovornicu."

17 Definicije na globalnom nivou kao što su kiber kriminal, kiber terorizam, kiber napad, kiber bezbednost i kiber rat još uvek su u procesu nastanka.

U okviru sistema Ujedinjenih nacija, države članice „poveravaju Savetu bezbednosti primarnu odgovornost za održavanje međunarodnog mira i bezbednosti“[18].

S obzirom da kiber operacije mogu negativno uticati na međunarodne odnose država, ne može biti nikakve sumnje da se uloga Saveta odnosi i na održavanje međunarodnog mira i bezbednosti u kiber prostoru. Kada Savet bezbednosti utvrdi postojanje „kršenja mira“, „akt agresije“ ili, najčešće, „pretnju miru“, može da preduzme mere potrebne da se održe ili povrate međunarodni mir i bezbednost[19]. Takve mere mogu biti ograničene na davanje preporuka[20] ili poziv zainteresovanim stranama da se povinuju privremenim merama[21], ali ujedno mogu uključivati oružanu i neoružanu akciju[22]. Povelja UN navodi kao primere neoružane akcije „kompletan ili delimičan prekid (...) telegrafskih, radio i drugih sredstava komunikacije“[23] , čime se obezbeđuje osnova za UN za uvođenje „kiber blokade“.

Ukoliko je Savet došao do zaključka da predložene mere iz člana 41 Povelje ne odgovaraju, ili se one pokažu kao neadekvatne, „može preduzeti akciju vazduhoplovnim, pomorskim ili suvozemnim snagama koje mogu biti potrebne da se održi ili povrati međunarodni mir i bezbednost“[24]. Pravnom metodom analize i tumačenja člana 42 Povelje UN moguće je utvrditi da se oružana prinuda može izvrši samo „vazdušnim, pomorskim, ili suvozemnim snagama“[25]. Postavlja se pitanje da li je član 42 samim nabrajanjem definisao prostor delovanja i time isključio kiber prostor iz svog delokruga delovanja. Ovo može proizaći iz teleološkog ili ciljnog tumačenja pravne norme koja je u pitanju. Član 42 Povelje UN ne može da se tumači kao lišavanje Saveta bezbednost mogućnosti da odobri upotrebu oružane sile u kiber prostoru[26]. Nastavlja se debata i postavlja pitanje o načinu na koji države u slučaju kiber napada mogu da zaprete – „ekonomskim sankcijama, diplomatskim protestom, preventivnim napadom ili čak vojnom intervencijom“[27]. Ovo pitanje je još aktuelnije od trenutka kada je bivši predsednik Sjedinjenih Američkih Država Barak Obama izjavio da jednu od najvećih opasnosti po SAD predstavljaju

18 Povelja UN predviđa da Savet Bezbednosti održava mir i bezbednost: 1) putem mirnog rešavanja sporova i 2) preduzimanjem preventivnih i prinudnih mera.
19 Poglavlje VII Povelje UN.
20 Član 39 Povelje UN.
21 Član 40 Povelje UN.
22 Čl. 41 i 42 Povelje UN.
23 Član 41 Povelje UN
24 Član 42 Povelje UN.
25 *Ibid*.
26 Nils Melzer, *Cyberwarfare and International Law*, 2011.
27 Makoff, Sanger and Shanker In Digital Combat, U.S. Finds No Easy Detteren, http://www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=all&_r=0/, pregledano 10. 7. 2016.

upravo kiber napadi i potencijalna upotreba Interneta u terorističke svrhe u vidu kiber terorizma.

Povelja može da postigne svoju sveobuhvatnu svrhu održavanja međunarodnog mira i bezbednosti i „da bi se sačuvale buduće generacije od zla rata"[28] ako zabranjuje pribegavanje bilo kojoj prisilnoj meri koja bi mogla da isprovocira bilo kakvu vrstu oružanog kontraudara i, na kraju, izbijanje međunarodnog oružanog sukoba[29].

Dok su kiber napadi do sada možda izgledali relativno pitomo u odnosu na uništenje koje mogu da izazovu tradicionalni instrumenti rata, stručnjaci se uglavnom slažu u proceni da bi potencijalni kiber napadi u veoma bliskoj budućnosti mogli da izazovu znatno veće posledice. Veća mrežna integracija infrastrukture jedne zemlje podrazumeva i veće potencijalne slabosti[30] Uzmimo, na primer, efekat kiber operacije koja onemogućava snabdevanje strujom velikih gradova, onesposobljavanje sistema kontrole u industrijskoj proizvodnji ili ubacivanje zlonamernih programa dizajniranih da ugroze čitav sistem protivvazdušne odbrane jedne države.

2. Član 2(4) Povelje UN

Povelja UN je u 21. veku najautoritativniji izvor kojim se reguliše upotreba sile, a član 2(4) Povelje UN je možda najviše citirana odredba savremenog međunarodnog prava. Prema članu 2(4) Povelje UN, „svi članovi se u svojim međunarodnim odnosima uzdržavaju od pretnje silom ili upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti svake države, ili na svaki drugi način nesaglasan s ciljevima Ujedinjenih nacija"[31]. Pitanje koje se postavlja jeste na koji način kiber operacije mogu biti okvalifikovane kao „sila" u smislu ove zabrane.

Iako je značenje pojma „sila" dovoljno široko da obuhvati i oružane i neoružane oblike prinude, većina današnjih akademika tumači termin „sila" iz člana 2(4) Povelje UN kao sinonim za „oružanu" ili „vojnu" silu[32]. To ne mora nužno da znači da je zabrana upotrebe sile ograničena na primenu tradicio-

28 Preambula Povelje UN.
29 N. Melzer, *Cyberwarfare and International Law*, 2011, str. 8, dostupno na: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.
30 J. A. Ophardi, *Cyberwarfare and the Crime of the Aggression: Need for Individual Accountability on Tomorrows Battlefield*, str. 3.
31 Član 2 Povelje UN.
32 Albrecht Randelzhofer, Article 2(4), in: B. Simma (ed.), *The Charter of the United Nations: A Commentary*, vol. I, 2002, str. 117; I. Brownlie, *International Law and the Use of Force by States*, 1963, str. 362, M. Roscini, World Wide Warfare – Jus ad bellum and the Use of Cyber Force, *Max Planck Yearbook of United Nations Law*, vol. 14, 2010, str. 105.

nalnog, kinetičkog, hemijskog, biološkog ili nuklearnog naoružanja[33]. Prema Međunarodnom sudu pravde, zabrana se odnosi na „upotrebu sile, bez obzira na upotrebljeno oružje“[34].

Bivši direktor Agencije za nacionalnu bezbednost SAD general-potpukovnik Aleksandar Kejt više puta je izjavio da „ne postoji međunarodni konsenzus o preciznoj definiciji upotrebe sile u ili van kiber prostora“[35]. Relativno je nesporno da kiber operacije potpadaju pod zabranu iz člana 2(4) Povelje UN kada se njihovi efekti mogu uporediti sa onima koji rezultiraju kroz upotrebu kinetičkog, hemijskog, biološkog ili nuklearnog oružja. To bi svakako uključivalo korišćenje kiber oružja kao ofanzivnog alata dizajniranog da izazove smrt ili povredu lica ili uništavanje objekata i infrastrukture, bez obzira na to da li takvo uništavanje podrazumeva fizičku štetu[36].

Ako tumačimo pojam „sile“ u smislu člana 2(4) Povelje UN, kiber operacija kojom se manipuliše ciljanim računarskim sistemima tako da se izazove kolaps u funkcionisanju kritične nacionalne infrastrukture (na primer, nuklearna elektrana[37], otvaranje brane iznad naseljenog područja, onemogućavanje kontrole letenja sa potencijalno užasnim posledicama u smislu izazivanja smrti, povreda i razaranja) predstavlja nedozvoljeni akt. Pravi problemi nastaju sa kvalifikacijom upotrebe „sile“ u kiber operacijama koje ne prouzrokuju smrt, povredu ili uništenje, ili bar to ne čine direktno[38]. Svaki kiber napad koji namerno izaziva destruktivnu snagu na teritoriji druge države jeste nezakonita upotreba sile koja može predstavljati oružani napad i traži pravo na samoodbranu[39]. Bilo bi nerazumno sugerisati da svaki kiber napad koji ne uništava objekte, u tradicionalnom smislu predstavlja upotrebu sile. Napadi mogu biti okarakterisani kao takvi u zavisnosti od njihovih efekata i posledica.

33 Pogledati: International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, advisory opinion, 1996, § 39; I. Brownlie, *International Law and the Use of Force by States*, 1963, pp. 362, 431.
34 Pogledati: *International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, advisory opinion*, 1996, str. 39; I. Brownlie, *International Law and the Use of Force by States*, 1963, str. 362–431.
35 M. C. Waxman Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), *Yale Journal of International Law*, 2011, str. 433.
36 M. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on aNormative Framework, *Columbia Journal of Transnational Law*, vol. 37, 1999, p. 916.
37 Kompjuterski crv staksnet (Stuxnet) nastao je sa ciljem sabotaže iranskog nuklearnog programa. Njegova meta bili su kontrolni sistemi gasnih centrifuga u iranskom postrojenju za obogaćivanje uranijuma „Natanz“.
38 N. Melzer, *Cyberwarfare and International Law*, 2011, str. 7, dostupno na: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.
39 W. G. Sharp, Cyberspace and the Use of Force, Ageis Research Corp, Falls Church, 1999, str. 133.

Dok Povelja UN ne definiše šta predstavlja „pretnju", Međunarodni sud pravde je utvrdio da „pojmovi 'pretnja' i 'upotreba' sile na osnovu člana 2, stava 4, Povelje stoje zajedno u smislu da ako je upotreba same sile u datom slučaju protivzakonita – iz bilo kog razloga – pretnja upotrebom sile isto je tako nezakonita. Čak ako i dođe do upotrebe sile ona, mora biti u skladu sa Poveljom UN"[40].

Povelja UN zabranjuje ne samo stvarnu upotrebu sile, već i samu pretnju silom u međunarodnim odnosima. Princip sadržan u članu 2(4) Povelje UN, koji predstavlja između ostalog i deo običajnog međunarodnog prava, zabranjuje upotrebu sile u svim situacijama, osim u dve pažljivo definisane: 1) Savet bezbednosti može da odobri kolektivnu akciju za održavanje i sprovođenje međunarodnog mira i bezbednosti; 2) države imaju pravo na „individualnu ili kolektivnu samoodbranu u slučaju oružanog napada na tu državu"[41]. U tom kontekstu treba napomenuti i da član 2(4) Povelje UN zabranjuje pribegavanje upotrebi sile između država, bez obzira na veličinu ili trajanje[42]. Kako se Međunarodni sud pravde (MSP) izjasnio u slučaju Nikaragva, čak i manje radnje upotrebe sile u međudržavnim odnosima potpadaju pod opšte zabrane iz člana 2(4) Povelje UN, bez obzira na to da li se oni kvalifikuju kao dela „agresije", ili kao „oružani napadi", čime se automatski stiče pravo država da posegnu za silom u samoodbrani[43].

Još uvek ne postoji konsenzus u pogledu preciznog kriterijuma po kom kiber napadi predstavljaju pretnju po međunarodni mir i kada mogu biti uzeti u obzir kao upotreba sile. Kiber napadi nisu predviđeni od strane autora Povelje UN i, za sada, ni praksa država ni međunarodna jurisprudencija nisu pružili jasne kriterijume u pogledu konsenzusa po kom se pretnje iz kiber prostora koje ne prouzrokuju smrt, povredu ili uništenje mogu smatrati zabranjenim članom 2(4) Povelje UN[44].

Član 2(4) Povelje UN upućen je državama i zabranjuje njihovo pribegavanje sili isključivo u njihovim međusobnim, „međunarodnim odnosima". To u

40 Savetodavno mišljenje Međunarodnog suda pravde o upotrebi nuklearnog oružja donetog na zahtev Generalne skupštine Ujedinjenih nacija, 1996.
41 Član 107 Povelje UN.
42Međunarodni sud pravde, slučaj Krfskog kanala (Ujedinjeno Kraljevstvo protiv Albanije) UN dokument A/ CN. 4/318/Add. 5–7, 1980, §§ 58, 86; A. Randelzhofer, Article 2(4), in: B. Simma (ed.), The Charter of the United Nations: A Commentary, vol. I, 2002, str. 123; I. Brownlie, *International Law and the Use of Force by States*, 1963, str. 241 i 432.
43 Međunarodni sud pravde, Vojne i paravojne aktivnosti u i protiv Nikaragve (Nikaragva protiv Sjedinjenih Američkih Država), 1986, Izveštaj međunarodne pravne komisije na 32. zasedanju održanom 5 maja do 25. juna 1980, Izveštaj Generalne skupštine UN na 35. zasedanju, UN dokument A/35/10, 1980, str. 44; Ian Brownlie, *International Law and the Use of Force by States*, 1963, str. 366.
44 N. Melzer, Cyberwarfare and International Law, 2011, str. 9, dostupno na: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

suštini znači da upotreba ili pretnja silom mora biti pravno pripisana jednoj državi i usmerena protiv jedne ili više drugih država. U međunarodnom pravu akti se mogu pripisati državi kada ih izvode lica ili entiteti koji deluju u ime ili na osnovu ovlašćenja ili odobrenja date države da se angažuje kako bi stekli međunarodnu pravnu odgovornost za svoje delovanje[45]. Lica ili entiteti koji ne deluju u ime države ili čija veza sa datom državom nije dovoljna da bi iznedrila međunarodnu pravnu odgovornost, s druge strane, ne mogu se smatrati državnim agentima i mogu se opisati kao „nedržavni akteri". Upotreba sile (uključujući kiber operacije) od strane pojedinih hakera i drugih nedržavnih aktera može biti relevantna prema međunarodnom humanitarnom pravu i u nekim slučajevima međunarodnog krivičnog prava, ali ovo nije zabranjeno članom 2(4) Povelje UN.

3. Da li su kiber napadi akt agresije?

Prema Rezoluciji Ujedinjenih nacija, agresija je „upotreba vojne sile od strane jedne ili više država koje imaju za cilj ugrožavanje teritorijalnog integriteta, suvereniteta i političke nezavisnosti druge države"[46].

Postavlja se pitanje da li kiber napadi mogu biti podvedeni i pod pojam agresije. U središte same definicije postavljena je teritorija. Svako ugrožavanje teritorije suverene države zabranjeno je u međunarodnim odnosima. Kiber napadi imaju određene specifičnosti koje treba uzeti u obzir povodom njihove klasifikacije kao agresije. Invazija na teritoriju nije moguća u kiber prostoru zbog sledećih razloga:

1) ne postoji vojska koja učestvuje u invaziji;

2) ne postoji akt fizičkog prelaska granice tokom kiber napada;

3) cilj invazije – da se osvoji teritorija – neostvariv je jer kiber napadi ne mogu da rezultiraju vojnom okupacijom u tradicionalnom vidu.

Dodatne poteškoće u većini slučajeva stvara nemogućnost da se identifikuju identitet napadača i lokacija sa koje je napad izvršen.

Država agresor može ilegalno pristupiti vitalnim sistemima države (poput sistemima odbrane ili sistemima nacionalne kritične infrastrukture) postavljajući viruse, trojance, crve i druge zlonamerne programe.

Kiber napadi imaju određene karakteristike koje bi trebalo uzeti u obzir prilikom odlučivanja da li se mogu kvalifikovati kao agresija. Pored toga što je

45 U unutrašnje organe za održavanje međunarodnih odnosa spadaju šef države, šef vlade, ministar spoljnih poslova, ostala ministarstva, predstavničko telo, a u spoljašnje diplomatski i konzularni predstavnici.

46 Rezolucija UN 3314-XXIX, 1974.

upotreba sile zabranjena u smislu člana 2(4) Povelje, agresori koji se oslanjaju na kiber napade imaju mogućnost da nanesu štetu odmah nakon dobijanja pristupa ciljanom sistemu[47], ili pak mogu da napadnu u trenutku koji im najviše odgovara.

Za razliku od tradicionalnih oružanih snaga, kiber napadi ne mogu da rezultiraju okupacijom teritorije. Ali oni imaju potencijala da uspeju u onome u čemu nisu uspela konvencionalna oružja i bombe, i to praktično bez kolateralne štete i ljudskih žrtava[48]. Modifikacija ili manipulacija podacima, napadi na veb-sajtove, ubacivanje kontradiktornih podataka, trajno uništavanje podataka konkurencije, napadi na državne ili privatne servise, fišing napadi, spam poruke, ubacivanje virusa, krađa identiteta, nezakonito prisvajanje dobiti hakovanjem, samo su neki od primera zloupotreba u kiber prostoru.

Kiber napadi mogu da izazovu stvarni gubitak života i uništavanje imovine. Takođe, rasprostranjene su pretnje od zlonamernog ometanja komunikacionih mreža i ekonomskih tržišta. Kiber napadač može manipulisati aktivnostima na berzi i uzrokovati finansijske gubitke, ili izazvati ogromne i stalne ispade bežičnih mreža. Dok ovi akti nemaju efekat fizičkog uništenja, potencijalne ekonomske posledice i širina njihovog uticaja mogu biti ozbiljna pretnja po normalno funkcionisanje države. Čak i državno sponzorisane manipulacije ekonomskih tržišta ne bi uspele da zadovolje tradicionalnu definiciju međunarodne agresije[49].

4. Pravo država na samoodbranu – član 51 Povelje UN

Autori Povelje UN uneli su izuzetno važnu klauzulu koja će omogućiti državama da se, u slučaju potrebe i po sopstvenoj proceni da li takva potreba postoji, sami pobrinu za svoju bezbednost – pravo na individualnu samoodbranu[50].

Prema članu 51 Povelje UN, „ništa u ovoj Povelji ne umanjuje urođeno pravo na individualnu ili kolektivnu samoodbranu ukoliko dođe do oružanog napada protiv članica Ujedinjenih nacija“[51]. U vezi sa upotrebom sile, ova ter-

47 J. Adams, The Next World War: The Warriors and Weapons in the New Battlefields in Cyberspace, Hutchinson, London, 1998, str. 199; D. Delibasis, A New Challenge for a New Century, *Peace Conflict and Development: An Interdisciplinary Journal*, Issue 8, 2006.
48 M. Benatar, The Use of Cyber Force: Need for Legal Justification?, *Goettingen Journal of International Law*, 1, 2009.
49 J. A. Ophandt, Cyber Warfere and the crime of Aggression: the Need for Individual Accountability on Tomorrow's Battlefield, *Duke Law & Technology Review*, 2010, str. 5.
50 O. Račić, *Ujedinjene nacije između moći i prava*, Službeni glasnik, 2010, str. 51.
51 Povelja UN, član 51.

minologija sugeriše jaz između zabrane „sile" prema članu 2(4) i izuzetak u slučaju „oružanog napada" po članu 51 Povelje UN.

Član 2(4) Povelje UN obimom je veći nego član 51, u smislu da zabranjuje ne samo oružani već i neoružani ili indirektan način upotrebe sile kao i pretnju silom. Drugim rečima, nije nužno da svaka pretnja ili upotreba sile zabranjena članom 2(4) automatski znači opravdanje za odbrambenu oružanu akciju[52].

Treba istaći, međutim, da tumačenje oružanog napada sprovedenog od strane nedržavnih aktera ostaje kontroverzno i ne odražava univerzalni konsenzus[53].

Iako je važno da se ispita da li akcija države predstavlja pretnju ili stvarnu upotrebu sile, „važno je postaviti pitanje da li akcija sprovedena oružanim napadom ovlašćuje napadnutu državu da odgovori u samoodbrani"[54] i, ako je odgovor pozitivan, na koji način će biti odgovoreno na pretnju. Do danas nije zabeležen slučaj da je jedan kiber napad okarakterisan kao „oružani napad" koji bi pozvao na dejstvo u smislu člana 51 Pozivanje na ovaj član Povelje UN u kiber svetu tek treba da se definiše.

Uzimajući u obzir nedostatak prakse u realnim okolnostima, možda ipak postoji mogućnost da država, žrtva zaista razornog kiber napada, ili obrazaca takvih napada, ubedi međunarodnu zajednicu da se „oružani napad" protiv nje dogodio i da je imala pravo na samoodbranu. Primer za to je kiber napad na Estoniju. U aprilu 2007. godine različita ministarstva i estonski parlament, finansijske institucije, banke i medijske kuće, bili su pogođeni nizom napada distribuiranog uskraćivanja usluga (DDoS), što je privremeno sprečilo pristup veb-sajtovima ovih institucija u Estoniji i njihovo normalno funkcionisanje[55]. Za napad je optužena Ruska Federacija. Estonija je pozvala Evropsku uniju i NATO, čija je članica, da razmotre hitne mere za reagovanje na ovaj kiber napad i ugrožavanje nacionalne bezbednosti. Ovo je ujedno i prvi poziv jedne države u (međunarodnu) pomoć u odbrani od kiber napada. Estonija se pozvala na član 5 NATO sporazuma o kolektivnoj samoodbrani, ali je usledio odgovor da kiber napadi „nisu definisani kao jasna vojna akcija" i da „kolektivna samoodbrana neće automatski biti pružena napadnutoj zemlji"[56].

52 Albrecht Randelzhofer, Article 51 UN Charter. The Charter of the United Nations: A Commentary, vol. I, 2002, str. 790; Ian Brownlie, International Law and the Use of Force by States, 1963, str. 278.

53 N. Melzer, *Cyberwarfare and International Law*, 2011, str. 9, dostupno na: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

54 G. H. Todd, Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, *Air Force Review*, Vol. 64, 2009, str. 71.

55 *Ibid*, str. 26.

56 A. D. Walker, *Applying International Law to the Cyber Attacks in Estonia*, Maxwell Air Force Base, 2008, str. 19.

Ne treba izgubiti iz vida da država može da donese odluku o samoodbrani samo na nacionalnom nivou[57]. Vredi napomenuti da, čak i u odsustvu međunarodne podrške, napadnuta država ima pravo da legalno ostvari svoje prirodno pravo na samoodbranu, sve dok se ponaša i deluje u granicama Povelje. U trenutku kada kiber napad dostigne nivo oružanog napada i kada može biti okvalifikovan kao takav, gotovo je neophodno da se na ovakav protivpravni akt odgovori na neki način.

Zaključak

Iako se često ističe da Ujedinjene nacije predstavljaju arenu koju velike sile koriste u cilju legitimizovanja svog delovanja, treba uzeti u obzir da je to najveća i najuglednija međunarodna organizacija. Ujedinjene nacije su postavile kamen temeljac granama međunarodnog prava nakon Drugog svetskog rata i stoga im treba dati mogućnost da i u oblasti kiber bezbednosti daju svoj doprinos.

Kako kiber prostor bude sazrevao, a opasnosti, pretnje i rizici se uvećavali, međunarodni sistem će biti suočen sa novim izazovima u suočavanju sa upotrebom sile. Međunarodni pravni sistem mora da se prilagodi i obezbedi mehanizme koji će zaštititi države. Države sve više postaju svesne da se u fazi povećanja opasnosti od ugrožavanja njihovog kiber prostora moraju naći odgovori na nove bezbednosne pretnje, ne samo kroz nacionalne strategije već i na međudržavnom nivou. Suočene kako sa tradicionalnim tako i netradicionalnim bezbednosnim izazovima, države su, kada deluju same, loše opremljene zbog čega postoji potreba za donošenjem zajedničke strategije i normi na međunarodnom nivou.

Kiber napadi, kiber ratovanje kao i druge kiber opasnosti staviće pred izazov Povelju Ujedinjenih nacija. Stoga je naglašena potreba za jasnoćom u tumačenju članova 2(4) i 51, pozivanje na ova dva člana, ali i stvaranje novog pravnog instrumenta ili međunarodnog ugovora pod okriljem Ujedinjenih nacija koji bi bio smernica državama.

Ujedinjene nacije kao najveća međunarodna organizacija imaju dužnost da pristupe izradi sveobuhvatne konvencije o pitanjima kiber bezbednosti. Kiber napadi su globalni izazov, globalna opasnost i zahtevaju globalni odgovor.

57 M. C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), *Yale Journal of International Law*, 2011, str. 12. Corfu Channel Case (Merits) [1949], ICJ Rep 4,22. 414, Getting It Right: Protecting American Critical Infrastructure in Cyberspace, S. M. Condron: Harvard Journal of Law & Technology, Vol. 20, Nr. 2, 2007.

Literatura

1. Adams, J; *The Next World War: The Warriors and Weapons in the New Battlefields in Cyberspace*, Hutchinson, London, 1998.
2. Benatar, M; The Use of Cyber Force: Need for Legal Justification?, *Goettingen Journal of International Law*, 1, 2009.
3. Brownlie, I; *International Law and the Use of Force by States*, 1963.
4. Dean, D. et al.; *The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy*, BCG Perspectives, 27 January 2012.
5. Delibasis, D; A New Challenge for a New Century, *Peace Conflict and Development: An Interdisciplinary Journal*, Issue 8, 2006.
6. http://m.guardian.co.uk/technology/2013/feb/21/white-house-cyber-threat-russia-china/, pregledano 5. 2. 2017.
7. http://www.telegraph.co.uk/news/uknews/defence/8369520/Military-Balance-report-countries-creating-new-cyber-warfare-organisations.html/, pregledano 3. 4. 2017,
8. International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, advisory opinion, 1996.
9. Klimburg A (Ed.); National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, 2012.
10. Makoff, Sanger, Shanker, *In Digital Combat, U.S. Finds No Easy Detteren*, http://www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=all&_r=0 /, pregledano 10. 7. 2016.
11. Međunarodni sud pravde, *Slučaj Krfskog kanala (Ujedinjeno Kraljevstvo protiv Albanije)*, UN dokument A/ CN. 4/318/Add. 5–7, 1980, §§ 58, 86.
12. Međunarodni sud pravde, Vojne i paravojne aktivnosti u i protiv Nikaragve (Nikaragva protiv Sjedinjenih Američkih Država), 1986, Izveštaj međunarodne pravne komisije na 32. zasedanju održanom 5. maja do 25. juna 1980, Izveštaj Generalne skupštine UN na 35. zasedanju, UN dokument A/35/10, 1980.
13. Melzer, N; *Cyberwarfare and International Law*, 2011, UNIDIR, dostupno na: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.
14. Ophandt, J. A; Cyber Warfere and the Crime of Sggression: The Need for Individual Accountability on Tomorrow's Battlefield, *Duke Law & Technology Review*, 2010.
15. *Povelja UN*, Udruženje za Ujedinjene nacije, Beograd, 2008.

16. Račić, O; *Ujedinjene nacije između moći i prava*, Službeni glasnik, 2010.
17. Randelzhofer, A; Article 2(4), in: Bruno Simma (ed.), *The Charter of the United Nations: A Commentary*, vol. I, 2002.
18. Randelzhofer, A; Article 51 UN Charter. The Charter of the United Nations: A Commentary, vol. I, 2002.
19. *Rezolucija UN 3314-XXIX*, 1974.
20. Roscini, M; World Wide Warfare – Jus ad bellum and the Use of Cyber Force, *Max Planck Yearbook of United Nations Law*, vol. 14, 2010.
21. Schmitt, M; Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, *Columbia Journal of Transnational Law*, vol. 37, 1999.
22. Schmitt, M; Cyber Operations and the Jus in Bello: Key Issues, *87 International Law Studies*, Naval War College, 2011.
23. Sharp, W. G; *Cyberspace and the Use of Force*, Ageis Research Corp, Falls Church, 1999.
24. Todd, G. H; Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, *Air Force Review*, Vol. 64, 2009.
25. Walker, A. D; *Applying International Law to the Cyber Attacks in Estonia*, Maxwell Air Force Base, 2008.
26. Waxman M. C; Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), *Yale Journal Of International Law*, 2011.

CYBER ATTACKS AND UNITED NATIONS CHARTER

Katarina Jonev

Abstract: The United Nations is the largest international organization with 193 member states. In the 21st century the influence of the United Nations as a global international organization has not decreased. Cyber attacks are a new form of potential warfare and do not fit into the traditional international framework governing the use of force. They appered as a potential threat much later than the UN Charter, which entered into force in 1945.
The aim of this paper is to present the interpretation of certain provisions of the UN Charter, primarily Article 2 (4) and Article 51, which could be used in the case of cyber attacks.
Keywords: the United Nations, cyber attacks, cyber security, the UN Charter, aggression