MEĐUNARODNA ODGOVORNOST DRŽAVE U DIGITALNOM (SAJBER) PROSTORU

Ljubomir TINTOR*

APSTRAKT

Sajber prostor je domen čije je korišćenje neophodno za celu ili bar značajan deo globalne populacije. Svedoci smo da je sajber prostor zbog svoje specifičnosti pogodan za hakerske napade na države. Uživanje ljudskih prava takođe može biti ograničeno ili onemogućeno usled hakerskih napada. Sajber prostor dovodi u pitanje opšta načela međunarodnog prava uključujući suverenitet, neintervenciju i jurisdikciju. Sve ovo otvara pitanje međunarodne odgovornosti države u sajber prostoru. U radu će najpre biti ukazano na specifičnosti sajber prostora. Potom će se analizirati mogućnost uspostavljanja međunarodne odgovornosti u sajber prostoru s obzirom na specifičnosti elementa pripisivosti usled čega će biti razmotren i značaj principa dužne pažnje kao alternative za uspostavljanje odgovornosti. Na kraju biće sagledano koje obaveze ima država u pogledu zaštite ljudskih prava u sajber prostoru. U zaključnim razmatranjima ponudiće se potencijalna rešenja za uočene probleme.

Ključne riječi: Sajber prostor, međunarodna odgovornost države, princip dužne pažnje, zaštita ljudskih prava

UVOD

Digitalni prostor je postao sastavni deo svakodnevnog života, a razvoj digitalne tehnologije pruža nove mogućnosti, ali i nove izazove za međunarodno pravo. S obzirom na brzi razvoj digitalne tehnologije, međunarodno pravo se suočava sa stalnom potrebom da trenutne međunarodne pravne okvire prilagodi kako bi se osigurala efikasna zaštita ljudskih prava i sigurnost u digitalnom prostoru. Primetno je da se sajber prostor pokazao kao idealna meta za napade hakerskih grupa na države. Sajber prostor ima sve veći značaj za međunarodnu

* Istraživač saradnik na Institutu za uporedno pravo. E mail: lj.tintor@iup.rs , ORCID 0009-0005-7565-154X. Rad je nastao kao rezultat naučnoistraživačkog rada Instituta za uporedno pravo koji finansira Ministarstvo nauke, tehnološkog razvoja i inovacija Republike Srbije prema Ugovoru o realizaciji i finansiranju naučnoistraživačkog rada NIO u 2023. godini (evidencioni broj: 451-03-47/2023-01/200049 od 3. 2. 2023).

bezbednost jer je postao centar svetske ekonomije, društva i politike. Ovaj prostor omogućava zemljama da komuniciraju i razmenjuju informacije brzo i efikasno, ali takođe predstavlja rizik za bezbednost država.Sajber napadi, krađa podataka i druge nezakonite aktivnosti u sajber prostoru mogu da izazovu veliku ekonomsku štetu, utiču na stabilnost finansijskih sistema, naruše javnu bezbednost i zaštitu i predstavljaju pretnju. Iz tog razloga, sajber bezbednost se smatra jednim od glavnih izazova savremenog sveta, a međunarodna zajednica preduzima napore da obezbedi bezbednost u sajber prostoru. Sajber prostor se pokazao kao vrlo pogodan za preduzimanje vojnih operacija i kao prostor za novi oblik konflikata poznat kao sajber ratovanje. Uživanje ljudskih prava takođe može biti ograničeno ili onemogućeno usled hakerskih napada. Sajber prostor dovodi u pitanje opšta načela međunarodnog prava važna za ljudska prava, uključujući suverenitet, neintervenciju i jurisdikciju države. Sajber prostor je alat u kome pojedinci mogu da ostvare svoja ljudska prava, ali sajber prostor ne može da garantuje našu slobodu. Sve ovo otvara pitanje međunarodne odgovornosti države u digitalnom prostoru. Jedno od ključnih pitanja na koje treba dati adekvatan odgovor je kako primeniti norme međunarodnog prava u digitalnom prostoru. Međunarodno pravo je razvijeno za primenu u tradicionalnom međunarodnom okruženju i nije uvek primenljivo u sajber prostoru. Međunarodno pravo se bavi pitanjima kao što su teritorijalni suverenitet, upotreba sile i zaštita ljudskih prava, ali ne postoje precizna pravila o primeni ovih principa u sajber prostoru. Iz tog razloga posebna pažnja se posvećuje razvijanju međunarodno-pravnog okvira koji će omogućiti saradnju među državama u borbi protiv sajber kriminala i drugih nezakonitih aktivnosti u sajber prostoru. Prvo će u radu biti ukazano na specifičnosti sajber prostora. Potom će se u radu analizirati mogućnost uspostavljanja odgovornosti u sajber prostoru s obzirom na specifičnosti elementa pripisivosti, zatim biće ukazano i na značaj primene principa dužne pažnje za uspostavljanje odgovornosti. Peti deo rada baviće se obavezama države da zaštite ljudska prava u sajber prostoru i odgovornosti za propuste. U zaključnim razmatranjima ponudiće se potencijalna rešenja za uočene probleme imajući u vidu da je ovo oblast međunarodnog prava koja će se rapidno razvijati.

DEFINISANJE (SAJBER) DIGITALNOG PROSTORA I NJEGOVE SPECIFIČNOSTI

Sajber (digitalni) prostor je virtuelni komunikativni prostor kreiran digitalnim tehnologijama.[1] Ovaj prostor nije ograničena na rad računarskih mreža, već obuhvata i sve društvene aktivnosti u kojima se primenjuju digitalne informaciono-komunikacione tehnologije. Sajber prostor je termin koji je nastao zajedno sa pojmom interneta i odnosi se na svet na mreži kao na svet razdvojen

[1] Termin „sajber prostor" prvi put je upotrebio pisac naučne fantastike Vilijam Gibson (William Gibson) u noveli Burning Chrome iz 1982. godine.

od svakodnevne stvarnosti.[2] Termin sajber prostor postao je konvencionalno sredstvo za opisivanje svega što je povezano sa internetom i raznolikom internet kulturom. Iako se u naučnoj literaturi i u zvaničnim vladinim izvorima može pronaći nekoliko definicija sajber prostora, još uvek ne postoji potpuno usaglašena zvanična definicija. Američko ministarstvo odbrane (*Department of Defence – DoD*) definiše sajber prostor kao „područje u informacionom okruženju koji se sastoji od nezavisnih mreža informacionih infrastruktura, uključujući Internet, telekomunikacione mreže, računarske sisteme, ugrađene procesore i kontrolere" odnosno „zamišljeno okruženje u kojem se digitalni podaci prenose pomoću računarskih mreža"[3] Benedikt (*Michael Benedikt*) sajber prostor definiše kao „novi univerzum, paralelni stvoren univerzum, koji je održavan pomoću 'svetskih računara' i komunikacionih linija".[4] Sa druge strane Hjuz (*Kevin Hughes*) je definisao sajber prostor kao „međusobno povezano računarsko okruženje koje predstavlja sve prethodno kreirane medije".[5] Jedna od najprihvatljivih definicija je da se sajber prostor sastoji od tri sloja: fizičkog sloja sastavljenog od sajber infrastrukture, drugi sloj softverske logike i treći sloj podataka.[6] Sajber prostor se razlikuje od tradicionalnih oblika prostora po tome što ne postoji jasna teritorijalna granica, niti fizički oblik. On je takođe karakterističan po tome što omogućava anonimnu i brzu razmenu informacija, što može biti i prednost i nedostatak, u zavisnosti od konteksta. Ono što je jedna od osobenosti sajber prostora je da se ljudi mogu sakriti iza lažnih identiteta i na taj način pokušati da nekažnjeno nanose štetu drugoj državi. Sajber prostor je heterogen i kompleksan, što predstavlja izazov za regulisanje i zaštitu prava i bezbednosti u tom prostoru. Sajber prostor je više definisan društvenim interakcijama nego njegovom tehničkom implementacijom. Procenjuje se da sajber prostor ima više pojedinaca nego bilo koja druga zemlja na svetu, ali da je bez ikakve centralizovane uprave ili bilo koje vrsti normi što usled čega nastaju poteškoće u zaštiti ljudskih prava. Fizička infrastruktura koja podržava Internet i sajber aktivnosti se uglavnom nalaze na suverenoj teritoriji i podležu jurisdikcija teritorijalne države. Zbog međusobno povezanih, interoperabilne prirode sajber prostora, operacije koje ciljaju na

[2] Cyberspace Definition of cyberspace in US English by Oxford Dictionaries. Internet: https://web.archive.org/web/20130218185858/http://oxforddictionaries.com/us/definition/american_english/cyberspace, 01.08.2023.

[3] Joint Publication 1-02, DoD Dictionary of Military Terms, Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7, October 17, 2008. www.dtic.mil./doctrine/jel/new_pubs/1_02.pdf, 01.03.2023.

[4] Michael Benedikt (Ed.), Introduction and Cyberspace: some proposals, in Cyberspace, First Steps, MIT Press, London, 1992, pp. 119-133.

[5] Volker Schneider, Dirk Hyner, *The Global Governance of Cybercrime: Issue Space and the Transnational Policy Network*, University of Konstanz, Germany, 2003, p. 4.

[6] Lior Tobanksy, "Basic concepts in cyber warfare", *Military and Strategic Affairs,* 2011, Vol. 3, pp.75–92.

umrežene informacione infrastrukture u jednoj zemlji mogu stvoriti efekte u drugoj zemlji.[7] Još jedna specifičnost sajber prostora da on prevazilazi državne granice, iako neke države poput Kine promovišu sajber suverenitet .[8].Kineski pristup sajber suverenitetu proteže se na sajber infrastrukturu pod njenom jurisdikcijom, nad svim aktivnostima na mreži koje se odvijaju unutar kineske jurisdikcije i nad ljudima unutar njih jurisdikcija Kine. Pored toga, suverenitet se proteže na informacije koje ulaze ili postaju dostupne unutar suverenog domena Kine.[9] Teorijski prihvatljivije bi bilo sajber prostor posmatrati kao globalno zajedničko dobro. Globalno dobro podrazumeva da je u pitanju resurs koji je pod internacionalizovanim vlasništvom kao što je na primer morsko dno pod upravom Vlasti koja simbolizuje međunarodnu upravu.[10] Međutim za sada sajber prostor nije dobio nikakav poseban status u međunarodnom pravu, iako smo ukazali na određene specifičnosti. Iako preovladava stav da je suverenitet prihvaćen nad sajber prostorom još uvek postoje različita tumačenja njegovog obima. Primena principa državnog suvereniteta u sajber prostoru ima svoje glavno obrazloženje u činjenici da vrhovni organi države moraju da regulišu bilo koju sajber infrastrukturu koja se nalazi na njenoj teritoriji. Fizički sloj sajber prostora je stoga podložan suverenitetu teritorijalne države, dok virtuelni domen sajber prostora ne potpada pod suverenitet određene države prema trenutnom shvatanju. Državni suverenitet u sajber prostoru predstavlja složen problem koji zahteva međunarodnu suradnju i uspostavu novih pravila i standarda u digitalnom okruženju kako bi se osigurala sigurnost, stabilnost i zaštita prava u sajber prostoru. Očigledno da će se pitanju suvereniteta u digitalnom prostoru u budućnosti morati posvetiti veća pažnja kako bismo dobili čvršća pravila i ujednačenija shvatanja.Kada se govori o sajber prostoru neophodno je naglasiti da u njemu deluju različiti akteri poput Timova mamaca (*troll army*) su subjekt, sponzorisani od strane države, koji koristeći lažne identitete učestvuju u blogovima, internet forumima i društvenim mrežama u cilju propagande, formiranja percepcije javnog mnjenja, podrivanja disidentskih struktura.[11] Drugu

[7] Harold H Koh, "International Law in Cyberspace", *Harvard International Law Journal,* 2012, Vol 54, No. 1, p. 6,

[8] Nart Villeneuve, "Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online" in Ronald Deibert, *et al,* Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, *MIT Press*, 2010, p. 57. Druga mogućnost stvaranja suvereniteta nad sajber prostorom je odvajanje nacionalnih mreža ka čemu teže neke države poput Irana i Rusije.

[9] *Ibid.*

[10] Moderna instancija koncepta globalnog zajedničkog dobra može se naći u članovima 87, 89. i 139. Konvencije Ujedinjenih nacija o pravu mora iz 1982. godine. Videti: United Nations Convention on the Law of the Sea (signed 10 December 1982).

[11] Patrick Duggan, "Harnessing cyber-technology's human potential", *Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School,* 2015, Vol. 28 Issue 4, p. 14.

grupu značajnih aktera u sajber prostoru čine timovi za formiranje grupnog mišljenja (*swarm stream teams*) su agresivno orijentisana grupa ljudi koja preko sajber prostora širi viralni (virusni) video s ciljem formiranja kolektivnog mišljenja.[12] Praksa država po tome što su smatrale da su sve sajber operacije koje utiču na kompjuterske sisteme u inostranstvu kršenje teritorijalnog suvereniteta država.[13]

PROBLEM PRIPISIVOSTI U SAJBER PROSTORU KAO USLOV MEĐUNARODNE ODGOVORNOSTI

Izvršenje sajber operacije podrazumeva umešanost jednog ili više ljudskih izvršilaca i kompjuterskih sistema. U jednu ruku, kompjuterski sistemi se mogu koristiti za kreiranje, pokretanje ili tranzit sajber operacije. S druge strane, uvek je čovek uključen u vršenje sajber operacija, čak i kada one podrazumevaju veliki nivo automatizacije.Akteri u sajber prostoru su države, pojedinci, drugi nedržavni akteri i njihovi punomoćnici.[14] Štetne međunarodne sajber operacije mogu se klasifikovati u različite vrste. Prvo, štetna prekogranična sajber aktivnost može biti označena kao sajber kriminal, delo počinjeno sa kriminalnom namerom i kao špijunaža.[15] Međunarodna odgovornost države nastala je po analogiji iz privatnog prava i dugo se razvijala kroz istoriju. Svoje osnovne elemente dobija kroz slučaj *Factory at Chorzów* koji se pojavio pred Stalnim međunarodnim sudom pravde, u kom je naznačeno da je za uspostavljanje međunarodne odgovornosti države neophodno da je došlo do povrede međunarodne obaveze i da se protivpravan akt može pripisati države.[16] Ova pravila su dosta kritikovana jer odgovornost država ne posmatra kao isključivu obrazac bilateralnih odnosa između počinioca i oštećene države. Odgovornost države dobija javnu dimenziju jer naglasak se stavlja na protivpravnost dela, a ne na nastalu štetu ili posledice prema žrtvi.[17] Atribucija ili pripisivost je pravno-tehnička operacija povezivanja uzročne veze između

[12] *Ibid*. p. 15

[13] *Ibid*.

[14] Jason Andress, Steve Winterfeld, Lillian Ablon*, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Elsevier, 2014, pp.83-101.

[15] Štetna međunarodna sajber operacija se takođe može identifikovati kao sajber napad. To je namerna akcija,politički ili strateški motivisani, preuzeti korišćenjem računarskih mreža da ometaju, manipulišu ili uništavaju informacije koje se nalaze u ciljnom informacionom sistemu.

[16] "The Factory at Chorzów Claim for Indemnity-Germany v. Poland", PCIJ, 1928, Ser. A, No 17, para. 29. Ovaj stav je prihvaćen i u članu 2 Nacrta pravila o odgovornosti države za protivpravan akt. Videti: "International Law Commission (ILC) Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries", Official Records of the General Assembly, Fifty-sixth session, Supplement, 2001, No 10 (A/56/10)", art.2.

[17] Postoje stavovi u doktrini međunarodnog prava da je pored pomenutih elemenata u Pravilima neophodno i postojanje štete kao i odsustvo osnova za isključenje protivpravnosti.

kršenja međunarodne obaveze i aktivnosti (propusta) države. Pripisivanje se odnosi na dodeljivanje dela državi. Prema trenutno važećim pravilima međunarodnog prava država bi odgovarala ako se dokaže aktivnom učešću državnih službenika u sajber napadima jer se radnje zakonodavnih, izvršnih i sudskih organa pripisuju državi. Država je odgovorna za ponašanje nedržavnog aktera koje nanosi štetu drugoj državi samo ako ponašanje može se pripisati državi. Prema međunarodnom pravu, sajber operacija nedržavnog aktera može se pripisati državi, posebno u sledeće tri okolnosti. Kada sajber čin izvrši lice ili entitet ovlašćen od strane države da vrši javna ovlašćenja.[18] Sajber operacija se smatra činom države ako država izričito priznaje i usvaja operaciju kao svoju. Obaveza sprečavanja štetnih međunarodnih operacije se takođe primenjuju u odnosu na one operacije pokrenute iz sajber infrastrukture koja je izvan teritorije države, ali je ipak pod isključivom kontrolom država, na primer u vojnom postrojenju u stranoj zemlji, na platformi na otvorenom moru ili u međunarodnom vazdušnom prostoru, ili u diplomatskim prostorijama.[19] Atribucija je generalno veoma zahtevna i komplikovana radnja i to je još vidljivije u sajber prostoru zbog prirode sajber domena. Atribucija je generalno veoma zahtevna i komplikovana radnja i to je još vidljivije u sajber prostoru zbog prirode sajber domena. Prva karakteristika sajber prostora koja otežava pripisivost je anonimnost, da autori sajber operacija mogu sakriti svoj identitet. Specifičnost u sajber prostoru je ogromno prisustvo aktivnih i sofisticiranih nedržavnih aktera.[20] Ovi akteri u velikoj meri nalaze se izvan dosega članova o odgovornosti države i tako uživaju relativan stepen nekažnjivosti za štetne posledice svojih sprovesti. Drugi uočeni problem je višestruka radnja tačnije problem da se protivpravni akt može izvršiti paralelno sa više računarskih mreža koje mogu biti smeštene u više država dakle nalaziti se pod više različitih jurisdikcija. Treći uočeni problem je brzina kojom se može izvršiti protivpravan akt u sajber prostoru i sam obuhvat napada. Da bi se pripisala odgovornost državi za akte privatnih lica neophodno je da su oni bili pod kontrolom države mada nije jasno utvrđeno koji stepen kontrole je dovoljan, efektivna ili opšta kontrola. Ako bi se standardi o pripisivosti koje su primenjivali međunarodni sudovi u dosadašnjim slučajevima koristili, u sajber prostoru teško da bi smo mogli dobiti adekvatne rezultate.[21] Iako ideja koncepta opšte kontrole izgleda privlačno ovaj

[18] International Law Commission (ILC) Draft *op.cit*., Art. 5

[19] Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace", In: K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace,* Tallinn: NATO CCD COE Publication 2013, pp. 189–216.

[20] Michael N Schmitt, "Grey Zones in the International Law of Cyberspace", *Yale Journal of International Law Online,* 2017, Vol. 42, p. 11.

[21] Grupe koje su u Gruziji (2008.godine) i Estoniji (2007.godine) izvršili sajber napade nisu se mogle povezati sa državom jer oni nisu označeni kao državni organi po ruskim zakonima i nisu u stanju potpuna zavisnost od vlasti. Štaviše, oni nisu delegirani da vrše državna ovlašćenja. Videti: I. Traynor, Russia accused of unleashing cyberwar to disable Estonia. *The Guardian.* Internet: https://www.theguardian.com/world/2007/may/17/topstories3.russia, 22.03.2023.

koncept je doveden u pitanje različitim tumačenjem praga potrebne kontrole Haškog tribunala za bivšu Jugoslaviju[22] i Međunarodnog suda pravde. Test efektivne kontrole (a ne ukupne kontrole) države nad aktivnostima privatnih grupa je u skladu sa ustaljenom jurisprudencijom, jer bi sprečio države od neozbiljnog optuživanja za sajber napade. Ovo je naročito značajno ako država koja je napadnuta želi da ovaj sajber napad iskoriste za protivudar u vidu samoodbrane.[23] Država bi prema odredbama Pravila međunarodne odgovornosti države za protivpravan akt mogla odgovarati za postupke privatnih lica ukoliko je pružala instrukcije za vršenje sajber napada. Kada se govori o sajber prostoru treba imati na umu da operacije koje sprovodi organ države koji je stavljen na raspolaganje drugoj državi mogu se pripisati ovoj potonjoj kada organ deluje u vršenju elemenata vlasti države na čijoj teritoriji deluje.[24] Država je odgovorna za pomoć drugoj državi u izvršenju međunarodno protivpravnog dela kada država pruža pomoć ili pomoć znajući za okolnosti međunarodnog protivpravnog dela i delo bi bilo međunarodno protivpravno da ga je sama počinila, kao i u situaciji kad kontroliše ili primorava drugu državu.[25] Pravila o pripisivosti ne odražavaju iskustva država o proksi ratovima koje vode nedržavni akteri u sajber prostoru.[26] Tri komponente atribucije pripisivanje mašini,pripisivanje čoveku i pripisivanje državi su nezavisni jedni od drugih. Identifikacija računarskog sistema možda neće pomoći da se identifikuje ljudski počinilac ili država koja sponzoriše sajber operacija.[27] U nekim slučajevima, identifikacija čoveka iza mašine Operacija je prvi korak ka identifikaciji države sponzora, ali nije preduslov. U svakom slučaju, pripisivanje odgovornosti državi nije sama sebi svrha, to je pre sredstvo za postizanje cilja Jedna velika razlika između sajber prostora i realnog prostora je u

[22] "Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)", Judgment, ICJ Reports 2007: 43. Internet: https://www.icj cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf , 07.03.2023.

[23] Marco Roscini, "World Wide Warfare – Jus ad bellum and the Use of Cyber Force", *(eds.), A. von Bogdandy and R. Wolfrum in* Max Planck Yearbook of United Nations Law , Martinus Nijhoff, 2010, Vol. 14, pp. 85-130.

[24] International Law Commission (ILC) Draft *op.cit* art. 17.

[25] *Ibid.* art 18.

[26] Proksi serveri omogućavaju korisnicima da sakriju svoju IP adresu tuneliranjem svih specifičnih tipova saobraćaja preko drugog servera, a host kojem se pristupa ne mora biti veb server. Postoji i drugi metod je korišćenje anonimnih mreža sa tehnikom „rutiranja luka", korišćenjem više javnih ili privatnih proksi servera za prenošenje šifrovanih podataka preko mnogih nasumično odabranih čvorova na mreži anonimnosti sa više slojeva enkripcije primenjene na prenete podatke, tako se podaci dešifruju do konačnog korisnika kome su namenjeni.

[27] Pripisivanje mašini ili ljudskom počiniocu može čak biti važno ključno u nekim slučajevima, za utvrđivanje da li je sajber operacija sponzorisana ili sprovedena od strane države. François Deleure, *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020. pp. 353–376.

tome što u sajber prostoru pojedinci mogu delovati kao potpuno samodovoljni entiteti, te im nije potreban bilo kakav oblik državne pomoći i kontrole. Sajber oružje u obliku virusa i njihove ekvivalente mogu izmisliti nedržavni akteri, oni su lako nabavljivi. Sajber-grupa može da deluje na koordinisan način ili da primaju naređenja od virtuelnog rukovodstva, ali je jako teško utvrditi od koga primaju informacije i lanac komande može biti veoma raširen. Sajber napadi mogu biti veoma lako preusmereni što otežava pripisivost, koja su zasnovano na konvencionalnim shvatanjima okruženja kroz koje deluju otelotvoreni entiteti fizičke radnje u stvarnom svetu. Specifičnost kod sajber prostora je u tome što se pripisivost protivpravnog dela vrši na osnovu lociranja *IP* adrese, koja identifikuje njegovu tačnu lokaciju. Stoga se čini da se međunarodno protivpravno delo u sajber prostoru pripisuje određenom računaru, dok se identitet osobe koja njime koristi dok se lice koje upravlja može samo pretpostaviti, značajno povećava sposobnost aktera da se uključi u napade sa „verovatnim poricanjem", delujući preko zastupnika i sugerisao da je ovaj izazov „više pitanja tehničke i političke prirode nego isključivo ili pretežno pitanje prava. U svrhu atribucije u sajber prostoru, mora se identifikovati izvor komunikacije prelaskom preko rute kojom komunikacija može doći uz obavezu identifikovanja lica ili entiteta koji stoji iza toga, i da li je to lice/entitet usmeravano ili kontrolisano od strane drugog lica, entiteta ili države.[28] Stav SAD u vezi sa „proksi akterima" u sajber prostoru je u skladu sa testom efektivne kontrole.[29] Čini se da nova praksa država u reagovanju na sajber operacije koje sponzoriše država pokazuje da su države sve više svesne svoje optužbe treba da potkrepe dokazima da države, a ne individue stoje iza sajber napada. Neki počinioci su čak ubacili pogrešne nagoveštaje u kompjuter kod virusa u pokušaju da se krivica prebaci na treću stranu. Države se sve više oslanjaju na međunarodne komisije za utvrđivanje činjenica nakon međunarodnih incidenata koji su možda doveli do međudržavnih sporova, a ovaj razvoj se ogleda u različitim granama i aspektima međunarodnog prava.[30] U svakom slučaju, pripisivanje odgovornosti državi nije sama sebi svrha, to je pre sredstvo za postizanje cilja. Jedna velika razlika između sajber prostora i realnog prostora je u tome što u sajber prostoru pojedinci mogu delovati kao potpuno samodovoljni entiteti, te im nije potreban bilo kakav oblik državne pomoći i kontrole. Sajber oružje u obliku virusa i njihove ekvivalente mogu izmisliti nedržavni akteri, oni su lako nabavljivi. Sajber-grupa može da deluje na koordinisan način ili da primaju naređenja od

[28] Ovo uključuje lociranje IP adrese ili adresa, određivanje tačke kontakta i namamljivanje hakera da otkrije više detalja o svom identitetu. Što je haker veštiji, to je manje uspešno praćenje postaje teže.

[29] Države su zakonski odgovorne za aktivnosti koje se preduzimaju preko „proki aktera", koji deluju po njima uputstvima države ili pod njenom upravom ili kontrolom. "International Law in Cyberspace", US Department of State, US CYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18 Sept. 2012.

[30] Joseph C. Witenberg, "La théorie des preuves devant les juridictions internationales", RCADI, Vol. 56, No. 1, 1936, pp. 6–7.

virtuelnog rukovodstva, ali je jako teško utvrditi od koga primaju informacije i lanac komande može biti veoma raširen. Sajber napadi mogu biti veoma lako preusmereni što otežava pripisivost, koja su zasnovano na konvencionalnim shvatanjima okruženja kroz koje deluju otelotvoreni entiteti fizičke radnje u stvarnom svetu. Specifičnost kod sajber prostora je u tome što se pripisivost protivpravnog dela vrši na osnovu lociranja *IP* adrese, koja identifikuje njegovu tačnu lokaciju. Stoga se čini da se međunarodno protivpravno delo u sajber prostoru pripisuje određenom računaru, dok se identitet osobe koja njime koristi dok se lice koje upravlja može samo pretpostaviti, značajno povećava sposobnost aktera da se uključi u napade sa „verovatnim poricanjem", delujući preko zastupnika i sugerisao da je ovaj izazov „više pitanja tehničke i političke prirode nego isključivo ili pretežno pitanje prava. Ali atribucija je pretežno pitanje zakona i ono se ne utvrđuje „na osnovu pukog priznavanja veze činjenične uzročnosti".[31] Sajber operacije mogu biti jedinstveno složene, skupe i dugotrajne. Višestepene sajber operacije predstavljaju jedan od glavnih izazova uproces identifikacije sajber operacija. Postoji mnogo različitih oblika višestepenih sajber operacija. Shodno tome, ne postoji konsenzus o velikim sajber napadima i njihovom povezanošću sa državom. Preovladavajuća pretpostavka iz današnje perspektive je da će se pitanje pripisivosti u sajber prostoru biti rešena novim tehnološkim rešenjima.[32] Ako sajber operaciju pokrenu privatni akteri sa nekim nivoom države umešanosti, kako bi se ta operacija pripisala upravo državi koji nivo učešća države će biti potreban. Dodatna komplikacija kod pripisivanja u sajber prostoru može nastati kada sajber operaciju ponovo pokrenu privatni akteri sa teritorije države, ali ovaj put je država preduzela neophodne mere da spreči (iako bez uspeha) dotične operacije može proizvesti međunarodnu odgovornost države. Uprkos navodima da su nedržavni akteri, kao i koordinirani transnacionalni sajber akteri kao što je *Anonimous,* učestvovali u velikim sajber operacijama unutar država kao što su SAD, Rusija, Kina, Izrael, ostaje upitno ko će snositi odgovornost za štetu koju oni pričine. Država bi mogla odgovarati samo ako se dokaže da ove grupe imaju javna ovlašćenja koja im je poverila ili ukoliko je u potpunosti kontrolisala njihove aktivnosti.[33] Identifikacija računara koji se koristi za dizajniranje i pokretanje sajber-a operacija nije neophodan preduslov za identifikaciju. Poteškoće sa pripisivošću u sajber prostoru stvorilo je ideju da se međunarodna odgovornost države uspostavi kroz imputiranu odgovornost. Ovaj novi koncept koji nastoji da

[31] Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries pp. 38–9.

[32] Robin Geiß, Henning Lahmann, "Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention", in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law*, International Relations and Diplomacy CCDCOE, Tallinn, 2014., p. 623.

[33] Nicholas Tsagourias, Michael Farrell, "Cyber attribution: Legal and technical approaches and challenges", *European Journal of International Law*, 2020, Vol. 31, p. 946.

državi pripiše odgovornost za sajber napade koji potiču sa teritorije države bez obzira ko ih preduzima.[34] Ovaj oblik odgovornosti zasnivao bi se na tome da država nije bila dovoljno agilna i preduzela odgovarajuće mere da spreči privatna lica na svojoj teritoriji da čine protivpravna dela. U skladu sa ovim idejama pojavila su se i tumačenja da ako država ne spreči hakere na svojoj teritoriji od pokretanja napada unutar svojih granica, ne mora se poštovati tradicionalni zahtev za međunarodnu atribuciju države kako bi se država smatrala odgovornom. U pitanju bi bila apsolutna odgovornost u sajber prostoru.[35] Prema odredbama međunarodnog prava država treba da se pridržava pravila *no harm* uspostavljenog u sporu oko Krfskog kanala prema kome država ne sme „svesno da dozvoli da se njena teritorija koristi za deluje protivno pravima drugih država".[36] Ovo bi podrazumevalo da država ne dozvoli sa njene teritorije koriste za sajber napade na druge države, tačnije država mora da vrši kontrolu svoje internet infrastrukture.[37] Povreda te obaveze može postaviti pitanje međunarodnu odgovornost te države. određeni akti mogu krše suverenitet druge države ili drugih država, u smislu mešanja u oblastima nadležnosti koje su isključivo rezervisane za svaku državu. Ovo može biti povezano sa incidentima elektronskog nadzora ili špijunaže vladinih službi i osoblja druge države.[38] Međutim, po ovom pitanju ne postoji konsenzus, jer postoje ozbiljne razlike u tumačenjima s obzirom da sajber špijunaža nije izričito zabranjena međunarodnim pravom. Ipak, mnoge države su prepoznale potrebu za zaštitom od sajber špijunaže i usvojile su nacionalne zakone koji zabranjuju takve aktivnosti.[39] Takođe, postoje inicijative da se uvedu međunarodni standardi i zakoni koji bi regulisali ovu oblast. Pored toga, postoji praksa međunarodnih organizacija, kao što su UN i NATO, da se sajber špijunaža smatra nelegalnom aktivnošću i da se preduzimaju mere za njeno sprečavanje i kažnjavanje.[40] Sajber napadi mogu

[34] Zhxiong Huang, "The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations", *Baltic Yearbook of International Law Online* Vol.14/1, *Brill- Nijhoff,* 2015, pp. 41–54.

[35] Vincent-Joel Proulx, "Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?", *Berkeley Journal of International Law*, 2005, Vol. 23, pp. 643–653.

[36] "International Court of Justice Reports of Judgments, Corfu Channel case (The United Kingdom v. Albania)", Merits, Judgment of 9 April 1949, p. 22.

[37] Michael Schmitt, Tallinn *Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013, p. 26.

[38] Hersch Lauterpacht, *Private Law Sources and Analogies of International Law*, The Lawbook Exchange, Ltd, 2002, p. 53.

[39] Nacionalni zakoni koji se bave sajber špijunažom, poput američkog Zakona o zaštiti računarskih podataka "Computer Fraud and Abuse Act", A BILL, May 25, 2017 To improve the prohibitions on money laundering, and for other purposes. Internet: https://www.congress.gov/bill/115th-congress/senate-bill/1241/text, 10.08.2023.

[40] Kada je reč o praksi međunarodnih organizacija, UN je usvojio Deklaraciju o suverenitetu u sajber prostoru u kojoj se naglašava da je sajber špijunaža nelegalna aktivnost koja može ugroziti međunarodni mir i bezbednost. The Application of International Law to State Cyberattacks. Internet: https://www.chathamhouse.org/2019/12/application-international-law-state cyberattacks /2-application-sovereignty-cyberspace, 11.08.2023.

izazvati opasnost po unutrašnje i spoljne poslove napadnute države. Ovo ukazuje na još jedan i možda u nekim slučajevima jedini osnov za zasnivanje odgovornost povreda obaveze dužne pažnje koja proizilazi iz principa da nijedna država može svesno dozvoliti da se njena teritorija koristi za ili da bude izvor, dela štetnih za druge države.[41] Jedan od najvećih problema kod pripisivosti ilustruje situacija prekogranične štete, gde država porekla, a ne država žrtva, kontroliše i ima nadležnost nad računarima i računarskim mrežama iz kojih je prekogranična šteta nastala.[42] Pošto sajber šteta može biti trenutna i razorna, najefikasniji način za ublažavanje takvih šteta je njihovo sprečavanje. Za razliku od mnogih drugih prekograničnih šteta, sajber akcije se mogu odvijati gotovo trenutno. Sama Pravila nisu prilagođena specifičnostima subjekata koji vrše protivpravne radnje u sajber prostoru, pa države vrlo često u manjoj ili većoj meri podržavaju i podstiču takve aktivnosti narušavajući suverenitet drugih država. Na ovaj način, adekvatan pravni odgovor na izazove atribucije u sajber prostoru mora da se pozabavi sa dva problema: prvo, kada države nose štetne sajber operacije u strateške svrhe treba ih zadržati odgovorni za svoje ponašanje uprkos gore navedenim poteškoćama i drugo, kada nedržavni akteri izvode štetne sajber operacije, ciljane protiv država one bi, u odgovarajućim okolnostima, trebale biti u mogućnosti da pribegnu mehanizmima za ulaganje pravnih lekova i rešavanje sporova proizašlih iz ovih aktivnosti.

PRINCIP DUŽNE PAŽNJE KAO ZAMENA PRIPISIVOSTI U SAJBER PROSTORU

Princip dužne pažnje predstavlja normu običajnog prava i dovoljno se fleksibilni tumači, pa je eventualna primena moguća i u sajber prostoru. Jedna od najvećih bojazni je da bi princip dužne pažnje mogao dovesti državu da ima apsolutnu odgovornost u sajber prostoru. Ipak zagovornici korišćenja principa dužne pažnje za uspostavljanje odgovornosti tvrde da bi država odgovarala pod precizno određenim uslovima.[43] Široko tumačenje obaveze dužne pažnje sprečilo bi državu da opravda nemarno ponašanje sa argumentima da država nije imala saznanja o preduzetim aktivnostima koje su u suprotnosti sa pravima druge

[41] Marco Mayer et al., "International Politics in the Digital Age:Power Diffusion or Power Concentration?", Working paper, University of Florence, 12-14 September 2013, pp. 1-64.

[42] Sajber špijunaža od strane hakerskog broda države A dok se pretpostavlja da koristi pravo na nevini prolaz u pomorskoj zoni obalske države (država B) usmeren na treću Država (država C) može prekršiti obavezu dužne pažnje države B da svesno ne dozvoli teritoriju koja će se koristiti protiv države C. Doktrina ide toliko daleko da to postavlja da nijedna sajber aktivnost koju preduzima brod dok je u nevinom prolazu ne sme ugrožavaju odnose obalne države sa drugim državama i njene dužnosti u pogledu druge države.

[43] Michael Schmitt, "In Defense of Due Diligence in Cyberspace", *The Yale Law Journal Forum,* 2015, pp. 68–80.

države, posebno kada država ima ograničen kapacitet da detektuju protivpravne sajber aktivnosti.[44] U izvesnom smislu, svaki element principa deluje kao razumno ograničenje potencijalne odgovornosti države. Prvi element, znanje, može se zadovoljiti i stvarnim i konstruktivnim znanjem. U skladu sa ovim principom pretpostavlja se da država ima znanje o svim aktivnostima na njenoj teritoriji. Svakako da država ima veće informacije o aktivnostima na javnoj nego na privatnoj infrastrukturi. Ukoliko se sajber napadi ponavljaju kroz domaću mrežu neke države mogu poslužiti kao dokaz da je država tranzita znao ili je trebalo da zna za napade. Shodno tome, ako država zna ili je trebalo da zna za štetnu sajber operaciju koja putuje kroz njenu teritoriju, obavezuje ga obaveza da pokušaj da se prekine.[45] Princip dužne pažnje bi se bavio samo sajber operacijama koje predstavljaju međunarodno protivpravno delo, a koje bi za posledicu imale ozbiljne štetne posledice po državu koja je žrtva ciljnog napada.[46] Treći element, koji se tiče izvodljivih mera, predviđa da države odgovaraju po osnovu propusta dužne pažnje samo u situacijama kada propuste da intervenišu u sajber operaciji kada imaju kapacitet da to učine i kada je to razumno u datim okolnostima. Ovaj element nudi najveću zaštitu državama od nametanja apsolutne odgovornosti.[47] Obim same obaveze za svaku državu variraće u zavisnosti od pojedinačnih kapaciteta svake države koji se ogledaju kroz financijske resurse, tehnološku opremljenost, te obučenosti kadrova kako bi mogli odgovoriti hakerskim napadima. Države neće kršiti međunarodno pravo ako nije sprečila složenu sajber operaciju za koje nema sposobnost da kontroliše.[48] Još jedan uslov znatno ograničava obaveze države u pogledu dužne pažnje u sajber prostoru tako država neće odgovarati ni u slučajevima kada države imaju kapacitet da spreče štetne sajber operacije sprovedene na njihovoj teritoriji, ako bi to u datim okolnostima bilo previše opterećujuće i nerazumno.[49] Na ovaj način, princip dužne pažnje može delovati kao standard pripisivanja u jasno propisanom spletu okolnosti. Države će biti odgovorne samo za sajber operacije sa ozbiljne štetne posledice, koje imaju kapacitet da identifikuju i odgovori na njih.[50] Država bi svoje obaveze u pogledu dužne pažnje dakle ispunila ako bi u datim okolnostima uradila ono

[44] *Ibid.*

[45] Scott Russell, et al.,"Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors", *Chicago Journal of International Law,* 2016, Vol. 17(1), pp. 1–50.

[46] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press 2017, p. 30 (Rule 6)

[47] *Ibid.* pp. 74–75.

[48] Karine Bannelier, ''Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?'' *Baltic Yearbook of International Law,* 2014, Vol. 14, pp. 23–39.

[49] *Ibid.*

[50] Michael Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, *op.cit*., p. 106.

što se od nje može „razumno očekivati".[51] Utvrđivanje da li je država postupila razumno u suočavanju sa pretnjom ili, događajem, štetnog sajber ponašanja zahteva razmatranje niza faktora, pre svega usvajanje svih raspoloživih sredstava od strane države. Ocenjivanje ovih faktora se svodi na subjektivni element. Treba naglasiti da je većina sajber prostora u vlasništvu privatnih kompanija koje njime upravljaju. Stoga će država često morati da traži od privatnih aktera koji deluju na njenoj teritoriji da preduzmu neophodne mere da spreče ili prekinu štetno međunarodno sajber ponašanje. Država je dužna da preduzme samo mere koje su „razumno dostupne" i u okviru njenih sposobnosti.[52] U takvim slučajevima, ako država svesno propusti da smanji štetu naneta susednoj državi bila bi odgovorna. Da bi se procenilo da li država postupa sa maksimalnim naporima treba sagledati stanje svake države u pogledu svih pomenutih relevantnih parametara. Stručnjaci međunarodnog prava iznose argumente u korist stvarnog znanja države u kontekstu principa dužne pažnje u sajber prostoru. Dosadašnje odluke međunarodnih pravosudnih organa su takođe uspostavili državni odgovornost na osnovu dokaza o stvarnim znanja.[53] Ovo nije univerzalno prihvaćeno tumačenje, a norma bi takođe mogla biti podložna širem tumačenju. Shodno tome, moglo bi se tvrditi da država ne uspeva ispuniti normativno očekivanje kada ono ne ulaže najbolje napore da spreči a sajber operacija o kojoj bi trebalo da zna. Jurisprudencija ovaj koncept označava kao konstruktivno znanje. Šire tumačenje dužne pažnje moglo bi državu sa čije teritorije potiču štetne aktivnosti u sajber prostoru izjednačiti sa državama tranzita.[54] Prihvaćeni standard pažnje, kada se primenjuje dužna pažnja, je jedan od razumnih sposobnosti, iako postoji neslaganje oko toga da li ovaj standard u bilo kom određenom slučaju objektivan ili subjektivan, čak i prema tumačenju da dužne pažnje, države ne bi bile odgovorne za svaki sajber čin koji potiče sa njihove teritorije. Pored neodgovornosti za minorna dela. primećuje se da države obično polažu dužnu pažnju da spreče štetu ako država ima saznanja o situaciji.[55] Iako neke države, poput Nemačke, Indije, Holandije,[56] odražavaju opšti zahtev da se osigura da se

[51] European Court of Human Rights Osman v United Kingdom application 87/1997/871/1083, Judgment 28 October1998, para. 116.

[52] *Ibid.*

[53] Alabama claims of the United States of America against Great Britain (1871, 125–134); ICJ (1980), paras. 125–134.

[54] Podrška za proširenje normativna očekivanja prema državama tranzita u pogledu dužne pažnje iznosi Francuska, dok druge države nemaju čvrsto izgrađene stavove po ovom pitanju.

[55] Sean Kanuck,"Sovereign Discourse on Cyber Conflict under International Law", *Texas Law Review,* 2010, Vol. 88, pp. 1571–1597.

[56] The Netherlands. 2019. Letter to the parliament on the international legal order in cyberspace.5 July 2019, Appendix 1. Internet: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, 26.03.2023.

sajber aktivnosti i sajber prostor države ne koristi za prekograničnu štetu, malo je dokaza da su države prihvatile ovu dužnost kao pitanje međunarodnog prava.[57] Trenutno najvažniji multilateralni sajber ugovor je Konvencija o Evropskom sajber kriminalu koja umesto uspostavljanja proaktivnih zahteva za sprečiti, je gotovo čisto proceduralna konvencija koja uspostavlja metodologije saradnje nakon sajber događaja kako bi se omogućila transnacionalna međunarodna istraga i krivično gonjenje.[58] Povećano prihvatanje Konvencije i pridržavanje njenih odredbi može čak dovesti do opšteg prihvatanja stvaranja domaćih zakona koji zabranjuju određene sajber akte, ali izgleda da takav konsenzus tek treba da se uspostavi. stručnjaci su tvrdili da mnoge od sajber-specifičnih obaveza nisu zasnovane na „izrazitoj primarnoj obavezi u pogledu štetnih sajber operacija kao takvih", već nego na „opštem principu dužne pažnje u sajber kontekstu. Iako se na prvi pogled princip dužne pažnje čini kao odlična alternativa za uspostavljanje odgovornosti u sajber prostoru nekoliko aspekata sajber operacija čini trenutnu primenu dužne pažnje od strane država neefikasnih u ograničavanju prekogranične štete nanete drugoj državi. Anonimnost akcija na internetu omogućavaju i državnim i nedržavnim akterima da sprovode sajber operacije. Za identifikovanje počinioca u sajber prostoru potrebno je dugo vremena, što obesmešljava eventualnu nadoknadu štete.[59] Usled toga pojavile su se ideje da se postupak pripisivanja pokuša ustanoviti u dosta ranijoj fazi, ako bi država koja je oštećena mogla ukazati na nedostatak dužne pažnje od strane države iz koje su potekle sajber operacije, atribucija bi se mogla pretpostaviti i stoga učiniti to stanje potencijalno odgovoran za štetu prouzrokovanu sajber aktivnostima. Primena dužne pažnje se u sajber prostoru ograničava sa težnjom da država strože shvati da ozbiljnije shvate svoju obavezu dužne pažnje. Činjenica da sajber napadi mogu imati trenutno dejstvo vremenska priroda sajber operacije dodaje nivo složenosti u određivanju i karakterizacije i namere sajber aktivnosti koje potkopavaju efikasnost tradicionalnih pojmova dužne pažnje.[60] Evolucija dužne pažnje svakako ima potencijal da se razvije na takav način kako bi se opravdala represija nad ljudskim pravima, rizik koji je takođe preti od strane države. Kako međunarodna zajednica jača obavezu država da prati svoje sajber aktivnosti takođe mora osigurati da postoje stroge zaštitne mere kako bi se sprečilo da države

[57] Andraž Kastelic, *Due diligence in cyberspace Normative expectations of reciprocal protection of international legal rights,* UNIDIR, 2021, p. 13.

[58] "Council of Europe Convention on Cybercrime, (The Budapest Convention) 23 November 2001", ETS, No. 185.

[59] Ako državni ili nedržavni akteri veruju da njihov žrtve neće moći da ih identifikuju kao sajber aktere mesecima ili čak godinama nakon događaja, mnogi će biti spremni da prihvate potencijalne rizike u nadi da će eventualni odgovori na odloženo pripisivanje će biti prigušeni tokom vremena.

[60] Eric Talbot Jensen, "Due dilligence in cyber activities", H. Krieger et al. (ed.) in *Due Diligence in the International Legal Order*, 2020, pp. 252–268.

koriste ovu dužnost za cenzuru komunikacija koje su kritične nastrojene prema politikama države.[61] Snažnija primena dužne pažnje u sajber sektoru, po uzoru na primenu principa u drugim sektorima, značajno bi povećala odgovornost država da spreče zlonamerne sajber radnje i posledično poboljšati sposobnost međunarodnog prava da obezbedi red i stabilnost u međunarodnom sistemu.[62] Jedina efikasna preventiva od štetnih sajber aktivnosti ogleda se kroz pristup jačanja državne odgovornosti kroz poštovanje dužne pažnje. Druga mogućnost je da države preduzmu protivmere u sajber prostoru protiv druge države koja preti sajber napadima. Proaktivna primena dužne pažnje u sajber sektoru, po uzoru na primenu principa u drugim sektorima, značajno bi povećala odgovornost država da spreče zlonamerne sajber radnje i posledično povećati sposobnost međunarodnog prava da obezbedi red i stabilnost u međunarodnom sistemu. Unapređenje principa dužne pažnje u sajber kontekstu bi se mogao postići prenošenjem rigoroznijeg oslanjanja na prevenciju sa drugih pristupa specifičnih za oblast životne sredine i usađivanjem u sajber sektor.[63] Mora se napraviti ravnoteža između prirode, razmera i obim potencijalne štete za teritorijalnu (ili tranzitnu) državu i štetu po državu žrtvu kako bi se utvrdilo da li je razmatrana radnja neophodna i proporcionalna.[64] Države to rade na osnovu izbora najboljih mera koje treba preduzeti, s obzirom na okolnosti, da pokušaju da spreče ili zaustave sajber zloupotrebu njihove teritorije.

OBAVEZA DRŽAVE DA ZAŠTITI LJUDSKA PRAVA U SAJBER PROSTORU

Sajber napadi mogu imati značajnog uticaja na uživanje ljudskih prava. U sajber prostoru mogu biti ograničeni pravo na mišljenje i izražavanje. S obzirom da država ima obavezu da obezbedi svim ljudima pod njenom jurisdikcijom uživanje ljudskih prava u punom obimu kompleksnost digitalnog doba i sajber prostora nameće ozbiljne izazove državi čije neprevazilaženje može povući i njenu odgovornost.[65] Ljudska prava u sajber prostoru ne treba da se artikulišu samo kao individualna prava, već treba da budu priznata i kao individualna i kao

[61] European Union, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence, "Building Strong Cybersecurity for the EU"', JOIN/2017/0450 final, 13 September 2017, p.18.

[62] *Ibid.*

[63] Karine Bannelier, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?" *op.cit.,* p. 29.

[64] Robert Kolb, "Reflections on Due Diligence Duties and Cyberspace." *German Yearbook of International Law* 2015, Vol 58, p.126.

[65] Međunarodno pravo ljudskih prava je podstaklo nesuglasice oko stepena do kojeg obaveze države u pogledu ljudskih prava ograničavaju njen suverenitet nad njenom teritorijom i koliko dozvoliti drugim državama da se mešaju u njene unutrašnje poslove.

kolektivna prava. Ljudska prava se podjednako primenjuju na internetu i u fizičkom prostoru. Digitalne tehnologije su otvorile mnoge nove i zanimljive načine izražavanja ideja, razmene informacija, udruživanja, protesta i drugih sličnih sloboda u okviru ljudskih prava. Ova prava uživaju univerzalnu zaštite i pripadaju svima, bez obzira na poreklo, status i druge lične osobine. Istovremeno, digitalizacija naše komunikacije i svakodnevnih poslova je takođe omogućio razvoj sredstava za zloupotrebe i povrede prava. Poteškoće sa kojima se susreću pri pripisivanju sajber akcija određenim akterima kako se zahteva prema principima države odgovornost izazvali su zabrinutost da vlade iskorištavaju ovaj problem i krše ljudska prava (npr. sprovođenje nadzora nad političkim protivnicima preko punomoćnika). Postoje nedoumice da li je s obzirom na učešće velikog broja nedržavnih aktera moguće u sajber prostoru imajući u vidu da ugovori o ljudskim pravima nameću obaveze jedino državama. Ipak bez obzira na ove nedostatke, međunarodno pravo ljudskih prava obavezuje teritorijalnu državu da preduzme sve mere u okviru svojih ovlašćenja da zaštiti ljudska prava u oblasti van njene efektivne kontrole.[66] Neiscrpna je lista ljudskih prava koja su posebno značajna u sajber prostoru, dodatno mnogi sajber prostor vide kao krucijalan za uživanje ekonomskih, socijalnih i kulturnih prava. Zavisnost od sajber prostora daje onlajn informacijama sve veću važnost u progresivnim ostvarivanje ovih prava pa se obezbeđivanje pristupu informacijama kao krucijalan za uživanje ljudskih prava u sajber prostoru.[67] Iako Komitet za ekonomska socijalna i kulturna pitanja pristup sajber prostoru uzima kao relevantan za ocenjivanje napretka u pogledu ostvarivanja i poštovanja ljudskih prava u državi, odnos između sajber prostora i ove grupe ljudskih prava treba prvenstveno gledati kroz prizmu buduće ostvarive perspektive, jer trenutno mnoge države imaju problema sa ostvarivanjem ekonomske grupe ljudskih prava za koje sajber prostor i pristup internetu su irelevantni poput obezbeđivanja adekvatne hrane, lekova, smeštaja, kanalizacije. Zamera se da je digitalno doba dovelo do diskriminacije u uživanju ekonomskih i socijalnih prava iz prostog razloga što je došlo do ogromnog jaza između razvijenih zemalja i zemalja u razvoju u pogledu pristupa internetu i informacionim tehnologijama. Sajber prostor je postao

[66] UN Human Rights Committee, "Concluding Observations: Russian Federation (28 April 2015), UN Doc CCPR/C/RUS/CO/7, para. 23(b) Human Rights Council, Situation of Human Rights in the Temporarily Occupied Autonomous Republic of Crimea and the City of Sevastopol (Ukraine)", 25 September 2017, UN Doc A/HRC/36/CRP.3, paras. 154–161.

[67] Kao primer se može uzeti uživanje prava na zdravlje, država ima dužnost poštovanja znači da vlada ne može ograničiti ili uskratiti ljudima pristup važećim zdravstvenim informacijama. Država je dužna da sve pojedince pod svojom jurisdikcijom zaštiti od prevare u pogledu lažnih informacija vezanim za zdravstveni sistem, kao i da proširi pristup Internetu informacijama i uslugama koje pružaoci zdravstvenih usluga i pojedinci mogu koristiti za poboljšanje zdravlja. ''International Covenant on Economic, Social and Cultural Rights, 16 December 1966, 993 UNTS 3"; Limburg Principles on the Implementation of the International Covenant on Economic, Social and Cultural Rights. Internet: http://www.escr-net.org/docs/i/425445 , 23.08.2023.

nezamenjiv za ostvarivanje efikasne borbe protiv nejednakosti i ubrzanje razvoja i ljudski napredak. Tipični oblici izražavanja koji inače ne bi trebalo da budu podložni ograničenjima, bilo van mreže ili onlajn, uključuju diskusiju o vladi politike i političke debate; izveštavanje o ljudskim pravima, aktivnostima vlade i korupcija u vladi, angažovanje u predizbornim kampanjama mogu biti ugroženi od strane države u sajber prostoru.[68] Pravo na privatni život podrazumeva kontrolu nad informacijama o nama, tj kontrolu da li će i ko znati koja mesta posećujemo, ko smo, gde živimo i sa kim se dopisujemo. Privatnost je nesporna važna za ličnu autonomiju svakog pojedinca i pretnje sa kojima se može suočiti postao sve očigledniji u digitalnom prostoru. Čitanje i zadržavanje sadržaja namenjenih onlajn komunikacijama biti poverljiv svakako ometa pravo na privatnost. Pravo na privatnost bi prema normama koje regulišu ljudska prava zahteva da integritet i poverljivost prepisku treba garantovati *de iure i de facto*."[69] Prepiska treba dostaviti adresatu bez presretanja i bez da se otvorena ili na drugi način pročitana."[70] Uokvirivanje pristupa sajber prostoru na ovaj način je u skladu sa sagledavanjem tehnologija kao sredstva za zaštitu i unapređenje ljudskih prava. Sve više je zagovornika teze da je pristup sajber prostoru i internetu novo ljudsko pravo, jer predstavlja preduslov za ostvarivanje prava mišljenja i izražavanja. Sa pojavom interneta, protok komunikacije među ljudima je postao povećao, posebno imajući u vidu da možemo da komuniciramo sa više ljudi na u isto vreme i da se mogu nalaziti na različitim kontinentima. Eklatantan primer uticaja pristupu sajber prostoru možemo videti kroz ostvarivanje prava na obrazovanje. Mark Zakerberg (*Mark Zuckerberg*), osnivač Facebook-a, tvrdio je da je internetska povezanost u sajber prostoru ljudsko pravo jer takva povezanost jeste sredstvo za postizanje političkih, ekonomskih i društvenih ciljeva koje režim ljudskih prava teži da ostvari.[71] Savet UN za ljudska prava je zauzeo stav da ljudi imaju ista ljudska prava na mreži kao i van mreže.[72] Ovaj stav ima implikacije na odgovornost države jer država ima obavezu da na isti način štiti ljudska prava, te njeni propusti za sobom povlače odgovornost. sajber prostor omogućava pojedincima da vrlo lako ugrožavaju ljudska prava i slobode. Neke od opasnosti koje u sajber prostoru prete pojedincima su sajber rasizam i homofobija.[73] Pored

[68] "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", May 16, 2011.

[69] "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism", 16-18, U.N. Doc. A/69/397 (Sept. 23, 2014).

[70] *Ibid.*

[71] C. Kang, M. Isaac, Defiant Zuckerberg says Facebook won't police political speech', New York Times. Internet: https://www.nytimes.com/2019/10/17/business/zuckerberg -facebook-free-speech.html , 16.03.2023.

[72] "Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet", UN Doc A/HRC/RES/32/13. 18 July 2016.

[73] Sajber rasizam može biti u obliku pojedinaca koji objavljuju rasističke komentare ili učestvuju na grupnim stranicama koje su posebno postavljene u rasističke svrhe.

pozitivnih obaveza države da u sajber prostoru štiti uživanje ljudskih prava pojedinaca od napada trećih osoba. Negativne obaveze nastavljaju da nameću teritorijalnoj državi, na primer, dužnost da ne krši pravo na život pojedinaca putem sajber napada, zabrana mučenja i nehumanog ili ponižavajućeg postupanja putem onlajn sredstava, i zabrane slobode izražavanja, uključujući podsticanje na rasnu mržnju ili terorizam.[74] Budućnost ljudskih prava u sajber prostoru zavisi od evolucije zakona i njegovog tumačenja od strane nacionalnih i međunarodnih upravnih tela. Savet bezbednosti UN je 22. maja 2020. u svojoj raspravi o sajber bezbednosti istakao potrebu da se sajber napadi prepoznaju kao jedno od pitanja ljudskih prava. Tok akcije koji je detaljno opisan ukazuje da potezi kao što su gašenje internet pristupa od strane vlade i hakovanje uređaja neistomišljenika, mogu dovesti do ozbiljnog kršenja ljudskih prava.[75] Osim toga sajber prostor omogućava određeni stepen anonimnosti, npr. možemo kreirati profile koji ne otkrivaju naš identitet i zbog toga mnogi mnogo slobodnije komuniciraju u sajber prostoru, smatrajući da posledice ponašanja na mreži ne moraju biti iste kao u fizičkom prostoru. Usled ove mogućnosti digitalni prostor je idealan za širenje ksenofobije i govora mržnje. Cenzura koja se javlja kroz filtriranje i blokiranje sadržaja i kojima pribegavaju razne države i korporacije, takođe predstavlja ozbiljan problem, jer nam onemogućava slobodan pristup informacijama. Sadržaj se može uređivati ne samo kroz cenzuru, već i njegovo postavljanje, tj. algoritmi mogu odlučiti koji tip sadržaja će biti vidljiv kom korisniku. Kao nov način komunikacije su kreirani, a broj načina da se oni ograniče rapidno se povećava, zaštita slobode izražavanja u digitalnom kontekstu stoga može biti posebno izazovna.[76] Nedostatak slobode izražavanja ima štetan uticaj na društvo jer ograničava pristup različitim idejama i informacijama koje mogu biti od javnog značaja. To može sprečiti napredak i otežati prepoznavanje društvenih problema. S druge strane, sloboda izražavanja uključuje i potrebu za reguliranjem potencijalne manipulacije i širenja lažnih informacija. Sloboda izražavanja je ključna za razvoj društva jer omogućuje razmjenu ideja, otvorenu raspravu i otkrivanje novih rešenja za društvene probleme. Kada ljudi mogu slobodno izražavati svoje misli, doprinosi se inovacijama, kritičkom razmišljanju i napretku. Bez slobode izražavanja, društvo može biti zatvoreno, neprogresivno i nesvesno važnih problema. Jedan od uočenih problema je i da država vrlo često nema adekvatne kapacitete kako bi odgovorila ugrožavanju ljudskih prava u sajber prostoru. Postavlja se pitanje kada postoji povreda osnovnih ljudskih prava

[74] UNGA, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (10 August 2011), UN Doc A/66/290, para. 81.

[75] Deborah Brown, It's Time to Treat Cybersecurity as a Human Rights Issue, Internet:https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue, 21.05.2023.

[76] Share Foundation, Introduction to Digital Rights. Internet: https://www.sharefoundation.info/wp-content/uploads/Digital-rights-intro_ENG-1.pdf , 18.08.2023.

pojedinca. Da li odgovornost treba da padne samo na nalogodavca ili bi teret trebalo da bude i na provajderu Internet usluga, te da li se u ovim slučajevima odgovornost može pripisati državi. Odgovor bi se mogao pronaći samo u širokom tumačenju obaveze poštovanja principa dužne pažnje. Radi lakše zaštite ljudskih prava u sajber prostoru i sve raznovrsnih telekomunikacionih sistema etablira nova generacija ljudskih prava poznata i kao digitalna ljudska prava.[77]

ZAKLJUČAK

Pravila o odgovornosti države za međunarodno protivpravna dela su veoma teško primenjiva u sajber prostoru jer postoje ozbiljne poteškoće prilikom samog pripisivanja protivpravnog akta jer su se Pravila razvijala tokom prošlog veka dok još sajber prostor nije bio u povoju i značajan kao danas. Specifičnosti velikog broja privatnih samodovoljnih pojedinaca koji mogu potpuno odvojeno delovati vrlo je teško uspostaviti odgovornost države. Težnje velikih geopolitičkih sila da formiraju sopstvene internet sisteme uspostavljanje međunarodne odgovornosti učiniće praktično nemogućim. Dodatan problem koji će se morati rešiti jeste postići konsenzus kako bi se uspostavila ujednačena pravila vezana za pitanje jurisdikcije i suvereniteta nad sajber prostorom. Iako se princip dužne pažnje čini kao adekvatna alternativa za nedostatke koji su primetni u primeni Pravila u sajber prostoru, dublja analiza ipak ukazuje da i primena principa dužne pažnje u sajber prostoru za uspostavljanje odgovornisti ipak ima određene zapreke koje nisu baš lako premostive. Usled toga države tek treba da postignu sporazum o obimu norme, uslovi potrebnog znanja sajber aktivnosti na njenoj teritoriji i pragovima potrebnim da bi se ustanovila odgovornost za propuste dužne pažnje u sajber prostoru. Sajber prostor je danas postao krucijalan za uživanje velikog broja ljudskih prava, ali istovremeno i pogodan prostor za njihovo ograničenje. Zbog svega toga pojavile su se ideje da se neometan pristup internetu proglasi za fundamentalno ljudsko pravo te da se stvori i nova generacija digitalnih ljudskih prava. Sajber prostor je idealan za širenje ksenofobije, rasizma i drugih oblika koji ugrožavaju ljudska prava, te je primetno da države nemaju dovoljno kapaciteta da bi zaštitile pojedince pod svojom jurisdikcijom, što dovodi do kršenja međunarodnih obaveza i dovodi do međunarodne odgovornosti države. Informacione tehnologije i regulisanje sajber prostora je u rapidnom razvoju stoga treba očekivati da će se Pravila odgovornosti države prilagođavati specifičnostima sajber prostora kroz verovatno usvajanje dodatnih protokola na postojeća pravila kako bi se prevazišle postojeće barijere.

[77] Wolfgang Kleinwächter, Do we need a new generation of Human Rights for cyberspace? Internet: https://www.orfonline.org/expert-speak/do-we-need-a-new-generation-of-human-rights-for cyberspace/, 16.07.2023.

INTERNATIONAL RESPONSIBILITY OF THE STATE IN CYBERSPACE

ABSTRACT

Cyberspace is a domain whose use is necessary for the whole or at least a significant part of the global population. We are witnessing that the cyberspace is suitable for hacker attacks on states due to its specificity. The enjoyment of human rights can also be restricted or disabled due to hacker attacks. Cyberspace calls into question the general principles of international law important for human rights. All this raises the question of the international responsibility of the state in cyberspace. First, the specifics of cyberspace will be pointed out in the paper. The paper will then analyze the possibility of establishing responsibility in cyberspace with regard to the specifics of the element of attribution, as a result of which the importance of the principle of due diligence as an alternative to establishing responsibility will be considered. At the end, it will be reviewed what obligations the state has in terms of protecting human rights in cyberspace.

Key words: Cyberspace, international responsibility of the state, principle of due diligence, protection of human rights

REFERENCES

1. "Alabama claims of the United States of America against Great Britain (1871)", ICJ 1980.
2. Andress, Jason, Winterfeld, Steve, Ablon, Lillian, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* Elsevier, Amsterdam, 2014.
3. "Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)", Judgment, *ICJ Reports,* 2007. Internet: https://www.icj cij.org/public/files/case-related /91/091-20070226-JUD-01-00-EN.pdf, 07.03.2023.
4. Bannelier, Karine, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?" *Baltic Yearbook of International Law,* 2014, Vol. 14.
5. Benedikt, Michael, (Ed.), *Introduction and Cyberspace: some proposals, in Cyberspace,* First Steps, MIT Press, London, 1992.
6. Benedikt, Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace", in: K. Ziolkowski (Ed.), *Cyberspace,* NATO CCD COE Publication, Tallinn, 2013.
7. Brown, Deborah, "It's Time to Treat Cybersecurity as a Human Rights Issue". Internet: https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue, 21.05.2023.

8. "Computer Fraud and Abuse Act", A BILL, May 25, 2017 To improve the prohibitions on money laundering, and for other purposes see Internet: https://www.congress.gov/bill/115th-congress/senatebill/1241/text,10.08.2023.
9. "Council of Europe Convention on Cybercrime, (The Budapest Convention), 23 November 2001", ETS, No. 185.
10. "Cyberspace Definition of cyberspace in US English by Oxford Dictionaries". Internet: https://web.archive.org/web/20130218185858/http://oxforddictionaries.com/us/definition/american_english/cyberspace, 01.08.2023.
11. Deleure François*, Cyber Operations and International Law,* Cambridge University Press, 2020.
12. Duggan, Patrick, "Harnessing cyber-technology's human potential", *Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School*, 2015, Vol. 28 Issue 4.
13. European Union, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence, 'Building Strong Cybersecurity for the EU', JOIN/2017/0450 final, 13 September 2017.
14. Geiß, Robin, Henning Lahmann, "Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention", in: K. Ziolkowski (Ed.), *Peacetime Regime for State Activities in Cyberspace: International Law*, International Relations and Diplomacy CCDCOE, Tallinn, 2014.
15. Huang, Zhxiong, "The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations", *Baltic Yearbook of International Law Online*, 2015, Vol.14/ 1.
16. Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc A/HRC/RES/32/13. 18 July 2016.
17. International Court of Justice Reports of Judgments, "Corfu Channel case (The United Kingdom v. Albania)", Merits, Judgment of 9 April 1949.
18. "International Law in Cyberspace", US Department of State, US CYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18 Sept. 2012.
19. "International Covenant on Economic, Social and Cultural Rights", 16 December 1966, 993 UNTS 3".
20. "International Law Commission (ILC) Draft Articles on the Responsibility of States for Internationally Wrongful Acts with commentaries 2001", Official Records of the General Assembly, Fifty-sixth session, Supplement No 10 (A/56/10)".
21. Joint Publication 1-02, DoD Dictionary of Military Terms, Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7, October 17, 2008. Internet: www.dtic.mil./doctrine/jel/new_pubs/1_02.pdf, 01.03.2023.

22. Kang, C. Isaac, M., Defiant Zuckerberg says Facebook won't police political speech', New York Times. Internet: https://www.nytimes.com/2019/10/17/business/zuckerberg -facebook-free-speech.html, 16.03.2023.
23. Kanuck, Sean, "Sovereign Discourse on Cyber Conflict under International Law", *Texas Law Review,* 2010, No. 88.
24. Kastelic, Andraž, *Due diligence in cyberspace Normative expectations of reciprocal protection of international legal rights,* UNIDIR, 2021.
26. Kleinwächter, Wolfgang, "Do we need a new generation of Human Rights for cyberspace?". Internet: https://www.orfonline.org/expert-speak/do-we-need-a-new-generation-of-human-rights-for cyberspace/, 16.07.2023.
26. Koh, Harold, H, "International Law in Cyberspace", *Harvard International Law Journal* 2012, Vol 54, No. 2.
27. Kolb, Robert, "Reflections on Due Diligence Duties and Cyberspace." *German Yearbook of International Law,* 2015, Vol 58.
28. Lauterpacht, Hersch, *Private Law Sources and Analogies of International Law*, The Lawbook Exchange, Clark NY, 2002.
29. "Letter to the parliament on the international legal order in cyberspace", 5 July 2019, Appendix 1. The Netherlands. 2019. Internet: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace, 26.03.2023.
30. "Limburg Principles on the Implementation of the International Covenant on Economic, Social and Cultural Rights". Internet: http://www.escr-net.org/docs/i/425445 , 23.08.2023.
31. Mayer, Marco, et al.,"International Politics in the Digital Age:Power Diffusion or Power Concentration?", Working paper, University of Florence, 12-14 September 2013.
32. "Osman v United Kingdom application 87/1997/871/1083", European Court of Human Rights, Judgment 28 October 1998.
33. Proulx, Vincent-Joel, "Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?", *Berkeley Journal of International Law,* 2005, Vol. 23.
34. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (May 16, 2011).
35. "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism", 16-18, U.N. Doc. A/69/397 (Sept. 23, 2014).
36. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", (May 16, 2011).

37. Roscini, Marco, "World Wide Warfare – Jus ad bellum and the Use of Cyber Force", in: A. von Bogdandy, R. Wolfrum (eds), *Max Planck Yearbook of United Nations Law ,* Martinus Nijhoff, Leiden, 2010, Vol. 14.
38. Russell, Scott et al."Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors", *Chicago Journal of International Law,* (1): 2016, Vol. 17.
39. Schmitt Michael, Tallinn *Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013.
40. Schmitt, Michael N, "Grey Zones in the International Law of Cyberspace",*Yale Journal of International Law Online,* 2017, Vol. 42.
41. Schmitt, Michael, "In Defense of Due Diligence in Cyberspace", *The Yale Law Journal Forum*, 2015.
42. Schmitt, Michael, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations ,Cambridge University Press 2017.*
43. Schneider,Volker, Hyner, Dirk, *The Global Governance of Cybercrime: Issue Space and the Transnational Policy Networ,.* University of Konstanz, Germany, 2003.
44. Share Foundation, Introduction to Digital Rights. Internet: https://www.sharefoundation.info/wp-content/uploads/Digital-rights-intro_ENG-1.pdf, 18.08.2023.
45. Talbot Jensen, Eric, "Due dilligence in cyber activities", in: H. Krieger et al. (eds), *Due Diligence in the International Legal Order*, 2020.
46. "The Application of International Law to State Cyberattacks". Internet: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace, 11.08.2023.
47. "The Factory at Chorzów Claim for Indemnity-Germany v. Poland", PCIJ, 1928, Ser. A No. 17.
48. Tobanksy, Lior, "Basic concepts in cyber warfare", *Military and Strategic Affairs,* 2011, Vol. 3.
49. Tsagourias Nicholas, Farrell Michael, "Cyber attribution: Legal and technical approaches and challenges", *European Journal of International Law,* 2020, Vol. 31.
50. UN Human Rights Committee, "Concluding Observations: Russian Federation (28 April 2015), UN Doc CCPR/C/RUS/CO/7, para 23(b) Human Rights Council, Situation of Human Rights in the Temporarily Occupied Autonomous Republic of Crimea and the City of Sevastopol (Ukraine)", 25 September 2017, UN Doc A/HRC/36/CRP.3.
51. UNGA, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", 10 August 2011, UN Doc A/66/290

52. United Nations Convention on the Law of the Sea (signed 10 December 1982)
53. Villeneuve, Nart, "Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online" in: Ronald Deibert, *et al.* (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, Cambridge, 2010.
54. Witenberg, Joseph C, "La théorie des preuves devant les juridictions internationales", *RCADI*, 1936, Vol. 56, No. 1.