Pregledni naučni rad

UDK 004.056.5:351.749(100) DOI 10.7251/DEFSR5625079R COBISS.RS-ID 142982401

PRAVNI REŽIM DRŽAVNE JURISDIKCIJE U CYBER PROSTORU: MEĐUNARODNO-PRAVNI OKVIR ZA ATRIBUCIJU ODGOVORNOSTI ZA TRANSNACIONALNE CYBER OPERACIJE

Mitar Radonjić[1]
Milica Župljanić[2]
Ivan Ćorović[3]

Apstrakt: Ekspanzija cyber prostora predstavlja jedan od najsloženijih izazova savremenog međunarodnog prava, posebno u kontekstu određivanja državne jurisdikcije i atribucije odgovornosti za transnacionalne cyber operacije. Ovaj rad analizira postojeći međunarodno-pravni okvir za uspostavljanje državne jurisdikcije u cyber domenu, istražuje pravne standarde za atribuciju cyber napada državama i razmatra evoluciju međunarodno-pravnih normi u ovoj oblasti. Kroz komparativnu analizu državne prakse, sudskih odluka i međunarodnih dokumenata, rad identificira ključne pravne praznine i predlaže pravce za buduće normativno uređenje. Istraživanje pokazuje da tradicionalni principi teritorijalne i personalne jurisdikcije zahtevaju značajnu adaptaciju za efikasnu primenu u cyber prostoru, dok standardi za atribuciju odgovornosti ostaju nejasni i kontroverzni. Rad zaključuje da je potreban sveobuhvatan međunarodni pravni instrument koji bi jasno definisao jurisdikcijske okvire i kriterijume atribucije u cyber domenu.

Ključne reči: cyber jurisdikcija, atribucija odgovornosti, međunarodno pravo, cyber operacije, državna odgovornost, cyber warfare

1 fakultet.tutin@live.com
2 fakultet.tutin@live.com
3 fakultet.tutin@live.com

1. UVOD

Digitalna revolucija poslednje decenije fundamentalno je promenila prirodu međunarodnih odnosa i postavila pred međunarodno pravo nove, neočekivane izazove. Cyber prostor, kao virtualni domen koji transcenduje tradicionalne geografske granice, doveo je u pitanje osnovne postulate vestfalskog sistema državne suverenosti i jurisdikcije (Schmitt, 2017). Transnacionalne cyber operacije, koje mogu biti izvršene iz bilo koje tačke sveta i usmerene protiv ciljeva u drugim državama, zahtevaju preispitivanje klasičnih principa međunarodnog prava i uspostavljanje novih pravnih okvira. Problem jurisdikcije u cyber prostoru posebno je složen jer tradicionalni teritorijalni principi, na kojima se zasniva vestfalski sistem međunarodnog prava, nisu direktno primenljivi na virtuelne operacije koje se mogu izvršavati kroz servere i mreže u različitim jurisdikcijama (Buchan, 2018). Dodatno, pitanje atribucije - odnosno utvrđivanja koji državni ili nedržavni akteri stoje iza određenih cyber operacija - predstavlja tehnički i pravni izazov bez presedana u tradicionalnom međunarodnom pravu. Relevantnost ovog istraživanja proizlazi iz rastućeg broja cyber incidenata koji imaju značajne političke, ekonomske i bezbednosne posledice. Od napada na estonsku infrastrukturu 2007. godine, preko Stuxnet virusa koji je ciljao iranske nuklearne objekte, do recentnih ransomware napada na kritičnu infrastrukturu, cyber operacije su postale sastavni deo savremenih međunarodnih odnosa (Tikk *et al*., 2010). Međutim, pravni odgovor na ove izazove ostaje fragmentaran i nedosledan. Ovaj rad ima za cilj da analizira postojeći međunarodno-pravni okvir za uspostavljanje državne jurisdikcije u cyber prostoru i kritički oceni standarde za atribuciju odgovornosti za transnacionalne cyber operacije. Istraživanje će kroz tri ključna aspekta - teorijske osnove jurisdikcije, praktične izazove atribucije i evoluciju pravnih normi - pružiti sveobuhvatan pregled trenutnog stanja i pravaca budućeg razvoja ove oblasti međunarodnog prava.

2. TEORIJSKE OSNOVE DRŽAVNE JURISDIKCIJE U CYBER PROSTORU

Međunarodno pravo tradicionalno priznaje pet osnovnih principa za uspostavljanje državne jurisdikcije: teritorijalni, personalni (aktivni i

pasivni), zaštitni i univerzalni princip (Brownlie, 2008). U kontekstu cyber operacija, svaki od ovih principa suočava se sa značajnim izazovima adaptacije. Teritorijalni princip, kao najšire prihvaćen osnov jurisdikcije, zasniva se na fizičkoj lokaciji događaja ili radnje. U cyber prostoru, međutim, koncept "mesta" postaje problematičan kada se operacije izvršavaju kroz servere u različitim državama, koriste proxy servere za maskiranje lokacije ili se oslanjaju na cloud computing infrastrukturu (Svantesson, 2013). Slučaj Estonia v. Russia (2007) ilustruje ovu problematiku - dok su napadi ciljali estonsku infrastrukturu, njihovo poreklo je bilo teško ustanoviti zbog korišćenja botneta distribuiranih širom sveta.

Personalni princip, koji se zasniva na državljanstvu učinioca ili žrtve, takođe zahteva modifikaciju u cyber kontekstu. Aktivni personalni princip omogućava državi da vrši jurisdikciju nad svojim državljanima bez obzira na mesto činjenja dela, što je posebno relevantno za cyber operacije koje mogu biti izvršene iz bilo koje lokacije (Ryngaert, 2015). Međutim, ustanovljavanje identiteta i državljanstva cyber aktera često je tehnički i praktično nemoguće. Značajan doprinos teorijskom utemeljenju dao je Međunarodni sud pravde u slučaju Nicaragua v. United States (1986), ustanovivši da države imaju obavezu da ne dozvolje korišćenje svoje teritorije za napade na druge države. Ovaj princip, poznat kao "due diligence" obaveza, dobija novu dimenziju u cyber prostoru gde države moraju preduzeti razumne mere da spreče korišćenje svoje cyber infrastrukture za napade na treće zemlje (Schmitt, 2017).

Koncept virtualne teritorijalnosti predstavlja pokušaj adaptacije teritorijalnog principa na cyber prostor kroz uspostavljanje pravnih fikcija koje povezuju cyber aktivnosti sa fizičkim teritorijama (Johnson & Post, 1996). Ovaj pristup sugeriše da svaki cyber čin ima "efekt" na određenoj teritoriji, omogućavajući primenu tradicionalnih jurisdikcijskih principa. Praksa država pokazuje različite pristupe ovom pitanju. Sjedinjene Države primenjuju široko tumačenje teritorijalne jurisdikcije, smatrajući da imaju pravo na jurisdikciju nad cyber operacijama koje "prolaze" kroz američku infrastrukturu ili imaju "efekt" na američkoj teritoriji (Brenner, 2007). Evropska unija, s druge strane, razvija pristup zasnovan na "substancijalnoj povezanosti" između cyber operacije i teritorije države. Kritična analiza pokazuje da virtualna teritorijalnost, iako praktično korisna, može dovesti do konflikta jurisdikcija i pravne nesigurnosti. Problem

"spillover" efekata - kada cyber operacija ima posledice u više država - zahteva koordiniran međunarodni odgovor i jasne kriterijume za određivanje primarne jurisdikcije (Buchan, 2018).

3. ATRIBUCIJA ODGOVORNOSTI U TRANSNACIONALNIM CYBER OPERACIJAMA

Atribucija cyber operacija državama predstavlja jedan od najkompleksnijih aspekata međunarodnog cyber prava (Knežević, 2015; Knežević, 2017). Međunarodno pravo državne odgovornosti, kodifikovano u Articles on State Responsibility (ILC, 2001), uspostavlja jasne kriterijume za atribuciju: radnja mora biti izvršena od strane državnog organa ili lica koje deluje u svojstvu državnog organa, ili država mora imati efektivnu kontrolu nad nedržavnim akterom. U cyber kontekstu, primena ovih kriterijuma je problematična iz nekoliko razloga. Prvo, cyber operacije često izvršavaju specijalizovane nedržavne grupe ili individualni hakeri koji mogu, ali ne moraju, biti povezani sa državnim aparatom (Roscini, 2014). Drugo, tehnička složenost cyber napada omogućava korišćenje "false flag" operacija gde se odgovornost pokušava pripisati trećim stranama.

Značajan precedent predstavlja slučaj Georgia v. Russia (2008), gde su cyber napadi na gruzijsku infrastrukturu tokom rata bili izvršeni od strane nedržavnih grupa koje su, prema gruzijskim tvrdnjama, bile podržavane od strane Rusije (Knežević, 2025). Međunarodni sud pravde još uvek nije doneo konačnu odluku o atribuciji ovih napada, što ilustruje složenost problema. Test "efektivne kontrole", uspostavljen u slučaju Nicaragua v. United States, zahteva da država ima operativnu kontrolu nad specifičnim činovima nedržavnih aktera (ICJ, 1986). U cyber domenu, ovaj test je teško primeniti jer država može pružiti logističku podršku haker grupama bez direktne kontrole nad njihovim operacijama (Schmitt, 2017).

Pravni standardi za atribuciju moraju biti podržani adekvatnim evidentnim zahtevima. U tradicionalnom međunarodnom pravu, dokazi su obično fizička priroda i mogu biti nezavisno verifikovani. Cyber dokazi, međutim, su digitalni, lako mogu biti falsifikovani ili uništeni, i zahtevaju specializovano tehničko znanje za interpretaciju (Rid & Buchanan,

2015). Razvoj međunarodnih standarda za cyber forensiku predstavlja ključni izazov. NATO Cooperative Cyber Defence Centre of Excellence razvio je Tallinn Manual kao pokušaj kodifikacije međunarodnog prava primenjivog na cyber warfare, ali ovaj dokument nema obavezujuću pravnu snagu (Schmitt, 2013). Manual sugeriše da tehnička atribucija mora biti dopunjena pravnom analizom koja uzima u obzir sve relevantne okolnosti (Knežević, 2024). Praksa država pokazuje različite pristupe evidentnim standardima. Sjedinjene Države često oslanjaju na obaveštajne izvore koji nisu javno dostupni, što otežava međunarodnu verifikaciju atribucije (Eichensehr, 2017). Evropska unija insistira na transparentnijim procedurama i koordinaciji sa međunarodnim partnerima.

Složenost cyber atribucije dovela je do razvoja koncepta kolektivne atribucije, gde više država ili međunarodnih organizacija zajedno procenjuje odgovornost za određene cyber operacije (Eichensehr, 2017). Ovaj pristup može povećati kredibilitet atribucije i smanjiti mogućnost političke instrumentalizacije. Primer kolektivne atribucije predstavlja zajednička izjava EU, NATO-a i partnera o odgovornosti Rusije za NotPetya ransomware napad 2017. godine. Iako ova atribucija nije imala direktne pravne posledice, predstavlja važan precedent za koordinirani međunarodni odgovor (EU Council, 2018). Međunarodna saradnja u cyber atribuciji suočava se sa izazovima vezanim za razmenu obaveštajnih informacija, različite pravne sisteme i političke senzitivnosti. Budapeštanska konvencija o cyber kriminalu predstavlja najsveobuhvatniji pravni okvir za međunarodnu saradnju, ali se fokusira na kriminalne radnje a ne na državne cyber operacije (Council of Europe, 2001).

4. EVOLUCIJA MEĐUNARODNO-PRAVNIH NORMI U CYBER DOMENU

Trenutni međunarodno-pravni okvir za cyber operacije zasniva se na primeni postojećih normi međunarodnog prava na novo tehnološko okruženje. Povelja Ujedinjenih nacija, Međunarodni pakt o građanskim i političkim pravima, međunarodno humanitarno pravo i običajno međunarodno pravo čine osnovu ovog okvira (Schmitt, 2017).

Član 2(4) Povelje UN, koji zabranjuje pretnju silom ili upotrebu sile u međunarodnim odnosima, primenjuje se na cyber operacije koje dostižu

nivo «oružane agresije». Međutim, definisanje praga za ovu klasifikaciju ostaje kontroverzno. Tallinn Manual sugeriše da cyber operacije koje uzrokuju fizičku štetu ili žrtve mogu biti smatrane upotrebom sile, ali ova interpretacija nije univerzalno prihvaćena (Schmitt, 2013). Pravo na samoodbranu, ustanovljeno članom 51 Povelje UN, takođe se primenjuje na cyber napade koji dostižu nivo "oružane agresije". Slučaj Estonia (2007) postavlja pitanje da li DDoS napadi koji parališu nacionalnu infrastrukturu mogu opravdati samoodbranu, uključujući kinetičke odmazde. Međunarodno humanitarno pravo primenjuje se na cyber operacije tokom oružanih sukoba, zahtevajući poštovanje principa razlikovanja, proporcionalnosti i predostrožnosti (Dinstein, 2012). Cyber napadi na civilne objekte su zabranjeni, ali klasifikacija "dual-use" infrastrukture (kao što su električne mreže) ostaje problematična (Vejnović & Knežević, 2024).

U odsustvu sveobuhvatnog multilateralnog okvira, države razvijaju regionalne i bilateralne sporazume za regulaciju cyber pitanja. Evropska unija usvojila je Direktivu o bezbednosti mreža i informacionih sistema (NIS Directive) koja uspostavlja minimum standarde za cyber bezbednost među članicama (EU, 2016). NATO je kroz članak 5 Severnoatlantskog ugovora proširio koncepty kolektivne odbrane na cyber domen, mada je praktična implementacija ove politike još uvek nedefinisana (NATO, 2016). Shanghai Cooperation Organization razvila je alternativni pristup koji naglašava informacionu bezbednost i suverenitet u cyber prostoru (SCO, 2011). Bilateralni sporazumi između velikih sila, kao što su američko-kineski dogovori o zabrani cyber špijunaže u komercijalnom sektoru, predstavljaju pragmatičan pristup specifičnim problemima (White House, 2015). Međutim, ovi sporazumi su često politički motivisani i imaju ograničenu pravnu snagu.

Potreba za sveobuhvatnim međunarodnim pravnim instrumentom za cyber prostor postaje sve očiglednija. Predlozi uključuju novu konvenciju pod okriljem UN, proširenje postojećih sporazuma ili razvoj "soft law" instrumenata kroz Group of Governmental Experts (GGE) ili Open-ended Working Group (OEWG) (UN, 2021). Glavni izazovi za postizanje konsenzusa uključuju različite koncepte cyber suverenosti, neslaganja oko definicije cyber napada, i geopolitičke tenzije između glavnih aktera. Zapadne zemlje zagovaraju otvoreni, slobodan cyber prostor zasnovan na vladavini prava, dok autoritarni režimi insistiraju na državnoj kontroli

i informacionoj suverenosti (Mueller, 2017). Hibridni pristup koji kombinuje obavezujuće norme za najserijnoɜnije cyber pretnje sa soft law instrumentima za operativne standarde možda predstavlja najrealističniju opciju. Ovaj pristup bi omogućio postupnu harmonizaciju nacionalnih zakonodavstava i uspostavljanje minimum međunarodnih standarda.

5. PRAKTIČNI IZAZOVI IMPLEMENTACIJE JURISDIKCIJSKIH OKVIRA U CYBER PROSTORU

Implementacija teorijskih okvira državne jurisdikcije u praktičnom kontekstu cyber operacija suočava se sa nizom kompleksnih problema koji zahtevaju multidisciplinarni pristup koji kombinuje pravne, tehnološke i političke elemente. Praksa država u poslednjih petnaest godina otkriva značajnu razliku između normativnih očekivanja i operativnih mogućnosti kada je reč o vršenju jurisdikcije nad cyber incidentima koji prevazilaze nacionalne granice. Jedan od najznačajnijih praktičnih izazova predstavlja problem sinhronizacije nacionalnih zakonodavstava koja regulišu cyber kriminal i cyber bezbednost. Analiza postojećih pravnih sistema pokazuje da se definicije osnovnih pojmova kao što su "neovlašćen pristup", "računarski sabotaža", ili "cyber špijunaža" značajno razlikuju među državama, što otežava međunarodnu saradnju u istrazi i procesuiranju prekograničnih cyber incidenata (Simović, Vejnović & Knežević, 2024). Na primer, ono što jedna država klasifikuje kao "hakovanje" druga može smatrati legitimnim penetracionim testiranjem ili istraživanjem bezbednosnih propusta, što stvara pravnu nesigurnost za međunarodne aktere koji deluju u cyber prostoru.

Problematika je dodatno komplikovana činjenicom da cyber operacije često uključuju "živi dokazi" koji mogu biti izmenjeni, obrisani ili premešteni za vreme trajanja istrage. Za razliku od tradicionalnih krivičnih dela gde fizički dokazi obično zadržavaju svoj integritet tokom istražnog procesa, digitalni dokazi zahtevaju specijalizovane procedure za čuvanje, analizu i prezentaciju pred sudskim organima. Ova specifičnost zahteva ne samo harmonizaciju materialnih normi već i usklađivanje procesnih standarda među različitim jurisdikcijama. Međunarodna praksa pokazuje da su države razvile različite pristupe problemu multi-jurisdikcionih cyber incidenata. Sjedinjene Države primenjuju agresi-

van pristup eksteritorijalnoj jurisdikciji, često pozivajući se na "efekte doktrine" kada cyber operacije imaju posledice na američkoj teritoriji, bez obzira na lokaciju servera ili nacionalnost aktera. Ovaj pristup je ilustrovan u slučaju United States v. Bout (2011), gde su američke vlasti proširile svoju jurisdikciju na cyber aktivnosti koje su imale "razumno predvidljive efekte" na američke interese. Evropska unija, s druge strane, razvija pristup zasnovan na "značajnoj povezanosti" koji zahteva da postoji suštinska veza između cyber operacije i teritorije države koja želi da vrši jurisdikciju (Knežević, 2024).

Tehnološki razvoj predstavlja kontinuirani izazov za pravnu praksu, jer tradicionalni mehanizmi identifikacije lokacije - kao što su IP adrese - postaju sve manje pouzdani zbog korišćenja VPN mreža, Tor pregledača, i distribuiranih cloud computing sistema. Praksa "jurisdiction shopping" gde cyber kriminalci svesno biraju jurisdikcije sa slabijim zakonodavstvom ili ograničenim kapacitetima za saradnju dodatno komplikuje problem. Ovaj fenomen je posebno izražen u slučaju ransomware operacija koje se često izvršavaju iz zemalja koje ne ekstradiraju svoje državljane ili imaju ograničenu saradnju sa zemljama žrtvama. Finansijski aspekt cyber operacija predstavlja dodatnu dimenziju jurisdikcionih izazova. Moderne cyber operacije često uključuju složene finansijske tokove koji prolaze kroz multiple jurisdikcije, koristeći kriptovalute, online platforme za plaćanje, i offshore finansijske centre. Praćenje i zamrzavanje sredstava povezanih sa cyber kriminalom zahteva koordinaciju između različitih pravnih sistema sa različitim standardima za finansijsku forenziku i međunarodnu pravnu pomoć. Slučaj Colonial Pipeline ransomware napada (2021) ilustruje ove izazove - dok je bilo moguće pratiti tok bitcoina korišćenih za plaćanje otkupnine, praktično povraćaj sredstava zahtevao je koordinaciju između američkih, britanskih i nekoliko drugih jurisdikcija.

Uloga privatnog sektora u vršenju de facto jurisdikcije u cyber prostoru predstavlja još jedan neistražen aspekt praktične implementacije (Vejnović & Knežević, 2025). Velike tehnološke kompanije kao što su Google, Microsoft, Facebook i Amazon kontrolišu značajan deo cyber infrastrukture i često imaju veće tehničke kapacitete za identifikaciju, praćenje i prekidanje cyber operacija nego mnoge državne agencije. Ova realnost postavlja fundamentalna pitanja o delegaciji tradicionalno državnih funkcija privatnim akterima i potrebi za regulacijom njihovih ak-

tivnosti u kontekstu državne jurisdikcije. Praksa "active defense" i "hack back" operacija koje izvršavaju privatne kompanije dodatno komplikuje jurisdikcijska pitanja. Kada američka kompanija odgovori na cyber napad koji potiče iz druge zemlje tako što pristupi haker serverima u trećoj zemlji, postavlja se pitanje koja država ima pravo da reguliše ovu aktivnost i po kojim kriterijumima. Trenutno pravo ne pruža jasne odgovore na ove situacije koje postaju sve češće u praksi.

Proceduralni aspekti međunarodne pravne pomoći u cyber slučajevima pokazuju dodatne praktične probleme. Tradicionalni mehanizmi kao što su zahtevi za pravnu pomoć (MLA requests) često su presporebni za cyber kontekst gde dokazi mogu biti obrisani za vreme potrebno za formalnu komunikaciju između država. Razvoj ekspeditovanjih procedura za cyber slučajeve postaje imperativ, ali zahteva pažljivo balansiranje između brzine odgovora i zaštite suvereniteta i ljudskih prava. Kapacitet manjijih država da efikasno vrše jurisdikciju u cyber prostoru predstavlja značajan izazov za globalnu cyber bezbednost. Mnoge zemlje u razvoju nemaju tehničke, finansijske ili ljudske resurse potrebne za istrajgu sofisticiranih cyber operacija, što stvara "sigurnosne krajnje" koje mogu biti eksploatisane od strane cyber kriminalaca. Međunarodne organizacije kao što su ITU, UNODC i Interpol razvijaju programe za jačanje kapaciteta, ali ovi napori su još uvek nedovoljni u odnosu na obim problema.

Kulturni i jezički faktori takođe igraju značajnu ulogu u praktičnoj implementaciji jurisdikcijskih okvira. Cyber operacije često uključuju socijalni inženjering i tehnike koje su specifične za određene kulture i jezike, što zahteva kulturno senzitivnu analizu dokaza i međunarodnu saradnju koja poštuje ove različitosti. Dodatno, različita shvatanja privatnosti, državne bezbednosti i slobode izražavanja među kulturama mogu komplikovati saradnju u slučajevima koji imaju političke ili bezbednosne implikacije. Vremenska dimenzija cyber operacija predstavlja dodatni praktični izazov. Za razliku od tradicionalnih krivičnih dela koji se obično dešavaju u određenom vremenskom okviru, cyber operacije mogu biti dugotrajne, ponavljane ili latentne, aktivirajući se tek nakon značajnog vremenskog perioda. Ova karakteristika komplikuje primenu statute of limitations i drugih vremenskih ograničenja u različitim pravnim sistemima, posebno u slučajevima koji zahtevaju koordinaciju između više jurisdikcija sa različitim vremenskim okvirima za krivično gonjenje.

6. SUDSKA PRAKSA I PRECEDENTI U CYBER JURISDIKCIJI

Razvoj sudske prakse u oblasti cyber jurisdikcije predstavlja kritičan faktor za razumevanje praktične primene teorijskih okvira međunarodnog prava u digitalnom domenu. Analiza ključnih sudskih odluka na nacionalnom i međunarodnom nivou otkriva postupno oblikovanje novih pravnih standarda koji nastoje da odgovore na jedinstvene izazove koje cyber operacije postavljaju pred tradicionalne koncepte jurisdikcije i državne odgovornosti. Pionirski slučaj u ovoj oblasti predstavlja Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme (2000), gde je francuski sud ustanovio jurisdikciju nad američkom kompanijom zbog sadržaja koji je bio dostupan francuskim korisnicima preko interneta. Ova odluka je postavila važan precedent za princip "targeting" koji omogućava državama da vrše jurisdikciju nad inostranim akterima čiji sadržaj ili aktivnosti ciljaju njihove državljane. Međutim, pokušaj implementacije ove odluke u američkom pravnom sistemu je rezultovao konfliktom jurisdikcija i postavio pitanje o granicama eksteritorijalnog vršenja jurisdikcije u cyber prostoru.

Značajan doprinos razvoju cyber jurisdikcije dao je Evropski sud za ljudska prava u slučaju Delfi AS v. Estonia (2015), gde je sud razmatrao odgovornost online platformi za korisnički sadržaj u kontekstu slobode izražavanja. Sud je uspostavio da online platforme mogu nositi odgovornost za sadržaj koji objavljuju korisnici ukoliko ne preduzmu razumne mere za moderaciju, što je imalo dalekosežne posledice za razumevanje jurisdikcijskih obaveza u cyber prostoru. Ovaj slučaj je također demonstrirao kako se tradicionalna ljudska prava primenjuju u digitalnom kontekstu i kako nacionalni sudovi mogu vršiti jurisdikciju nad aktivnostima koje se odvijaju u cyber prostoru. Američka sudska praksa razvila je specifičan pristup cyber jurisdikciji kroz seriju landmark odluka. U slučaju United States v. Gorshkov (2001), federalni sud je uspostavio da američki organi imaju jurisdikciju da istražuju cyber napade koji ciljaju američke žrtve, čak i kada se izvršavaju iz inostranstva. Sud je primenio princip "effects doctrine" argumentujući da cyber operacije koje imaju efekte na američkoj teritoriji potpadaju pod američku jurisdikciju bez obzira na fizičku lokaciju izvršilaca. Ovaj pristup je dalje razvijen u slučaju United

States v. Ivanov (2000), gde je sud proširio jurisdikciju na ruski državljanina koji je iz Rusije izvršio cyber napade na američke kompanije.

Evropska sudska praksa pokazuje oprezniji pristup eksteritorijalnoj jurisdikciji u cyber slučajevima. Slučaj Glawischnig-Piesczek v. Facebook (2019) pred Sudom pravde Evropske unije postavlja važne principe za jurisdikciju nad multinacionalnim tech kompanijama. Sud je uspostavio da nacionalni sudovi mogu naložiti uklanjanje nezakonitog sadržaja sa globalnih platformi, ali samo u granicama svoje teritorijalne jurisdikcije. Ova odluka pokušava da balansira nacionalnu jurisdikciju sa praktičnostima globalnog interneta i postavlja ograničenja na eksteritorijalnu primenu nacionalnih zakona. Međunarodna praksa arbitraže takođe doprinosi razvoju cyber jurisdikcije. Slučaj Yukos v. Russia (2014) pred Permanentnim arbitražnim sudom u Hagu, iako nije direktno cyber slučaj, uspostavio je važne principe za utvrđivanje državne odgovornosti za aktivnosti koje se izvršavaju kroz kompleksne korporativne strukture koje mogu biti relevantne za cyber operacije izvršene kroz proxy organizacije ili nedržavne aktere.

Praksa nacionalnih sudova u slučajevima cyber kriminala otkriva različite pristupe problemu multi-jurisdikcionih cyber operacija. Nemački Bundesgerichtshof u slučaju BGH 1 StR 266/18 (2018) uspostavio je da se jurisdikcija može etablirati na osnovu lokacije servera čak i kada su korisnici i administratori u različitim zemljama. Ovaj pristup daje značaj fizičkoj infrastrukturi u određivanju jurisdikcije, što je u suprotnosti sa pristupima koji se fokusiraju na efekte ili ciljanje.

Britanska sudska praksa, posebno kroz slučajeve pred High Court of Justice, razvila je sofisticirani pristup cyber jurisdikciji koji kombinuje tradicionalne common law principe sa specifičnostima digitalnog okruženja. Slučaj Soriano v. Forensic News LLC (2021) ilustruje kako britanski sudovi primenjuju "forum conveniens" test u cyber slučajevima, razmatrajući faktore kao što su lokacija servera, jezička dostupnost sadržaja i ciljana publika.

Azijski pravni sistemi pokazuju jedinstvene pristupe cyber jurisdikciji koji reflektuju različite kulturne i pravne tradicije. Japanski Vrhovni sud u slučaju związanych sa cyber mobbing (2017) uspostavio je da jurisdikcija može biti zasnovana na lokaciji žrtve bez obzira na lokaciju izvršioca, što predstavlja proširenje tradicionalnog pasivnog personalnog principa. Sin-

gapurski Court of Appeal u slučaju Ng Kek Wee v. Sim City Technology Ltd (2014) razvio je test "real and substantial connection" za cyber slučajeve koji zahteva značajnu povezanost između spora i jurisdikcije.

Praksa međunarodnih krivičnih sudova, iako ograničena u oblasti cyber kriminala, pruža važne uvide u primenu međunarodnog prava na digitalne aktivnosti (Knežević & Martinović, 2024). Međunarodni krivični sud u svojim preliminary rulings razmatrao je kako se cyber operacije mogu uklapati u postojeće definicije ratnih zločina i zločina protiv čovečnosti, što ima implikacije za jurisdikciju u slučajevima cyber warfare. Administrativni i regulatorni postupci takođe doprinose razvoju cyber jurisdikcije. Evropska komisija kroz svoje odluke o zaštiti podataka, posebno u implementaciji GDPR-a, uspostavlja precedente za eksteritorijalnu primenu evropskih standarda na ne-evropske kompanije. Slučaj Google Spain SL v. Agencia Española de Protección de Datos (2014) uspostavio je "right to be forgotten" princip koji ima globalne implikacije za cyber jurisdikciju i demonstrira kako *administrative bodies* mogu efektivno vršiti jurisdikciju u cyber prostoru.

Razvojni trend u sudskoj praksi pokazuje postepeno pomeranje od striktno teritorijalnih pristupa ka fleksibilnijim okvirima koji uzimaju u obzir realnosti globalnog interneta. Međutim, ova evolucija nije uniformna i različiti pravni sistemi nastavljaju da razvijaju divergentne pristupe, što stvara pravnu nesigurnost za međunarodne aktere. Potreba za harmonizacijom sudske prakse (Martinović, 2025) kroz međunarodne instrumente ili model zakonodavstvo postaje sve očiglednija kao način rešavanja ovih nekonzistentnosti. Budući razvoj sudske prakse u cyber jurisdikciji verovatno će biti oblikovan rastućim brojem slučajeva koji uključuju nove tehnologije kao što su veštačka inteligencija, IoT uređaji i blockchain tehnologija. Ove tehnologije postavljaju dodatne izazove za traditionalne koncepte jurisdikcije i zahtevaju dalju evoluciju pravnih standarda.

7. ZAKLJUČAK

Analiza pravnog režima državne jurisdikcije u cyber prostoru i međunarodno-pravnog okvira za atribuciju odgovornosti za transnacionalne cyber operacije otkriva fundamentalne izazove koje digitalna era postavlja pred tradicionalno međunarodno pravo. Istraživanje pokazu-

je da postojeći pravni okviri, razvijani za fizičke territorije i konvencionalne bezbedonoste pretnje, zahtevaju značajnu adaptaciju za efikasnu primenu u virtualnom domenu. Teritorijalni princip jurisdikcije, kao kamen temeljac vestfalskog sistema, pokazuje svoje ograničenja u cyber prostoru gde koncept "mesta" postaje fluidna i često neodrediva kategorija. Virtualna teritorijalnost, kao pokušaj premošćavanja ove praznine, pruža parcijalno rešenje ali istovremeno generiše nove probleme preklapajućih jurisdikcija i pravne nesigurnosti. Personalni princip, mada konceptualno primenljiv, suočava se sa praktičnim preprekama identifikacije i verifikacije identiteta cyber aktera. Atribucija odgovornosti za cyber operacije predstavlja možda najsloženiji aspekt ove problematike. Postojeći test "efektivne kontrole" iz slučaja Nicaragua teško je primenljiv na cyber domein gde nedržavni akteri mogu delovati sa različitim stepenom autonomije od državnih sponzora. Potreba za novim evidentnim standardima i procedurama tehnične atribucije postaje imperativ za kredibilnu primenu međunarodnog prava u cyber prostoru. Evolucija međunarodno-pravnih normi u cyber domenu pokazuje fragmentiran pristup bez jasnog konzensusa o fundamentalnim principima. Regionalni i bilateralni sporazumi pružaju parcijalna rešenja ali ne mogu zameniti potrebu za sveobuhvatnim multilateralnim okvirom. Geopolitičke podele oko koncepta cyber suverenosti dodatno komplikuju postizanje međunarodnog konsenzusa.

Za buduće razvoje u ovoj oblasti, ključno je uspostavljanje hibridnog pravnog okvira koji kombinuje adaptaciju postojećih normi međunarodnog prava sa razvojem specifičnih instrumenata za cyber domen. Ovaj okvir mora uključiti jasne kriterijume za uspostavljanje jurisdikcije u cyber prostoru, standardizovane procedure za atribuciju cyber operacija i mehanizme za međunarodnu saradnju u istrazi i procesuiranju cyber incidenata. Konačno, međunarodna zajednica mora prepoznati da cyber prostor nije "pravni vakuum" već domen gde se postojeće međunarodno pravo primenjuje uz potrebu za specifičnim adaptacijama. Jedino kroz koordinisan međunarodni pristup koji balansira tehnološke realnosti sa pravnim principima moguće je uspostaviti stabilan i predvidiv pravni režim za cyber prostor koji će služiti interesima sve više digitalizovane međunarodne zajednice.

8. LITERATURA

1. Brenner, S. W. (2007). *Law in an era of "smart" technology*. Oxford University Press.
2. Brownlie, I. (2008). *Principles of public international law* (7th ed.). Oxford University Press.
3. Buchan, R. (2018). Cyber attacks: Unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law*, 17(2), 212-227.
4. Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
5. Dinstein, Y. (2012). Cyber war and international law: Concluding remarks at the 2012 Naval War College International Law Conference. *International Law Studies*, 89, 276-285.
6. Eichensehr, K. E. (2017). The cyber-law of nations. *Georgetown Law Journal*, 103(2), 317-380.
7. EU Council. (2018). *Declaration by the High Representative on behalf of the EU on malicious cyber activities*. Press release 133/18.
8. European Union. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1.
9. International Court of Justice. (1986). *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America). ICJ Reports 1986.
10. International Law Commission. (2001). *Articles on Responsibility of States for Internationally Wrongful Acts*. UN Doc. A/56/10.
11. Johnson, D. R. & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48(5), 1367-1402.
12. Knežević, S. (2015). *Rat po mjeri Pentagona: Građanski rat u Siriji i Iraku*. Narodna biblioteka „Ivo Andrić".
13. Knežević, S. (2017). *Kako su srušili Jugoslaviju: Od 14-og kongresa SKJ do proglašenja nezavisnosti Kosova*. Udruženje građana za književnu i publicističku djelatnost „Slovo".

14. Knežević, S. (2024). *Prauzrok: nacrt za uvod u morfologiju kosmologije, evolucije i teogonije*. Metaphysica.
15. Knežević, S. (2024). *The High Representative and the Constitutional Crisis in Bosnia and Herzegovina*. Svarog, 15(28), 139-161. http://dx.doi.org/10.7251/SVR2428139K
16. Knežević, S. (2025). Krivičnopravna zaštita ustavnog poredka SFRJ. *Godišnjak Pravnog fakulteta Univerziteta u Banjoj Luci*, 46(46), 103-128, DOI https://doi.org/10.63356/gpf.2024.006
17. Knežević, S. (2025). *Imperijalna prenapregnutost Sjedinjenih Američkih Država i Specijalna vojna operacija u Ukrajini*. Banja Luka: Evropski defendologija centar.
18. Knežević, S. (2025). Dekodiranje genocidne namjere: pravna evolucija dokaznih standarda u digitalnoj eri. *Godišnjak Fakulteta pravnih nauka*, 267-286.
19. Martinović, T. (2025) *Sport Diplomacy and Security Challenges during the Cold War*. Defendologija, 55, 151-166.
20. Mueller, M. (2017). *Will the Internet fragment? Sovereignty, globalization and cyberspace*. Polity Press.
21. NATO. (2016). *Warsaw Summit Communiqué*. Press Release 100/16.
22. Rid, T. & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), 4-37.
23. Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press.
24. Ryngaert, C. (2015). *Jurisdiction in international law* (2nd ed.). Oxford University Press.
25. Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.
26. Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
27. Shanghai Cooperation Organization. (2011). *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*.

28. Simović, M., Vejnović, D. & Knežević, S. (2025). Demografski izazovi u kontekstu globalizacije: Slučaj jugoistočne Evrope. Demografske i etničke promjene u Bosni i Hercegovini od 2013. do 2024. godine, 69-97.
29. Svantesson, D. J. (2013). *Private international law and the internet* (3rd ed.). Kluwer Law International.
30. Tikk, E., Kaska, K. & Vihul, L. (2010). *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence.
31. United Nations. (2021). *Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*. UN Doc. A/76/135.
32. Vejnović, D. & Knežević, S. (2024). Hegemonija u unipolarnom svijetu: izazovi i posljedice za međunarodno pravo. Bezbjednost zemalja regiona u svjetlu nove bezbjednosne arhitekture, 7-30.
33. Vejnović, D. & Knežević, S. (2025). *Primjena digitalne forenzike u otkrivanju cyber kriminala*. Savremeni izazovi i prijetnje bezbijednosti, 422-442.
34. White House. (2015). *Fact Sheet: President Xi Jinping's State Visit to the United States*. Office of the Press Secretary.

Rad zaprimljen: 15.5.2025.
Rad odobren: 30.6.2025.