Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

MEĐUNARODNO PRAVO I CYBER SIGURNOST
INTERNATIONAL LAW AND CYBER SECURITY

Pregledni naučni rad

Prof. dr. Sakib Softić[117]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Cyber napadi predstavljaju novu sigurnosnu prijetnju koja se pojavila u dvadeset prvom vijeku. Ova sigurnosna prijetnja stavlja nove izazove pred pojedine države i međunarodnu zajednicu u cjelini. Sigurnosna prijetnja može dolaziti od drugih država ili od nedržavnih aktera.
Ciljevi rada (naučni i/ili društveni): Autor se u ovom tekstu bavi pitanjima koja se tiču primjene pravila međunarodnog prava odnosno prava oružanih sukoba na suzbijanje ove prijetnje.
Metodologija/Dizajn: Prvo se nastoji objasniti i definisati pojam međunarodnog prava cyber sigurnosti, zatim se analizira pitanje odnosa države prema cyber napadima i pravo države da upotrijebi silu radi suzbijanja cyber napada i na kraju se analizira pitanje da li se *cyber* napad može smatrati kao napad koji povlači pravo na individualnu i kolektivnu samoodbranu u smislu Povelje UN. I pod kojim uslovima.
Ograničenja istraživanja/rada: Rad je pregledni i pravno-teorijske prirode.
Rezultati/Nalazi: Pravo država na samoodbranu nije samo pasivno pravo države da čeka da se napad zaista i desi i da šteta bude pričinjena. Država ima pravo na aktivnu samoodbranu koja se između ostalog manifestuje i kao pravo na anticipativnu samoodbranu. Država, također, ima pravo na proporcionalne kontramjere.
Generalni zaključak: Pravo država na samoodbranu postoji i u slučaju napada počinjenog od nedržavnih aktera.
Opravdanost istraživanja/rada: Ovaj članak daje odgovor na složena međunarodnopravna pitanja vezana za ovu sigurnosnu prijetnju što svakako doprinosi boljem razumijevanju ovog pitanja i predstavlja doprinos razvoju nauke međunarodnog prava u ovoj materiji.

Ključne riječi

sigurnosna prijetnja, pravo oružanih sukoba, cyber sigurnost, upotreba sile, pravo države na samoodbranu

Abstract

Reason for writing and research problem (s): Cyber attacks constitute a new security threat in the twenty-first century. This security threat put new known and unknown challenges to the international community in the whole. The security threat may come from other states or from non-state actors.

[117] FKKSS, Univerzitet u Sarajevu

Aims of the paper (scientific and/or social): In this article the author deals with issues related to the application of the rules of international law and the right of armed conflict to counteract this kind of threats.
Methodology/Design: At first the author endeavor to explain and define the concept of international cyber security law, then analyzes the question of the state's relationship to cyber-attacks and the right of the state to use force to counter cyber-attacks, and finally analyzes whether cyber-attack can be considered as an act that entitles rights to individual and collective self-defense within the meaning of the UN Charter. And under what conditions.
Research/Paper limitation: This is a review paper and legal theory.
Results/Findings: The right to self-defense is not just a passive right of the state to wait for to be attacted. And that the damage be done. The state has the right to active self-defense, which also manifests itself as the right to anticipatory self-defense. The state is also entitled to proportional countermeasures.
General Conclusion: The right to self-defense also exists in the case of attacks committed by non-state actors.
Research/Paper Validity: This article givs answers to complex international legal issues related to this security threat, which certainly contributes to a better understanding of this issue and represents a contribution to the development of international law science in this matter.

Keywords
security threat, the right of the armed conflict, cyber security, use of force, the right of the state to self-defense.

1. Uvod

Cyber napadi predstavljaju novu sigurnosnu prijetnju sa kojom se države suočavaju početkom dvadeset prvog vijeka. *Cyber* napadi mogu po svojoj težini biti ekvivalentni konvencionalnim napadima sa kojima su države bile suočene u svojoj ranijoj historiji. Mogu proizvesti iste ili čak štetnije posljedice za državu i njene stanovnike nego konvencionalni napadi. Stoga se postavlja pitanje primjenjivosti međunarodnog prava odnosno prava oružanih sukoba i međunarodnog humanitarnog prava na situacije uzrokovane *Cybe*r napadima.

Pošto se radi o novoj pojavi nužno je utvrditi nova ili potvrditi primjenu postojećih pravila međunarodnog prava na *cyber* napade. O ovim pitanjima još uvijek ne postoji puna saglasnost među državama kao ni među pravnim piscima. Kao što je poznato međunarodno pravo je proizvod međudržavnih odnosa i kreira se putem međunarodnih ugovora i međunarodnih običaja. Problem je u tome što ne postoje međunarodni ugovori koji se direktno bave *cyber* napadima.[118] Također ni međunarodno običajno pravo u ovoj materiji

[118] Konvencija Vijeća Evrope iz 2001. godine donesena je radi sprečavanja djela koja narušavaju povjerljivost, integritet i dostupnost kompjuterskih sistema, mreža i podataka, kao i sprečavanje zloupotrebe tih sistema, mreža i podataka, osiguravajući usvajanje ovlasti dovoljnih da bi se omogućila efikasna borba protiv tih

nije dovoljno razvijeno. Jer se radi o novoj pojavi. Pitanje postojanja međunarodnopravnih normi primjenjivih na *cyber* napade postavilo se naročito nakon hakerskih napada u prvoj deceniji ovog vijeka. Što je ovu vrstu napada stavilo u fokus pažnje savremenih država i međunarodne zajednice u cjelini. Neke države kao naprimjer Kanada, Velika Britanija i SAD-e su usvojile određene dokumente kao reakciju na ovu vrstu prijetnji. [119] Također je ovo pitanje dospjelo na dnevni red Ujedinjenih nacija koje su potvrdile da je međunarodno pravo i to naročito onaj dio koji je sadržan u Povelji UN primjenjiv i na Cyber napade.[120] Neke međunarodne organizacije su nastojale utvrditi pravila međunarodnog prava primjenjiva na oružane sukobe.[121] Većina pravnih pisaca je shvatanja da se međunarodno pravo primjenjuje i na Cyber prostor.[122] Mada su neki mišljenja da je primjena međunarodnog prava na Cyber sigurnost u krizi.[123]

Da bi se uopšte postavilo pitanje primjenjivosti međunarodnog pravo na *Cyber* napade potrebno je da oni imaju određenu težinu. Prema mišljenju Međunarodnog suda pravde pravo oružanih sukoba se primjenjuje na ,,bilo koju upotrebu sile, bez obzira na upotrijebljeno oružje''.[124] Ali 'upotrijebljena sila'' mora proizvesti posljedice relevantne za međunarodno pravo.

Međunarodno pravo sadrži dvije grupe odredaba primjenjivih na ove situacije. Prva se odnosi na *jus ad bellum* odnosno na pravo pribjegavanja upotrebi sile. Druga grupa *jus in bell*o se primjenjuje kad je rat već otpočeo i tiče se primjene pravila međunarodnog

krivičnih djela, olakšavajući njihovo otkrivanje, istragu i gonjenje, kako na unutrašnjem tako i na međunarodnom nivou, i predviđajući materijalne odredbe u cilju brže i povjerljivije međunarodne saradnje. Vidi uvod: Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004).

[119] Ministarstvo odbrane SAD je 2011. godine izdalo Strategiju za djelovanje u cyber prostoru označavajući cyber napade kao sigurnosnu prijetnju. Strategija je nekoliko puta dopunjena.

[120] Vidi: U.N. Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, U.N. GAOR, 68th Sess., U.N. Doc. A/68/150 (June 24, 2013).

[121] NATO suradnički centar za izvrsnost u Cyber odbrani sa sjedištem u Talinu, izdao je 2013. godine ''Talin manuel o međunarodnom pravu koje se primjenjuje na cyber ratovanje. Priručnik (*manuel*) je dopunjen 2017. godine i predstavlja najpotpuniju kompilaciju međunarodnog prava primjenjivog na ovu oblast. Sačinjen je od strane istaknutih neovisnih međunarodnih pravnika iz dvadeset pet zemalja. U daljem tekstu: *Talin manuel*. Vidi: https://ccdcoe.org/research/tallinn-manual/.

122 Vidi npr. Gary D. Brown: International law Apllies to Cyber Warfare! Now What. 355 BROWN (DO NOT DELETE) 4/11/2017 7:52 PM. https://www.swlaw.edu/sites/default/files/2017-08/355%20International%20Law%20Applies%20to%20Cyber%20Warfare-Brown.pdf 20.09.2019.; MIRANDA GRANGE: CYBER WARFARE AND THE LAW OF ARMED CONFLICT LAWS 533: LAW OF ARMED CONFLICT, RESEARCH PAPER. Faculty of Law Wictoria 2014. https://core.ac.uk/download/pdf/41339676.pdf . 20.09.2019.

123 Vidi: Kubo Mačák: Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict. 127-139.

124 INTERNATIONAL COURT OF JUSTICE REPORTS OF JUDGMENTS, ADVISORY OPINIONS AND ORDERS LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS ADVISORY OPINION OF 8 JULY 1996. U daljem tekstu: Nuclear Weapons Advisory Opinions, para. 39.

ratnog prava, prava oružanih sukoba i međunarodnog humanitarnog prava na konkretnu situaciju.[125]

Naročiti problem za primjenu pravila međunarodnog prava na *cyber* napade uzrokovani su karakterom ''internetske mreže'' koja otežava otkrivanje i identifikovanje napadača. Nesporno je da države nastoje prikriti činjenicu da su one izvršilac *cyber* napad. To im olakšava mogućnost angažovanja anonimnih pojedinaca i grupa koje će izvršiti *cyber* napad. Nakon čega se brišu svi tragovi koji bi mogli dovesti u vezu državu napadača sa izvršenim napadom.

Pošto je pitanje primjenjivosti odredaba međunarodnog prava na *cyber* napade nova tema to je o njoj bilo vrlo malo riječi. Stoga je namjera autora da doprinese razvoju ovog dijela međunarodnog prava i da istraži i analizira primjenjivost nekih od postojećih instituta međunarodnog prava na *cyber* napade.

2. Pojam Međunarodnog prava cyber sigurnosti

Međunarodno pravo *cyber* sigurnosti je novi pojam u međunarodnom pravu. Služi nam da identifikujemo one dijelove međunarodnog prava koji se bave neprijateljskom upotrebom *Cyber* prostora. I ako je međunarodno pravo *cybe*r sigurnosti novi pojam u međunarodnom pravu on ne znači stvaranje neke nove grane međunarodnog prava.[126] Ne stvaraju se novi instituti međunarodnog prava. Ovdje se više radi o specifičnostima primjene postojećih instituta na novu situaciju.

Međunarodno pravo uspostavlja odgovornost država za međunarodne protivpravne akte počinjene od njenih državnih organa kao i nekih nedržavnih aktera čiji su akti pod određenim okolnostima pripisivi državi.[127] Po međunarodnom pravu države mogu biti odgovorne za *cyber* operacije svojih državnih organa i nedržavnih aktera koji joj se mogu pripisati.

Ovdje se radi o neprijateljskim *cyber* napadima takve težine da aktiviraju primjenu pravila međunarodnog prava koja zabranjuju upotrebu sile protiv drugih nezavisnih država. Ili spadaju u napade takvog intenziteta da povlače primjenu glave VII Povelje UN koja

125 Vidi: Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).

[126] Ovaj pojam je više deskriptivan i obuhvata pojmove suverenosti, jurisdikcije i odgovornosti država ukoliko se ovi bave međunarodnim pravom rata i međunarodnim pravom u ratu. Vidi: Talin manuel o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 24

[127]United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

predviđa pravo država na individualnu ili kolektivnu samoodbranu kao i upotrebu sile od strane Savjeta sigurnosti UN u cilju suzbijanja (*cyber*) napada.

Povelja UN zabranjuje nezakonitu upotrebu sile u odnosima između država koristeći pri tome dva pojma značajna za našu temu.

Prvi je ''upotreba sile'' protiv druge države.

Opća zabrane rata temelji se na odredbi člana 2. stav 4. Povelje UN: "Svi članovi će se u svojim međunarodnim odnosima uzdržavati od prijetnje silom ili od upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti ma koje države, ili koja bi na ma koji drugi način bila u suprotnosti sa ciljevima Ujedinjenih nacija."

Ova zabrana upotrebe sile prihvaćena je kao međunarodno običajno pravo i čak kao *ius cogens* norma kako je to potvrđeno u presudi Međunarodnog suda u Hagu u predmetu *Nikaragva* protiv SAD.[128]

Drugi upotrijebljeni izraz je ''agresija''. Član 39. Povelje daje ovlaštenje Savjetu sigurnosti da procjenjuje da li se radi o prijetnji miru, povredi mira ili aktu agresije. Ujedinjene nacije su svojom rezolucijom 3314 (XXIX) iz 1974. godine definsale agresiju kao:

''...upotreba oružane sile od strane neke države protiv suvereniteta, teritorijalne cjelovitosti ili političke nezavisnosti neke druge države ili upotrebu oružane sile koja je na bilo koji drugi način nespojiva s Poveljom Ujedinjenih nacija...''.

Povelja UN ne definiše napad. Ali to čini drugi opšteprihvaćeni međunarodnopravni dokument. Dopunski protokol I iz 1977. godine na Ženevske konvencije iz 1949. godine. Članom 49 Protokola I napad se definiše kao ''akti nasilja protiv protivnika, bilo da su ofanzivni ili defanzivni''.

Protokol I se primjenjuju na sve napade, bez obzira na kojoj se teritoriji preduzimaju, uključujući nacionalnu teritoriju koja pripada strani u sukobu, ali koja je pod kontrolom protivničke strane. Također, Protokol I se primjenjuje na kopneno, zračno ili pomorsko ratovanje koje može pogoditi civilno stanovništvo, pojedine civile ili civilne objekte na kopnu.[129]

Da bi cyber napadi predstavljali napade u smislu člana 49. Dopunskog protokola I moraju uzrokovati fizičku destrukciju ili štetne povrede kao i druge vrste oružja: konvencionalno,

---

[128] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986, p 14, para 190.
[129] Vidi: Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).

nuklearno, hemijsko i biološko.[130] Zapaženo je nekoliko pristupa u analizi da li neki cyber napad predstavlja napad u smislu međunarodnog prava.

Prvi je pristup zasnovan na učinku. Da bi se radilo o napadu zahtijeva se da *cyber* napad uzrokuje iste posljedice kao i druge vrste napada. Drugi je pristup zasnovan na cilju. Ukoliko je napad usmjeren protiv bilo čega što se zove kritična infrastruktura onda napad zadovoljava kriterije koje postavlja međunarodno pravo. Pristup koji uključuje upotrijebljena sredsta za napad je odbačen kao neprimjenjiv na ovu vrstu napada.[131]

Međunarodno pravo oružanih sukoba primjenjuje se i na *cyber* operacije kao i na druge operacije preduzete tokom oružanog sukoba. Tako prema *Talin manuelu* ,,*Cyber* operacije izvršene u kontekstu oružanog sukoba podliježu pravu oružanih sukoba''.[132] Pravo oružanih sukoba primjenjuje se na *cyber* operacije bez obzira da li se radi o međunarodnom ili unutrašnjem oružanom sukobu.[133]

S druge strane pravo oružanih sukoba se ne primjenjuje na aktivnosti privatnih korporacija koje nisu povezane sa oružanim sukobima.[134] Za *cyber* oružane sukobe ključna su pitanja: mjesto sa kojeg su *cyber* operacije pokrenute, lokacija gdje su smješteni uređaji za *cyber* operacije i mjesto na koje su usmjerene *cyber* operacije. Također, sa ovim pitanjima povezana su i pravila o neutralnosti koja nenamjerno mogu biti povrijeđena ovom vrstom operacija.

''Međunarodni oružani sukob postoji kadgod postoje neprijateljstva koja mogu uključiti ili biti ograničena na *cyber* operacije, koji se odvijaju između dvije ili više država.''[135] Dok ''Nemeđunarodni oružani sukob postoji kadgod postoji produženo oružano nasilje, koje može uključiti ili biti ograničeno na *cyber* operacije, koji se odvijaju između vladinih oružanih snaga i snaga jedne ili više oružanih grupa, ili između takvih grupa. Sukobljavanja moraju dostići minimalni stepen intenziteta i strane uključene u sukob moraju pokazati minimalni stepen organizacije''.[136]

Pravo cyber oružanih sukoba se ne odnosi samo na pitanja njegove primjene *jus ad bellum* nego i na *jus in bello*. *Talin manuel* reguliše pitanje krivične odgovornosti komandanata i nadređenih za ratne zločine nastale kao posljedica naredbe da se izvrše *cyber*

---

[130] Vidi: Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp. 271 – 280.
[131] Vidi: Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp 275.
[132] Član 20 *Talin manuela*.
[133] Vidi članove 22 i 23 *Talin manuela*.
[134] Vidi *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 69.
[135] Član 22 *Talin manuel*-a.
[136] Član 23 *Talin manuel-a*.

operacije koje predstavljaju ratni zločin. Također, komandant i nadređeni su odgovorni za nepreduzimanje mjera da se takvi zločini spriječe odnosno da se počinioci kazne.[137]

3. Država i cyber napadi

Osnovno je pravilo da država može na temelju svoje suverenosti vršiti kontrolu nad *cyber* infrastrukturom i aktivnostima unutar svoje teritorije.[138]

Ovo pravo proizlazi iz koncepta suverenosti kako je utvrđen međunarodnim pravom. Suverenost podrazumijeva vršenje efektivne vlasti nad teritorijom i stanovništvom. ''*Država ne mora imati bilo kakav poseban oblik vlasti, ali tu mora postojati neka vlast koja vrši funkcije vlade i biti sposobna da predstavlja entitet u međunarodnim odnosima*.''[139]

U predmetu: Ostrva Aland (*Aaland Islands*) imenovan je *Međunarodnog odbora pravnika sa zadatkom da* istraži status ostrva povodom pitanja vremena uspostave Finske republike. Pitanje je postavljeno radi utvrđivanju odgovornosti za nerede koji su nastupili tokom ruske revolucije i državnog osamostaljenja Finske. Odbor je sačinio Izvještaj u kome je iznio *stav o pravnim aspektima pitanja Alandskih ostrva.* U Izvještaju se o sticanju suverenosti navodi:

''*To se sigurno nije desilo dok nije stvorena stabilna politička organizacija, i dok javna vlast nije postala dovoljno jaka da se učvrsti na državnom teritoriju bez pomoći stranih trupa*.''[140]

Maks Huber je u predmetu *Palmas Island* istakao:

''*Suverenost između država znači nezavisnost. Nezavisnost u odnosu na dio zemljine površine je pravo da se na tom dijelu, uz isključenje svake druge države, vrše državne funkcije. Razvoj države kao nacionalne organizacije tokom nekoliko posljednjih vjekova, i kao prirodna posljedica, razvoj međunarodnog prava, utemeljili su ovaj princip isključive nadležnosti države u odnosu na njenu vlastitu teritoriju na takav način da predstavlja tačku razdvajanja u rješavanju većine pitanja koji se tiču međunarodnih odnosa*.''[141]

Postoje dvije posljedice suverenosti države nad *cyber* infrastrukturom. Prva je da je *cyber* infrastruktura podvrgnuta pravnoj i regulatornoj kontroli države. I druga je da državni

---

[137] Član 24. Talinnmanuel-a.
[138] *Talin manuel* str. 25.
[139] Carter/Trimble/Bradley. *(2003) International Law*, forth edition. New York: Aspen Publisher. Str. 433.
[140] L.N.O.J., Special Supp. No. 3., p.3 (1920). Harris (2004) Cases and Materials on International Law, sixth edition. London: Thomson, Sweet§Maxwell. Str. 100-101; Shaw, N. M. (2008) International Law, sixth edition, Cambridge: Cambridge University Press. Str.200-201.
[141] Island of Palmas Case. RIAA II 829, at 838. Cit. Prema Malanczuk, P. (1997) Akehurst's modern introduction to International Law, seventh revised edition, London and New York: Routledge. Str. 109-10.

suverenitet štiti takvu infrastrukturu.[142] *Cyber* napad od strane jedne države usmjeren protiv *cyber* infrastrukture druge države predstavlja povredu njene suverenosti.[143]

Svaka država ima pravo da uređuje svoj pravni poredak i radi toga da uređuje prava i obaveze svih pravnih subjekata koji se nalaze na njenoj teritoriji. U isto vrijeme država ne može izvršavati bilo kakav akt vlasti na teritoriji koja pripada nekoj drugoj državi. Ova prava proizlaze iz prava jurisdikcije.

Jurisdikcija je usko povezana sa suverenošću jer predstavlja primjenu državne vlasti kojom nastaju, prestaju ili se mijenjaju prava i obaveze pravnih subjekata na područjima na kojima država ima teritorijalni suverenitet.

Talin manuel u članu 2. potvrđuje jurisdikciju država u odnosu na *cyber* infrastrukturu:

,,Bez prejudiciranja primjene međunarodnih obaveza država može ostvarivati vlastitu jurisdikciju:

a) Nad osobama angažovanim u *cyber* aktivnostima na njenoj teritoriji,
b) Nad *cyber* infrastrukturom koja se nalazi na njenoj teritoriji, i
c) Ekstrateritorijalno, u skladu sa međunarodnim pravom.''

Da bi država bila odgovorna za počinjenje *cyber* napada kao međunarodnog protivpravnog djela ponašanje (napadi) mora biti pripisivo toj državi. Generalno pravilo je da samo ponašanje državnih organa ili njenih agenata[144] može biti pripisivo državi.

Član 4. Pravila o odgovornosti država za međunarodna protivpravna djela pobliže određuje koji su to organi države čije ponašanje povlači odgovornost države. [145]

"1. *Ponašanje bilo kojeg državnog organa će se smatrati aktom države prema međunarodnom pravu, bilo da organ vrši zakonodavnu, izvršnu, sudsku ili kakvu god drugu funkciju, bez obzira koju poziciju ima u državnoj organizaciji i bez obzira da li ima karakter organa centralne vlade ili vlade teritorijalne jedinice države. 2. Organ uključuje lice ili subjekt koji ima status u skladu sa domaćim pravom države*.''

Država odgovara također, i za lica ili subjekte koji faktički postupaju kao organi države, čak i ukoliko nisu tako klasificirani po unutrašnjem pravu države. Akti osoba ili subjekata

---

[142] *Talin manuel*. str. 25.
[143] Vidi Talin manuel. str. 25 -27.
[144] Osobe ili entiteti koji djeluju po uputstvima, ili su poticani ili kontrolisani od strane države odnosno njenih organa.
[145]United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

koji nisu državni organi, ali su po unutrašnjem pravu ovlašteni da vrše elemente javne vlasti, smatrat će se kao akti države ako u konkretnom primjeru osoba ili subjekt postupa u tom kapacitetu.[146]

Pravila pokrivaju i relativno nove fenomene kao što su paradržavni organi i privatizirane državne korporacije. Čak i privatne osobe i subjekti mogu biti obuhvaćeni ako su po domaćem pravu ovlašteni da izvršavaju državne funkcije kao što su izvršavanje državnih propisa o izvršavanju kazne lišenja slobode, što je slučaj u nekim državama.

Međunarodno protivpravno djelo države postoji kad je ponašanje države, koje može biti činjenje ili propuštanje: '' (a) *pripisivo državi po međunarodnom pravu; i (b) predstavlja povredu neke međunarodne obaveze države*.''[147]

Ukoliko je neko djelo protivpravno djelo po međunarodnom pravu, njegova protivpravnost se ne može isključiti njegovom karakterizacijom kao dopuštenog djela pravilima unutrašnjeg pravnog poretka. Karakterizacija jednog akta države kao protivpravnog po međunarodnom pravu vrši se prema kriterijima ustanovljenim u međunarodnom pravu (član 3. Pravila).

4. Upotreba sile od strane država radi suzbijanja *cyber* napada

Kao što je već rečeno član 2. tačka 4. Povelje zabranjuje svaku upotrebu sile i propisuje da će se svi članovi UN u svojim međunarodnim odnosima uzdržavati od prijetnje silom ili od upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti druge države, ili koja bi na ma koji drugi način bila u suprotnosti sa ciljevima Ujedinjenih nacija**.**

Povelja Ujedinjenih nacija je centralizovala kontrolu upotrebe sila u rukama Savjeta sigurnosti UN. Samo Savjet sigurnosti ima pravo da utvrdi *''postojanje prijetnje miru, povrede mira ili agresije*" (Član 39. Povelje UN).

Izraz ''zabrana upotrebe sile'' upotrijebljen u članu 2. stav 4. Povelje UN nije definisan. Također, postojanje prijetnje miru, povreda mira i akt agresije, izrazi upotrijebljeni u članu 39. Povelje UN nemaju preciznu definiciju. To daje široke mogućnosti Savjetu sigurnosti prilikom odlučivanja da li postoji situacija iz člana 39. Povelje, ili se pak radi o nekoj

[146] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. Articl 5.http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.
[147] United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. Articl 2.http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

drugoj situaciji. Član 51. Povelje UN daje državama pravo na individualnu i kolektivnu samoodbranu u slučaju oružanog napada.

Međunarodni sud pravde je u predmetu *Nikaraqua* naveo da se član 2. tačka 4. i član 51. Povelje primjenjuju na ,,bilo koju upotrebu sile, bez obzira na upotrijebljeno oružje''.[148]

Prema članu 10. *Talin Manuela* ''*Cyber* operacije koje predstavljaju prijetnju ili upotrebu sile protiv teritorijalnog integriteta ili političke nezavisnosti bilo koje države, ili koja je na bilo koji drugi način nespojiva sa ciljevima UN, je nezakonita.''[149]

Ne postoji jedan autoritativan međunarodni dokument koji definiše prijetnju silom i upotrebu sile.

Član 11. *Talin Manuela* definiše upotrebu sile u *cyber* prostoru navodeći da : ,,*Cyber* operacije predstavljaju upotrebu sile kad se njen obim i posljedice uporedivi sa ne-*Cyber* operacijama uzdižu do nivoa upotrebe sile.''

Ovdje se naglašavaju obim i posljedice kao kvantitativni i kvalitativni faktor za definisanje upotrebe sile.

Međunarodni sud pravde u predmetu *Nikaraqua* razlikuje najozbiljnije oblike upotrebe sile koji predstavljaju oružane napade od manje ozbiljnih oblika.[150] Ovakav stav Suda implicira da se svaka nezakonita upotreba sile određenog obima koja je uzrokovala određene posljedice može kvalifikovati kao oružani napad.

Prilikom procjene da li neku situaciju kvalifikovati kao oružani napad države uzimaju u obzir određene faktore: ozbiljnost, neposrednost, direktnost, invazivnost, mjerljivost posljedica, vojni karakter, uključenost države i pretpostavljena legalnost.[151]

Član 12. *Talin Manuela* definiše *cyber* prijetnju na sljedeći način: ''*Cyber* operacija, ili prijetnja *cyber* operacijom, predstavlja nezakonitu prijetnju silom, koja bi ukoliko bi bila provedena, predstavljala nezakonitu upotrebu sile.''

Član 13. *Talin Manuela* potvrđuje pravo na samoodbranu protiv oružanog napada. ''Država protiv koje je usmjerena *cyber* operacija koja se uzdiže do nivoa oružanog

[148] Nuclear Weapons Advisory Opinion, para. 39.
[149] *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 45.
[150] Nuclear Weapons Advisory Opinion, para. 191.
[151] Vidi: *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 49 – 52.

napada može vršiti vlastito urođeno pravo na samoodbranu. Da li jedna *cyber* operacija predstavlja oružani napad zavisi od obima i posljedica.''

5. Pravo država na samoodbranu od oružanog napada

Kao što smo vidjeli član 13. *Talin Manuela* slijedi pravila opšteg međunarodnog prava u pogledu prava država na samoodbranu protiv *cyber* napada.

Član 51. Povelje Ujedinjenih nacija koji predstavlja izvor prava na samoodbranu glasi:

*"*Ništa u ovoj Povelji ne ograničava urođeno pravo na individualnu i kolektivnu samoodbranu u slučaju oružanog napada protiv neke članice Ujedinjenih nacija, dok Savjet sigurnosti ne preduzme mjere potrebne za održavanje međunarodnog mira i sigurnosti. O mjerama koje preduzmu članice pri vršenju tog prava na samoodbranu, odmah će se obavijestiti Savjet sigurnosti, i one neće ni na koji način dovesti u pitanje ovlašćenje i obavezu Savjeta sigurnosti da, na osnovu ove Povelje, preduzme u svakom trenutku korak koji smatra nužnim radi održanja ili uspostavljanja međunarodnog mira i sigurnosti.*"*

Da bi se utvrdilo tačno značenje ovog člana potrebno ga je razmotriti u kontekstu Povelje UN kao i u odnosu prema međunarodnom običajnom pravu. U kontekstu Povelje UN potrebno je prije svega posmatrati ga u vezi sa članom 2. (4) koji obavezuje sve članove UN-a da se u svojim odnosima uzdrže od prijetnji silom ili upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti ma koje države, ili koja bi na ma koji drugi način bila u suprotnosti sa ciljevima Ujedinjenih nacija.

Oružani napad treba biti usmjeren protiv teritorijalnog integriteta ili političke nezavisnosti. Takav oružani napad dopušta izuzetak od opće zabrane upotrebe sile prema Povelji, i daje pravo svakoj državi da pribjegne samoodbrani.

Postoje situacije koje su očigledne i koje državama bez ikakve sumnje daju opravdanje za samoodbranu.

U predmetu *Nicaraqua* Međunarodni sud pravde je koristio definiciju agresije (član 3. g)[152] da bi definisao značenje pojma oružani napad u međunarodnom pravu. Oružani napad mora obuhvatati ne samo upotrebu regularnih oružanih snaga nego i ''slanje od države ili u ime države oružanih bandi, grupa, iregularaca ili plaćenika, koji vrše akte oružanog nasilja protiv druge države takve težine da znače stvarni oružani napad, ili njeno

[152] United Nations General Assembly Resolution 3314 (XXIX). Definition of Aggression. Dostupno na: http://jurist.law.pitt.edu/3314.htm,

bitno učešće u njemu. Ali Sud ne smatra da se pojam oružani napad proteže na pomoć pobunjenicima u formi nabavke oružja ili logističku ili drugu podršku.[153]''

Nakon terorističkog napada od 11. septembra 2001. godine, rezolucijom 1368. od 12. septembra 2001.[154]godine, teroristički napad je označen kao prijetnja međunarodnom miru i sigurnosti u smislu poglavlja VII Povelje UN.

Pravo na država na samoodbranu proteže se i na odbranu od cyber napada. ''Međunarodna grupa eksperata jednoglasno je zaključila da neke cyber operacije mogu biti dovoljno ozbiljne da opravdaju njihovo klasifikovanje kao 'oružani napad' unutar značenja Povelje.[155] Što onda povlači pravo države na samoodbranu u skladu sa Poveljom UN. Ovaj zaključak je u skladu sa mišljenjem Međunarodnog suda pravde datom u predmetu *O zakonitosti upotrebe nuklearnog oružja* gdje se navodi da se: ,,Ove odredbe ne odnose na određeno oružje. One se primjenjuju na bilo koju upotrebu sile, bez obzira na upotrijebljeno oružje''.[156]

Pravo na samoodbranu od *cyber* napada obuhvata i upotrebu dopuštenih kontramjera čiji je cilj da potakne državu povreditelja da prestane sa kršenjem međunarodnopravnih obaveza i da počne poštovati svoje međunarodne obaveze.[157] Pravo na kontramjere traje dok postoji nezakanito ponašanje. Sa prestankom kršenja međunarodnih obaveza prestaje i pravo na kontramjere. Kontramjere moraju biti nužne i proporcionalne te su vremenski ograničene.

Talin Manuel u članu 9. potvrđuje pravo države na kontramjere:

''Država povrijeđena međunarodnim protivpravnim djelom može, protiv odgovorne države, pribjeći proporcionalnim kontramjerama, uključujući i *cyber* kontramjere.''

[153] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986, p 14, para 195.
[154] Resolution S/RES/1368 (2001), Dostupno na: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement, 21.12.2010.
[155] *Talin manuel* o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017. str. 54.
[156] Nuclear Weapons Advisory Opinion, para. 39. https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf. 1.9.2019.
[157] Vidi čl.49. Draft articlies. United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. Pristupio *16*.09.2019.

6. Preduvjeti za postojanje prava na samoodbranu

U pravnoj literaturi je skoro jednoglasno prihvaćeno da je za ostvarenje prava na samoodbranu neophodno ispunjenje uvjeta: neophodnosti (nužde) i proporcionalnosti.

Međunarodni sud pravde u predmetu *Nikaragva* ističe da član 51. "ne sadrži neko specifično pravilo kojim bi samoodbrana garantovala samo mjere koje su proprcionalne oružanom napadu i potrebne da se njima odgovori, pravilo dobro ustanovljeno u međunarodnom običajnom pravu."[158]

Pravila nužde i proporcionalnosti su pravila međunarodnog običajnog prava i njihov sadržaj zavisi od okolnosti svakog konkretnog slučaja. Da li su ti uvjeti ispunjeni cijene prvo, država koja se nađe u situaciji koja zahtijeva pribjegavanje samoodbrani, a zatim i međunarodna zajednica. "Svaka nacija je slobodna u svako vrijeme bez obzira na odredbe ugovora da se brani i jedini sudija u tome šta znači pravo samoodbrane i nužde i šta oni obuhvataju."[159]

Stanje nužde postoji kad je država u odgovoru na oružani napad prinuđena da upotrijebi svoje oružane snage pošto nema drugih sredstava da bi zaštitila neko svoje pravo.

"Običajno pravo o samoodbrani uključuje pretpostavku da upotrijebljena sila mora biti proporcionalna prijetnji."[160] *Proporcionalnost* se mora cijeniti sa potrebnom mjerom fleksibilnosti, jer nema proporcionalnosti ukoliko na povrede granice malog obima država odgovori neproporcionalnim sredstvima, posebno što napadi malog intenziteta često mogu biti proizvod greške ili pogrešno shvaćenog naređenja od nižih komandi.

Talin Manuel propisuje u članu 14. da: ''Upotreba sile koja uključuje *cyber* operacije poduzeta od strane države u ostvarivanju njenog prava na samoodbranu mora biti nužna i proporcionalna.''

U vezi sa pravom na samoodbranu postavlja se pitanje da li je ona moguća i prije nego što se stvarni napad desi. Ovo pitanje je posebno značajno za zemlje koje posjeduju nuklearno oružje odnosno koje bi mogle biti objektom njegovog udara, ali i za druge s obzirom da od prve upotrebe oružja možda zavisi i ishod rata.

Član 51. Povelje, dopušta samoodbranu samo u slučaju postojećeg oružanog napada. U pogledu prava preventivne samoodbrane mišljenja su podijeljena. Dok jedni smatraju da

---

[158] Dinstein, Y. (1994). op. cit. str. 202, nota 124; Vidi također: Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986 .
[159] Brownlie, I. (2003). Ibid., str. 237, nota 4.
[160] Ibid., str. 261.

ne postoji pravo na preventivni rat odnosno anticipatornu samoodbranu, većina pravnih pisaca smatra da međunarodno običajno pravo dopušta ovakvu samoobranu.

Prema *Westlaku*:

"Država se može braniti preventivnim sredstvima ako je po njenoj savjesnoj prosudbi to neophodno protiv napada druge države, prijetnji od napada ili pripremanja ili drugog postupanja iz koga se namjera napada može razumno zaključiti."[161]

Prema *Westlaku*:

"Država se može braniti preventivnim sredstvima ako je po njenoj savjesnoj prosudbi to neophodno protiv napada druge države, prijetnji od napada ili pripremanja ili drugog postupanja iz koga se namjera napada može razumno zaključiti."[162]

Izrael je 1967. godine, izvršio preventivni napad na svoje arapske susjede zbog blokade luke Elijat i zaključenja vojnog pakta između Egipta i Jordana. Značajno je da Ujedinjene nacije u raspravama koje su nakon toga uslijedile nisu osudile ovaj izraelski napad i način ostvarenja samoodbrane. Međunarodni sud u predmetu Nikaragva nije se bavio pitanjem neposredne prijetnje oružanim napadom, pošto ovo pitanje pred njega nije ni stavljeno.

Talin Manuel u članu 15. propisuje: ''Pravo na upotrebu sile u samoodbrani ako se desi cyber oružani napad ili napad neposredno predstoji.''

Sa predhodnim pitanjem povezano je i pitanje da li država može upotrijebiti silu da zaštiti svoje državljane i imovinu u inozemstvu? Do donošenja Povelje UN-a ovo pitanje je bilo van svake sumnje. Stav međunarodnog običajnog prava bio je da države mogu braniti svoje državljane odnosno osobe koje su podlijegale njenoj jurisdikciji kao i imovinu bez obzira gdje se ona nalazila. Ukoliko se oni nalaze na teritoriji odnosne države nije bilo nužno da se primjenjuju odbrambene mjere. Ali ako se oni nalaze na teritoriji druge države, međunarodno običajno pravo je dopuštalo primjenu mjera samoodbrane i na takvoj teritoriji.

Ukoliko posmatramo ovo pitanje u smislu člana 51. Povelje, uočljivo je da on ne dopušta pravo samoodbrane radi zaštite državljana i imovine u inozemstvu. I pored toga većina pravnih pisaca stoji na stanovištu da međunarodno običajno pravo dopušta ovaj vid samoobrane. Što je još značajnije savremena praksa pokazuje da ono još uvijek egzistira u međunarodnim odnosima. Oni koji podržavaju ovo pravo kao uvjet njegovu primjenu

[161] Ibid., str. 257, nota 5.
[162] Ibid., str. 257, nota 5.

vezuju za državljanstvo osoba kao i neposrednu opasnost koja prijeti životima ili imovini. Tako je američki predstavnik na Konferenciji u Havani 1928. godine izjavio:

"Šta da radimo kad vlada padne i u opasnosti su životi američkih građana?... Sada je to princip međunarodnog prava da u takvim slučajevima država ima puno opravdanje da preduzme akciju - ja bih to nazvao uplitanje privremenog karaktera zbog ciljeva zaštite života i imovine državljana.."[163]

Ovo pitanje je isticano posljednih godina u nekolicini primjera. Poznata je američko-belgijska akcija spašavanja talaca u Kongu 1964. godine. "Najpoznatiji incident, međutim, bio je spašavanje talaca od Izraela koje su držali Palestinci i drugi teroristi na *Entebbe*, slijedeći oteti avion francuske kompanije. Debata u Savjetu sigurnosti u ovom slučaju bila je bez zaključaka. Neke države podržavale su izraelski stav da je to bilo zakonito djelovanje u zaštiti njenih državljana u inostranstvu, gdje je lokalna država pomagala otmičarima. Drugi su prihvatili stav da je Izrael počinio agresiju protiv Ugande ili koristio prekomjernu silu."[164]

,,SAD-e su izvršile bombaški napad na Libiju 15. aprila 1986. godine koji je posljedica navodne libijske uključenosti u napad na američke službenike u zapadnom Berlinu. Ovo je pravdano od SAD-a kao akt samoodbrane."[165]

"Britanski ministar vanjskih poslova je zaključio 28. juna 1993. godine da:

'Sila može biti primijenjena u samoodbrani protiv prijetnji nečijim državljanima ako (a) je tu dobar dokaz da bi napadnuti cilj nastavio da se drugdje koristi podrškom druge države u terorističkim napadima protiv nečijih državljana, (b) ako nema drugog efikasnog načina da se preduprijede neposredni dalji napadi na nečije državljene, i (c) ako je upotrijebljena sila proporcionalna prijetnji.'"[166]

Član 51. Povelje UN-a, navodi između ostalog da je pravo na kolektivnu samoodbranu prirođeno pravo svake države. Ova ideja se dalje razvija u članu 52. gdje stoji da (ova) Povelja ničim ne isključuje postojanje regionalnih sporazuma ili ustanova čija je svrha bavljenje pitanjima koja se tiču održanja međunarodnog mira i sigurnosti i koja su podesna da budu predmet regionalne akcije, pod uvjetima da su ti sporazumi i ustanove i njihovo djelovanje u skladu sa ciljevima i načelima Ujedinjenih nacija.

---

[163] Bowett, D. W. (1958). Ibid., str. 99 - 100, nota 1.
[164] Shaw, N. M. (1997). International Law. Cambridge: University Press. str. 792, nota 84, 85. i 86.
[165] Ibid., str. 793. nota 90.
[166] Ibid., str. 793. nota 92.; "Prema Waldoku uvjeti za primjenu sile za zaštitu državljana u inostranstvu su: (1) Neposredna prijetnja štete državljanima, (2) Propust ili nesposobnost na strani teritorijalnog suverena da ih zaštiti, (3) Mjere zaštite su strogo ograničene na objekat koji se štiti od povrede." Dinstein, Y. (1994). Ibid., str. 226. nota 51.

Talin Manuel propisuje: ''Pravo na samoodbranu može se ostvarivati kolektivno. Kolektivna samoodbrana protiv *cyber* operacija znači da oružani napad može biti izvršen na zahtjev države žrtve i u okviru zahtjeva.''[167]

7. Samodbrana protiv terorizma

Kao odgovor na teroristički napad od 11. septembra Sjedinjene Američke Države pokrenule su vojnu kampanju protiv Avganistana poznatu kao Operacija trajne slobode (engl. *Operation Enduring Freedom*)[168] 7. oktobra 2001. godine. Prilikom informisanja Savjeta sigurnosti o poduzetim akcijama SAD su tvrdile da postupaju u samoodbrani. Velika Britanija se također pozvala na individualnu i kolektivnu samoodbranu. Uprkos ranijim dilemama po pitanju prava na samoodbranu protiv proteklih terorističkih napada, ove akcije naišle su na opštu podršku. Rezolucija Savjeta sigurnosti 1368 od 12. septembra 2001. godine, izričito je priznala pravo na samoodbranu protiv terorizma. Kasnija Rezolucija 1373 od 14. novembra 2001. godine,[169] također se poziva na individualno i kolektivno pravo na samoodbranu.

Ovdje se očito radi o proširenju tradicionalnog modela prava država na samoodbranu kako je to propisano Poveljom UN. Ali pošto se radi o opštoj podršci pravu na samoodbranu u slučaju terorističkog napada na djelu je reinterpretacija odredaba Povelje stvaranjem instant međunarodnog običaja koji to dopušta.

''Sada je očigledno prihvaćeno da je teroristički napad na državnu teritoriju od nedržavnih počinitelja, oružani napad koji opravdava odgovor protiv države koja pruža utočište odgovornim.''[170] Povodom ovog napada NATO se po prvi put pozvao na član 5. osnivačkog ugovora koji propisuje da će se napad na jednu državu članicu smatrati napadom na sve njih.

Sjedinjene Američke Države i Velika Britanija smatraju da imaju pravo i na anticipatornu i preventivnu samoodbranu protiv terorizma. Ovo pravo je prihvaćeno od velikog broja država ali samo u odnosu na terorističku prijetnju ali ne i izvan toga. Ali i u tom pogledu uslov je da Savjet sigurnosti svojom rezolucijom utvrdi postojanje terorističke prijetnje.

Talin Manuel u članu 36. propisuje: ''*Cyber* napadi ili prijetnja cyber napadima, čiji je primarni cilj teror među civilnim stanovništvom, su zabranjeni.'' Na ovaj način *Talin Manuel*

---

[167] Talin manuel, član 16.
[168] Operation Enduring Freedom , Dostupno na: http://www.history.army.mil/brochures/Afghanistan/Operation%20Enduring%20Freedom.htm, 23.12.2010.
[169] Security Council Resolution S/RES/1373 (2001), Dostupno na: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement, 23.12.2010.
[170] Gray, C. The use of force and the international legal order. U Evans. M. D. (ed.). (2003). International Law. Oxford: University Press. str. 604.

prepoznaje *cyber* napade kao teroristički akt i kao terorističku prijetnju na koju se primjenjuju ista pravila kao na bili koju drugu terorističku prijetnju.

8. Zaključak

Cyber napadi su po svojoj sadržini vrsta oružanih sukoba. Primjena prava oružanih sukoba ne zavisi od klasifikacije oružanog sukoba niti od vrste vojnih operacija i korištenih metoda ratovanja. Stoga *cyber* operacije mogu same, bez prisustva drugih vrsta operacija značiti i međunarodni i nemeđunarodni oružani sukob.

Pravo oružanih sukoba se primjenjuje na sve aktivnosti poduzeta tokom trajanja oružanog sukoba i na sve posljedice nastale na teritoriji država koje su uključene u oružani sukob ne ograničavajući se samo na prostor gdje se vrše vojne operacije.

Da bi *cyber* napadi predstavljali napade relevantne za pravo oružanih sukoba moraju biti takve težine i uzrokovati fizičku destrukciju ili štetne povrede kao i druge vrste oružja: konvencionalno, nuklearno, hemijsko i biološko. Odnosno, potrebno je da cyber napad uzrokuje iste posljedice kao i druge vrste napada ili da je napad usmjeren protiv bilo čega što se zove kritična infrastruktura.

Cyber napadi podliježu primjeni pravila *jus ad bellum* koja se odnose na pravo države na upotrebu sile u cilju realizacije svoje nacionalne politike. Također podliježu primjeni pravila *jus in bello* kojima se reguliše način vođenja oružanih sukoba.

Za primjenu prava oružanih sukoba na *cyber* ratovanje nisu neophodni neki novi izvori prava. Na *cyber* napade se primjenjuju postojeći pravni izvori: međunarodni ugovori, međunarodni običaji i opća pravna načela.

Sve suverene države su na osnovu prava na jurisdikciju ovlaštene vršiti kontrolu nad *cyber* infrastrukturom i *cyber* aktivnostima unutar svoje teritorije.

Posljedice suverenosti države nad cyber infrastrukturom su da je *cyber* infrastruktura podvrgnuta pravnoj i regulatornoj kontroli odnosne države i da državni suverenitet štiti takvu infrastrukturu.

Cyber napad ili ozbiljna prijetnja cyber napadom od strane jedne države usmjeren protiv *cyber* infrastrukture druge države predstavlja povredu njene suverenosti što povlači odgovornost države za međunarodne protivpravne akte. Generalno pravilo je da samo ponašanje državnih organa ili njenih agenata može biti pripisivo državi.

Država koja je meta cyber napada ima pravo na samoodbranu u skladu sa Poveljom UN uz obavezu poštovanja prava nužde i proporcionalnosti.

U vezi sa preventivnim pravom na samoodbranu mišljenja su podijeljena. Ali ipak prevladava stav o njenoj opravdanosti i zakonitosti.

Literatura:

Knjige i članci:

1. Akehurst's modern introduction to International Law, seventh revised edition, 1997. London and New York: Routledge.
2. Brownlie, J: International Law and the use Force by States, Oxford University Press 1963.
3. Bowett, D. W.: Self - Defence in International Law, Manchester University Press, 1958.
4. Carter/Trimble/Bradley. *(2003) International Law*, forth edition. New York: Aspen Publisher. Dinstein, Y.: War, Agression and Self -Defence, Cambridge University Press, 1994.
5. Harris (2004) Cases and Materials on International Law, sixth edition. London: Thomson, Sweet§Maxwell.
6. Mateusz Piatkowski, The Definition of the Armed Conflict in the Condition of Cyber Warfera, Polish politikal Science Yearbook vol. 46 (2017) pp. 271 – 280.
7. Michael N Smitt, ''Attack'' as a Term of Art in International law: The Cyber Operations Context. 2012 4thInternational Conferenc on Cyber Conflict. (283-293).
8. Softić, S. (2012). *MEĐUNARODNO PRAVO.* Sarajevo: DES doo - Sarajevo.
9. Shaw, N. M. (2008) International Law, sixth edition, Cambridge: Cambridge University Press.

Drugi izvori:

1. Talin manuel o međunarodnom pravu koje se primjenjuje na *cyber* ratovanje. General editor Michael N Schmitt. Cambridge University Press 2017.
2. International Court Of Justice Reports Of Judgments, Advisory Opinions And Orders Legality Of The Threat Or Use Of Nuclear Weapons Advisory Opinion Of 8 July 1996.
3. United Nations A/RES/56/83 from 28 January 2002. Responsibility of States for internationally wrongful acts. http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
4. Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, ICT Reports 1986.
5. Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004).