SAJBER KRIMINAL – GLOBALNI MEĐUNARODNI IZAZOV

DA LI JE KONVENCIJA O VISOKOTEHNOLOŠKOM KRIMINALU ADEKVATAN INSTRUMENT U BORBI?

AUTOR: Katarina Jonev[1]

APSTRAKT:

Zbog rastućih pretnji u sajber prostoru, postalo je jasno da mnogobrojni tradicionalni krivični zakoni nisu dovoljno precizni niti adekvatni da odgovore na sajber zločine. Veliki broj država ima svoju zakonsku regulativu koja reguliše ovu oblast ali ne postoji konzistentnost među njima. Nedostaju adakvatne akcije u sprečavanje visokotehnološkog kriminala I sajber napada koji ugrožavaju nacionalnu bezbednost ugrožavajući političku, vojnu I ekonomsku stabilnost država. Shodno tome, bilo je više poziva na povećanu regulaciju i upravljanje aktivnostima na Internetu. Potrebno je da države zajedničkim snagama učestvuju u stvaranju globalnog dokumenta koji se tiče ove oblasti. Konvencija o viskotehnološkom kriminalu Saveta Evrope, poznata I kao Budimpeška konvencija, prvi je I za sada jedini multilateralni međunarodni ugovor koji se bavi nelegalnim aktivnostima počinjenim preko Interneta i korišćenjem kompjuterskih mreža. Konvencija je važan korak u daljem razvijanju sajber prava I definisanja nelegalnih kriminalnih aktivnosti počinjenih upotrebom računara.

POTREBA DRŽAVA ZA REGULISANJEM SAJBER KRIMINALNIH AKTIVNOSTI

Internet, IKT tehnologija koja ga podupire kao I računarski sistemi su poslednje dve decenije učinile naš svet umreženijim, a život olakšanim. Učimo, radimo, poslujemo, zarađujemo, komuniciramo, funkcionišemo, u sajber prostoru. Zavisnost država, nacionalnih infrastuktura, organizacija, civilnog sektora, korporacija, individua od Interneta je sve primetnija. Rastuća potreba za aktivnostima u sajber prostoru nažalost, nije dovoljno uticala da ga sačuvamo bezbednim.

---

[1] Diplomirani politikolog za međunarodne odnose, Master međunarodnog prava

Zbog velikih ulaganja i uspešnog poslovanje u IT sektoru koji konstantno beleži rast, neophodne su nove veštine za zaštitu od sajber napada. Nedostatak zakona u sajber prostoru kao I sama transnacionalna priroda opasnosti, zatim različita praksa država I ograničena međunarodna saradnja, ohrabruju formiranje i globalno poslovanje organizovanog sajber kriminala koji generiše ogromne prihode. Iako na globalnom nivou ne postoji zajednički pogled o tome šta predstavlja nezakonite aktivnosti na Internetu, niti su takvi akti taksativno pobrojani u jednom globalnom dokumentu, većina akademika I stručnjaka za bezbednost se slaže da je visokotehnološki kriminal jedan od najbrže rastućih oblika kriminala[2].

Svakoj državi je u interesu da donese zakone iz oblasti zaštite od sajber kriminala kao I da stvori efikasan mehanizam sprovođenja tih prava. Doslednost, efikasnost I stručnost su nužni u tom procesu I stoje rame uz rame sa samom potrebom stvaranja akata koje se tiču ove oblasti. Činjenica je da su pored donošenja zakona potrebni I kapaciteti izvršenja. Mnoge policijske snage država nisu opremljene da reaguju u sprečavanju visokotehnološkog kriminala ili nemaju mogućnost da to na adekvatan način učine.

Kada se priča o sajber kriminalu, mora se uzeti u obzir njegova specifičnost. Napadača nije uvek moguće identifikovati, utvrditi odakle je napad sproveden, što dodatno otežava mogućnost istrage, krivičnog gonjenja, I izvođenje pred Sud.

Države se zalažu za povećanje regulacije i upravljanja Internet aktivnostima kao I za formiranje globalnog odgovora na sajber pretnje. Sajber napadi I sajber kriminalne aktivnosti ne treba tumačiti kao ‘’sivu zonu prava’’ već kao realnost koju treba regulisati u što hitnijem roku. Ovo je transnacionalna pretnja koja je poznaje granice I svako može biti meta. Međutim, iako velika većina država I međunarodnih organizacija slaže da sajber kriminal predstavlja značajan problem, malo je konsenzusa o tome kako da se taj isti problem reši.

POZIV SAVETA EVROPE NA AKCIJU

Sa razvojem Interneta I samog sajber prostora evaluirali su sajber zločini različitih oblika.

---

[2] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

1989. godine Savet Evrope je objavio je niz preporuka koje se odnose na kriminalne aktivnosti počinjene putem računarskih mreža[3]. Studija iz 1995. godine[4], pokazala je da su zakoni koji se tiču ove oblasti nekoherentni I neadekvatni a da u mnogim zemljama uopšte I ne postoje. Iako se velika većina savremenog društva slaže da sajber kriminal predstavljaja značajan problem, malo je konsenzusa na globalnom nivou kako pristupiti rešavanju ovog problema[5].

Jedna grupa država je reagovala na poziv Saveta Evrope I učestvovala u izradi Konvencije o visokotehnološkom kriminalu. Konvencija poziva države članice da stvore nove zakone koji se odnose na različite zločine počinjene na ili upotrebom Interneta, i apeluje na povećanu saradnju između bezbedonosnih agencija zemalja kako bi se istrage krivičnih dela efikasnije sprovodile. Savet Evrope, organizacija 47 evropskih zemalja, imenovao je 1997.godine Komitet eksperata za kriminal u sajber prostoru[6], sa ciljem da identifikuju i definišu nove zločine, nadležnost prava i obaveze koje se tiču krivičnih dela počinjenih na Internetu. Cilj je bio da se stvori set zakona koji se odnose na sajber kriminalne aktivnosti i da se formira zajednička politika zaštite protiv sajber opasnosti koje vrebaju.

Konvencija o visokotehnološkom kriminalu (ETS 185)[7], pripremljena od strane Saveta Evrope uz saradnju SAD, Kanade i Japana, prvi je međunardni ugovor koji se bavi sajber kriminalnim aktivnostima i idalje je jedini globalni dokument koji se bavi ovom problematikom. Dokument je prvi međunarodni pokušaj da se definišu sajber zločini i da se razvije politika za sprečavanje određenih krivičnih dela korišćenjem Interneta I računarskih sistema. Usvojena je u junu 2001.godine i otvorena za potpisivanje u Budimpešti 23. novembra 2001. godine. Konvencija je stupila na snagu 1. jula 2004. godine[8]. Otvorena je za pristup svim zemljama i jedini je obavezujući međunarodni sporazum za ovu oblast koji je do danas usvojen. Protokol o

---

[3] Preporuka No. R. (89) 9 Komiteta Ministara u vezi sajber kriminala dostupno na: http://www.cm.coe.int/ta/rec/l989/89r9.

[4] Preporuka No. R. (95) 13 Komiteta Ministara koji se tiču problematike proceduralnog prava sa IT tehnologijom Dostupno na: http://www.coe.int/ta/rec/l995/95r13htm

[5] Amalie M. Weber,The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425 (2003) str 427 Available at: http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28

[6] Jonathan Clough ‘’A world of difference: the Budapest Convention on cybercrime and the challenges of harmonisation’’, International Serious and Organised Crime Conference, Brisbane, 29–30 July 2013.

[7] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[8] Sporazum je stupio na snagu nakon što je pet država , uključujući I najmanje tri države članice Saveta Evrope, ratifikovala. Američki Senat ratifikovao je ugovor 3. avgusta 2006. godine .

kažnjavanju akata rasizma i ksenofobije učinjene korišćenjem kompjuterskih sistema (ETS 189) je otvoren za potpisivanje januara 2003. godine i na snazi je od marta 2006. godine.

Budimpešku Konvenciju je ratifikovalo 45 zemalja (zemlje EU i SAD); potpisalo ju je 53 (zemlje EU, Kanada, Japan, Južnoafrička Republika, članice NATO-a). Poslednja država koja je ratifikovala Konvenciju je Panama (1.3.2014)[9].

Konvencija se koristi kao smernica, referentni standard i model za zakone u više od 100 zemalja. Pored toga, Konvenciju podupiru, i na nju se pozivaju i druge organizacije, među kojima su: Evropska Unija, Organizacija američkih država, OEBS, Azijsko-pacifička ekonomska saradnja; Interpol kao i pripadnici privatnog sektora. Konvencija je otvorena ne samo za članove Saveta Evrope ili nečlanica koje su učestvovale u njenoj izradi već mogu da pristupe i druge države shodno svojoj volji. Ruska Federacije je, između ostalih, jedna od država koja je dobila poziv da je ratifikuje i implementira u svoje zakonodavstvo. To nije učinila.

SADRŽAJ KONVENCIJE

Konvencija o sajber kriminalu je prvi istinski pokušaj rešavanja problema međunarodnog sajber kriminala. Obuhvata: odredbe usmerene ka borbi protiv kriminalnih aktivnosti i krivična dela počinjenih korišćenjem Interneta i kompijutera; neovlašćen pristup kompjuterskom sistemu; nedozvoljeno presretanje i oštećenje podataka; zloupotrebu uređaja; kompjutersku prevaru; distribuiranje dečije pornografije; povredu autorskih prava i prava intelektualne svojine; sugeriše sredstva za efikasnu istragu i zaštitu[10]. Primenjuje se na bilo koji prestup počinjen putem kompjuterskog sistema i na sve dokaze u elektronskoj formi. Konvencija takođe deluje kao okvir za međunarodnu saradnju između zemalja po pitanju istrage i krivičnog gonjenja mogućih sajber zločina. Deo ugovora obuhvata I proceduru ekstradicije [11].

Konvencija od zemalja potpisnica traži da stvore osnovnu pravnu infrastrukturu neophodnu za efikasnu borbu protiv sajber kriminala i da pomažu drugim zemljama potpisnicama u istrazi i gonjenju sajber kriminalaca. Dokument predstavlja jedan osnovni ali i suštinski deo međunarodnog zakonodavstva. Pruža dobru zbirku pravnih i tehničkih definicija na osnovu kojih

[9] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
[10] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[11] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

se mogu razvijati drugi sporazumi o saradnji iz ove oblasti. Budući da postoji značajno preklapanje pojmova ali i suštinskih delovanja između sajber kriminala, sajber terorizma i sajber rata, kriminalizovanje svih vidova sajber napada, u Konvenciji, bez obzira na motive, znači da su države potpisnice, kada se to od njih traži, obavezne da uhvate i predaju krivičnom gonjenju sve međunarodne sajber kriminalce.

Sporazum je organizovan u četiri poglavlja. Svako poglavlje sadrži različite sekcije sa pojedinostima datim u 48 članova[12]. U prvom poglavlju se nalaze opšte definicije. Drugo poglavlje se fokusira na usklađivanje materijalnih i proceduralnih nacionalnih zakona u vezi sa sajberkriminalom. U trećem su detalji međunarodne saradnje dok je četvrto rezervisano za izvršenje, potpisivanje, ratifikaciju Ugovora.

Glavni cilj Budmipeške Konvencija je, kako stoji u samoj Preambuli, da bude zajednička vodilja državama u borbi protiv nelegalnih akata I da zaštiti društvo od sajber kriminala[13]. Ostvarivanje ovog cilja leži u pronalaženju zajedničkog rešenja na nedostatka krivičnog zakona, nedostatak procesnih ovlašćenja. kao i nedostatak uzajamnih izvršnih odredbi. Pobrojani nedostaci stvaraju jaz u nadleznosti po pitanju sajber kriminala. Savet Evrope je zahtevao da stranke potpisnice usvoje odgovarajuće zakonodavne mere protiv sajber kriminala čime bi se osiguralo uspešno implementiranje Konvencije. Predstavnici zakona moraju da imaju potrebne proceduralne alate za efikasno sprovođenje istrage i krivično gonjenje sajber kriminalnih dela kao I da obezbede uspešnu međunarodnu saradnju na ovom polju.[14]

Međutim, uzimajući u obzir činjenicu da svaka država donosi svoju posebnu perspektivu,
I svoju pravnu tradiciju, ‘’obojenu’’ kulturnim i istorijskim faktorima, kao I da veliki broj država nema čak ni osnovni set pravnih instrumenata koje se bave ovom tematikom, harmonizacija zakona, iako od ključnog značaja za efikasnu saradnju na polju sajber bezbednosti, nije uspela u potpunosti kako su tvorci Konvencije želeli.

---

[12] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[13] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[14] Amalie M. Weber,The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425 (2003). Available at: http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28

NAJBITNIJI (PRAVNI) ASPEKTI KONVENCIJE O VISOKOTEHNOLOŠKOM KRIMINALU

Konvecija je predložila da se kao kriminalna aktivnost deklariše 9 krivičnih dela podeljenih u 4 kategorije. U prvu kategoriju spadaju: "dela uspemerena protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema[15]''. U to spadaju: nelegalni pristup, nelegalno presretanje I ometanje podataka, smetnje na sistemu I zloupotreba uređaja[16]. U drugoj kategoriji "prekršaji počinjeni upotrebom računara", se nalaze odredbe koje pozivaju na kriminalizaciju kompjuterskih falsifikata i računarskih prevara[17]. "Prekršaji u vezi sa sadržajem[18]" zahtevaju kriminalizuju dela povezanih sa dečijom pornografijom. (Ova kategorija je dopunjena novim Protokolom usvojenim 7. novembar, 2002 a tiče se širenja rasističkog ili ksenofobičnog materijala preko računarskih sistema, prim.aut) Četvrti kategorija tiče se "prekršaja u vezi sa kršenjem autorskih i srodnih prava[19]''.

Konvencija Saveta Evrope o visokotehnološkom kriminalu sadrži odredbe usmerene na podsticanje međunarodne saradnje preko policijskih i pravosudnih mehanizama i privremenih mera u hitnim slučajevima, na primer, neformalno pružanje informacija po zahtevu (čl. 26)[20] i osnivanje kriznih centara koji su u mogućnosti da reaguju 24/7 (čl. 35)[21]. Takve odredbe mogu obezbediti pravni mehanizam koji omogućava korišćenje čak i neformalnih sredstava komunikacije i razmene informacija između stranka Konvencije, čak i ako one nemaju takvu odredbu u svom nacionalnom zakonodavstvu[22]. Sporazum daje policijskim snagama ovlašćenje da istraže i procesuiraju počinioce sajber zločina u okviru svog delokruga, odnosno u okviru nacionalnih granica.

Konvencija o sajber kriminalu bavi se proceduralnim pravnim pitanjima. Ona zahteva od država da uspostave minimalni set proceduralnih alata na nacionalnom nivou pri čemu su nadležni organi za sprovođenje zakona u država imaju ovlašćenje da vrše određene vrste istražnih

---

[15] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[16] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[17] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[18] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[19] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[20] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[21] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[22] Bendžamin Baklend i dr."Demokratsko upravljanje, Izazovi sajber bezbednosti", DCAF, Ženeva 2012. str. 41

aktivnosti specifičnih za sajber kriminal. Sporazum takođe uključuje odredbu kojom je država-učesnica nadležnost preko krivična dela počinjena na teritoriji te države[23]. Ovo znači da država ima nadležnost u kompjuterskom zločinu koji uključuje kompjuterski sistem na svojoj teritoriji, čak i ako je počinilac počinio krivično djelo iz daljinskom kontrolom sa lokacije koja se nalazi izvan granice države[24].Osim toga, Konvencija dodeljuje državi nadležnost nad građaninom te države koje počini krivično delo izvan državne granice, dokle god je ‘’to delo takođe kažnjivo krivičnim zakonom u državi u kojoj je počinjeno ili ako se krivično delo dogodilo izvan teritorijalne nadležnosti bilo koje države’’[25].

Od država koje nisu pristupile Konvenciji ne može se očekivati da sprovede odredbe sporazuma. Čak i one zemlje koje su ratifikovale sporazum, odredbe ne moraju izvršiti u potpunosti. Postoji mnogo primedbi na ugovor koji otežava njegovu punu primenu. Treba uzeti u obzir I neujednačenosti nacionalnih zakona država, što dodatno otežava kooperaciju. To ipak ne može umanjiti veliki doprinos donošenja Konvencije I važan korak u pravom smeru ka daljem unapređivanju brobe protiv kriminala I nedozvoljenih aktivnosti u sajber prostoru. Ovo je ipak najznačajniji međunarodni sporazum za rešavanje nelegalnog kompjuterskog kriminala. Konvencija Saveta Evrope jeste prvi veliki korak ali postoji niz nedostataka koji se odnose recimo na definicije termina, pitanja privatnosti, istražna ovlašćenja[26].

Iako je međunarodna perspektiva u borbi protiv sajber kriminala od vitalnog značaja, konsenzus je u isto vreme teško postići. Imajući to u vidu, upravo je sa tom namerom Savet Evrope pozvao predstavnike mnogih država, kako članica tako I onih koje to nisu, da uzmu učešće u izradi Konvencije, I uz kvalitetne diskusuje I predloge, raspravljaju o definicijama određenih radnji počinjenih na Internetu ili pomoću njega. Takođe, cilj je bio definisati odgovarajući mere koje bi bile prihvatljive za pokretanje efikasne borbe protiv sajber zločina.

Jedan od preduslova da Konvencija bude delotvorna jeste da joj mnogo veći broj zemalja pristupi i ratifikuje je, kao I da je implementira u svoja nacionalna zakonodavstva.

---

[23] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[24] Amalie M. Weber,The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425 (2003). http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28, str.432
[25] Ibid, str. 433
[26] Nancy E. Marion ‘’The Council of Europe’s Cyber Crime Treaty: An exercise in Symbolic Legislation’’, International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010

KRITIKA KONVENCIJE

Konvencija Saveta Evrope o sajber kriminalu naišla je na niz kritika. Jedno od najbitnijih je samo sprovođenje Konvencije - ne postoje međunarodna institucionalizovna kontrola koja bi nadgledala sprovođenje odredbi[27]. Takođe, Konvenciju odlikuje nedostatak globalnog učešća država u njenom pristupanju.

Ugovor se oslanja na međunarodnu saradnju u sprovođenju istrage i kažnjavanju sajber kriminalaca. S obzirom na neujednačenu razvijenost država i na različite pristupe ovoj problematici, može se zaključiti da su države različito opremljene za istraživanje sajber kriminala. Pošto ugovor nije pravno obavezujući, usklađivanje mera će imati samo ograničen efekat. Konvencija poziva na ‘’efikasnu saradnju državnih institucija I vlada država’’ što zvuči savršeno prihvatljivo u teoriji, ali vrlo je teško postići dobre I kvalitetne rezultate u praksi[28].

Postoje razlike između zemalja kada su u pitanju istrage sajber dela. Pojedine ne poseduju adekvatne resurse da odgovore na sajber pretnje. Neke zemlje mogu smatrati da nemaju nadležnost nad ovim delima jer nemaju razvijenu nacionalnu regulativu i zakonodavstvo koje se tiče ove materije[29]. Obučenost policijskih službi je različita. Iako su neke zemlje su uspostavile agencije sa zadatkom da koordiniraju istrage sajber kriminala, veliki broj njih nije. Na primer, Evropska unija je stvorila agenciju ENISA čiji je primarni zadatak koordinacija I vođenje istrage kompjuterskog kriminala u okviru zemalja članica[30]. Državama je takođe dozvoljeno da stave rezerve na pojedine odredbe ugovora, što može dovesti do nedoslednosti primene. Kada Američki Senat razmatrao Konvenciju, izabrao je da odustane od pojedinih odredbi. SAD zadržava pravo da ne primenjuje određene stavove Ugovora, i zadržava pravo da nametne druge pravne lekove umesto krivične odgovornosti kao što je predloženo u ugovoru[31].

---

[27] Nancy E. Marion ‘’The Council of Europe’s Cyber Crime Treaty: An exercise in Symbolic Legislation’’, International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010

[28] Walden, I. (2004). Harmonising Computer Crime Laws in Europe. European Journal of Crime, Criminal Law and Criminal Justice, 12(4), 321-336.

[29] Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013 © 2013 by NATO Cooperative Cyber Defence Centre of Excellence str 578

[30] http://www.enisa.europa.eu/about-enisa

[31] Nancy E. Marion ‘’The Council of Europe’s Cyber Crime Treaty: An exercise in Symbolic Legislation’’, International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010

Sajber kriminalce je teško locirati, pratiti a potom I krivično goniti. Računarski podatak je veoma nestabilna kategorija, jer se uz nekoliko komandi na tastaturi mogu izbrisati ključne informacije. Nije uvek lako locirati ili uopšte ući u trag izvršiocu krivičnog dela. Sajber kriminalci mogu biti veoma mobilni – ako se počini sajber zločin u jednoj državi, mogu se sakriti u drugoj. Oni će tražiti utočište u zemljama koje nisu ratifikovale sporazum, onim koje nemaju razvijana nacionalna zakonodavstva gde će biti relativno bezbedni od krivičnog gonjenja. To su uglavnom zemlje u razvoju i siromašne zemljama. U Konvencija nisu obuhvaćene sankcije za prekršaje. Umesto toga, svakoj zemlja je dozvoljeno da propiše sankcije u skladu sa njihovom kaznenom strukturom . To je takođe jedna od stavki koja se doživljava kao slabost ugovora[32].

Uprkos kritikama, značaj donošenja same Konvencije iz oblasti visokotehnološkog kriminala je ipak veći. Konvencija treba da posluži kao adekvatna smernica državama I preporuka je državama da joj pristupe koristeći je kao putokaz za kriminalne aktivnosti počinjene uz korišćenje kompijutera I Interneta.

ZAKLJUČAK

Bitanje sajber napada I sajber kriminalnih aktivnosti je u vrhu bezbedosnosnih izazova država I cele međunarodne zajednice. Tehnologija se razvija mnogo brže od međunarodnog sajber prava. Efikasna borba protiv visokotehnološkog kriminala zahteva globalnu saradnju I uključuje veći broj država nego što je trenutno potpisnica Konvencije. Pre same harmonizacije odnosno usklađenosti nacionalnih zakona potrebno je da države na svom unutrušnjem nivou prepoznaju problem I u skladu sa svojim kapacitetima I potrebama stvore set zakona kao I adekvatan sistem rešenja ove

[32] Coleman, C. (2003). Security Cyberspace—New Laws and Developing Strategies. *Computer Law and Security Repor*t, *19*(2), str. 131-136.

problematike. Svaka država u dogovoru sa svojom akademskom zajednicimo, bezbedonosnim službama, institucijama I IT sektorom, predstavnicima privrede, civilnim sektorom I lokalnim zajednicama treba da oformi sopstvenu sajber strategiju.

Konvencija Saveta Evrope je koristan instrument koji treba da potonjim međunarodnim Ugovorima bude vodilja. Njena simbolika je velika I značajna kao I putokazi propisani u dokumentu. U vremenu koje dolazi, biće neophodno na mnogo širem nivou formirati konsenzus država koji će biti ne samo smernica već formalni sporazum sa ciljem da problematiku sajber kriminala reguliše.

LITERATURA:

1.http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

2. Jonathan Clough ‘’A world of difference: the Budapest Convention on cybercrime and the challenges of harmonisation’’, International Serious and Organised Crime Conference, Brisbane, 29–30 July 2013.

3. Michael A. Vatis The Council of Europe Convention on Cybercrime, Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, http://www.nap.edu/catalog/12997.html

4. Amalie M. Weber,The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425 (2003). http://scholarship.law.berkeley.edu/btlj/vol18/iss1/28

5. Nancy E. Marion ‘’The Council of Europe’s Cyber Crime Treaty: An exercise in Symbolic Legislation’’, International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010

6. Coleman, C. (2003). Security Cyberspace—New Laws and Developing Strategies. *Computer Law and Security Repor*t, *19*(2)

7. Walden, I. (2004). Harmonising Computer Crime Laws in Europe. European Journal of Crime, Criminal Law and Criminal Justice, 12(4)

8. Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013 © 2013 by NATO Cooperative Cyber Defence Centre of Excellence

9. Bendžamin Baklend i dr."Demokratsko upravljanje, Izazovi sajber bezbednosti", DCAF, Ženeva 2012.

10. Kristin Archick, ‘’Cybercrime: The Council of Europe Convention’’ CRS Report for Congress, July 22, 2004

11.United Nation Office on Drugs and Crime UNODC ‘’Comprehensive Study on Cybercrime’’ Draft—February 2013

12. Allen Hammond IV ‘’The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?’’ Santa Clara University, June 2001