DOI: 10.5937/vojdelo1803157P

SAJBER KRIMINAL KAO GLOBALNA PRIJETNJA U SVIJETU

Mijomir Perović
MUP Crne Gore / Univerzitet u Nišu, Pravni fakultet

Društvo ima najveću odgovornost u borbi protiv sajber kriminala. Bezbjednost je moguća jedino angažovanjem stručnih kadrova koji prate najnovije metode i trendove u svijetu radi otkrivanja i blagovremenog djelovanja i spriječavanja hakera. S obzirom na to da sajber terorizam predstavlja opasnost u eri globalizacije i povezivanja u svijetu u radu je izvršena analiza međunarodnopravnog okvira borbe protiv ove vrste kriminala s osvrtom na Konvenciju o sajber kriminalu. Savjet Evrope pokušao je ukazati na nedostatke ove konvencije.

Ključne reči: *prijetnje, bezbjednost, internet, sajber kriminal, hakeri*

Uvod

Sajber prijetnja, sajber kriminal i sajber prostor su termini koji se danas često koriste. Izraz sajber kriminal je novijeg nastanka, jer se kompjuter u početku koristio samo u naučnim svrhama i pri razmjeni podataka preko interneta. Kasnije izvor podataka počinje sve više da se koristi u različitim granama privrede. Pored dobrih namjena stvara i probleme, koje koriste i zloupotrebljavaju kriminalne grupe. Treba imati u vidu da svakodnevno milioni ljudi posjećuju sajtove i bezbroj stranica internet mreže. Svi oni imaju različite ciljeve: jednima je on potreban za rad, drugima za razmjenu mišljenja, trećima za učenje. Internet pojednostavljuje mnoge pravne operacije između subjekata različitih država. (Mentokova & Dobrovina) 2013:81. Danas države usavršavaju kadrove da koriste tehnologije koje će moći da prate u radu i da sarađuju na globalnom nivou kako bi se mogle razmjenjivati informacije , radi sprječavanja ovih modernih oblika krivičnih djela.

Krivična djela sajber terorizma i problemi bezbjednosti

Razvoj informacionih sistema doprinosi cjelokupnom razvoju društva. Taj napredak ima i drugu stranu, a jednu od njih predstavlja sajber kriminal kojem se treba suprotstaviti, a koji u strukturi krivičnih djela u savremenom svijetu zauzima primarno mjesto. Sama riječ syber (cyber) na grčkom znači neko ko upravlja ili vlada, a značenje termina je nevidljivo, neupadljivo i neograničeno.

U svijetu danas postoji veliki broj računara koji su umreženi internetom. Brojka mobilnih telefona sa mogućnostima interneta stalno se uvećava, pa se uvećava i mogućnost korišćenja sajber prostora. Sajber kriminal predstavlja stručno, specijalno znanje i pozna-

vanje kako bi se izvršilo krivično djelo. Smanjivanjem mogućnosti kontrole, nacionalna bezbjednost susreće se sa novim i opasnim vidom kriminala, pa se postavlja pitanje – kako obezbjediti demokratski metod kontrole propisa koji su vezani za internet, kao i zaštitu od ovog vida kriminala, odnosno hakerske djelatnosti. U savremenom svijetu sajber propaganda često postaje prethodnica ratova, revolucija i vojnih akcija.

Sajber napad je teško otkriti, a obavještajne agencije ometaju ovakva otkrivanja, usmjeravajući svoju aktivnost na paralisanje službi koje vrše zaštitu i kontrolu. Teškoće se javljaju i na međunarodnom nivou, jer problemi rješavanja su, kao zakonska regulativa, različiti od zemlje do zemlje, pa još uvijek nema propisa koji bi se mogli primjeniti na globalnom nivou. Već stvaranjem grupe G8 mogu se primjeniti početni koraci odupiranja ovom vidu kriminala na međudržavnom nivou. Ali, ipak može se reći da su velike države, odnosno sile u svijetu, imale odlučan uticaj, tako da su njihovi interesi izbili u prvi plan. S obzirom na to da većina zemalja u svijetu nema osnovnu IT strukturu, postoji niz faktora koji vrše svoj uticaj, a to su: politički, pravni, psihološki, tehnički itd. Ove faktore možemo podijeliti na: *pravne*, koji se odnose na krivičnopravnu regulativu, kao i otkrivanje krivičnih djela i njihovo procesuiranje; *socijalne,* koji utiču na suštinu ovog oblika kriminala, kao i opasnost od ovog oblika krivičnih djela u jednom društvu.

Može se postaviti i još jedno važno pitanje: „Kojim bi se demokratskim procesima ili pravnim standardima trebalo rukovoditi prilikom donošenja odluke o eventualnoj reakciji? Ova poslednja tačka je naročito važna jer neki faktori dramatično smanjuju transparentnost Sajber rata u odnosu na druge tipove konflikata." (Buckland, Schreirg, Winkler 2010:10). Može se reći da pojedinci i manje korporacije vrše zloupotrebu domaće teritorije za pokretanje hakerskih napada. Napadnute firme ne žele da daju informacije, pa ih zbog bezbjednosti čuvaju kao tajnu. Države nemaju puno načina da saznaju činjenice o preduzetim mjerama (Giles 2010.). Većina zemalja u svijetu nije svjesna i ne zna da sa njihovih teritorija pojedinci i različita preduzeća pokreću hakerske napade. Teškoću za obavještajne izvore predstavlja veliki broj informacija o interesantnim događajima, koje pojedinačno ne predstavljaju opasnost, ali zajedničkim djelovanjem pričinjavaju pravu štetu. Obično pojedinci neće da otkriju hakerske napade, zbog, kako oni smatraju, neažurnosti policije kao i zbog izbjegavanja bilo kakvih kontakata sa policijom, smatrajući ih negativnim. Ni sama zakonska regulativa u tom domenu nije opširna i dobro objašnjena kako bi upravna vlast mogla zakonito reagovati i sprovoditi kako preventivne tako i represivne mjere, odnosno, kako bi se adekvatno reagovalo upotrebom softvera, čime bi se detektovao napad. U pravnoj regulativi ne postoji ni način da se sazna ko može dijeliti saznanja i informacije i sa kojim licima. Odgovornost, naročito u privatnom sektoru, trebalo bi rešavati brže i efikasnije. U ovakvoj situaciji teško se može govoriti o koordiniranim akcijama i reakcijama radi spriječavanja ovog oblika kriminaliteta – koordiniranjem pravovremenog reagovanja, saradnjom policije, obavještajne službe, kontraobavještajne službe, kao i vojnih službi. U suštini, nažalost, ta koordinacija ne postoji ili postoji u mnogo manjem obimu, dajući na taj način mogućnost i šansu ovom obliku kriminaliteta. „Demokratsku vlast kad je u pitanju reagovanje na sajber terorizam podriva niz dodatnih problema. Prvi među njima je disperzija odgovornosti. Ukratko, zbog velikog grupisanja nekada samostalnih aktera često je izuzetno teško utvrditi ko je zadužen za konkretnu oblast. Zbog toga postoji potreba da se premoste pređašnje pojedinačne uloge ministarstva i mehanizmi prijetnji i reagovanja. Ovo je naročito slučaj kada je u pitanju sve više vještačka podjela na bezbjednost države i druge državne mreže sa različitim ulogama i odgovornostima." (Buckland i dr. 2010:26). Društvo mora biti

odgovorno i ozbiljno prići ovim oblicima krivičnih djela, jer pristup tome je veoma važan radi suzbijanja sajber kriminala, što predstavlja odgovornost društva, pa je ona „definisana kao etička ideologija kod koje enitet (pojedinac ili preduzeće) ima obavezu da djeluje sa zabrinutošću osjetljivosti i svijesti o uticaju svojih akcija na druge." (Mamić, 2012:4). Ovom definicijom se jasno ispoljava da postoji individualna odgovornost kao i odgovornost društva u cjelosti. Što se tiče individualne odgovornosti, ona se odnosi na svakog pojedinca i njegove pojedinačne odgovornosti u odnosu na zajednicu, dok se kod korporativne odgovornosti može primjetiti da prati, odnosno izvršava u skladu sa zakonom, istovremeno izvršavajući i poštovanje međunarodnih normi. Razvojem internet tehnologije nastaje i problem usavršavanja i razvoja novih informacionih prijetnji, koje postaju opasnost za cijelo društvo, odnosno čovječanstvo u globalu. Značajno mjesto zauzimaju istraživanja problema, naročito multidisciplinarna, radi rješavanja pitanja informativne bezbjednosti. Treba postaviti pitanje da li organi bezbjednosti mogu da nadgledaju dopisivanje, pa tako u savremenom svijetu mnoge zemlje (njihove bezbjednosne službe) nadgledaju i prate komunikaciju raznih terorističkih grupa i kriminalnih organizacija. Pitanje privatnosti predstavlja značajan problem. U kompjuterima faktički postoje podaci o ljudima koji su dostupni cijelom svijetu. Koliko god tehnologija ne ugrožava privatnost ljudi, ljudi su ti koji zloupotrebljavaju tehnologiju za sajber kriminal, kontrolu lične privatnosti. Zbog toga je svakom društvu potrebna jača kontrola i suzbijanje takvog vida kriminala. „Jedino preostalo mjesto za kolonijalizaciju su samostalni mediji. To je novo područje za ljudsku interakciju, ekonomsku ekspanziju i društvenu i političku mahinaciju". (Rushkoff, 1996:4). U svijetu skoro i da ne postoji vlada koja po pitanju bezbjednosti može da prisili firme da preduzmu mjere koje ona želi, jer najveći uticaj imaju transnacionalne sile i pojedinci koji imaju svoje interese i ciljeve. Sajber bezbjednost nailazi ponekad na prepreke, a to su pravo na privatnost i sloboda izražavanja. Problem je povezan sa tehnološkim znanjima. Tome možemo dodati i javno-privatnu saradnju iz koje proizlazi sajber bezbjednost koja je disperzivna i izlazi iz okvira agencijskih ovlašćenja. Vidimo da je danas postupak svakog državnog agenta povezan sa lancem odgovornosti, a sa druge strane, uvođenjem privatnih aktera situacija se iskomplikovala zbog smanjenje mogućnosti, a time i mogućnosti efikasnog nadzora.

Izvori i prijetnje sajber kriminala

Ključan izvor predstavljaju strane obavještajne službe, koje uz pomoć sajber prijetnji vrše destabilizaciju i zastrašivanje u pojedinim državama. To se obično kada suprotne obavještajne službe, naročito rivalske, „pothranjuju" dezinformacijama i puštanjem glasina radi zastrašivanja, što ponekad može preći u pravi sajber obračun. Kad je u pitanju narušavanje privatnosti i bezbjednosti pojedinca države predstavljaju prijetnju, jer ih lako otkrivaju. Veliki problem predstavlja to što organi država u velikom broju slučajeva čine bez sudskog naloga i demokratske kontrole. U globalnom svijetu velike korporacije mogu da budu u sprezi sa kriminalom, i dobro obučenim hakerima radi sabotaža i špijunaže. Korporacije sakupljaju veliki broj ličnih podataka, time ugrožavaju ljudska prava, u zavisnosti od interesa koji imaju, dijele ih sa pojedinim kriminalnim organizacijama i vladama koje sarađuju sa njima. Hakeri predstavljaju izvor prijetnji, jer uz pomoć interneta mogu da izazovu napad na sajtove žrtava. Sredstva za napad iz dana u dan su bolja, pa su i rezultati boljeg napada i očigledniji. U novije vrijeme sve se više napadaju vebsajtovi koji nanose političke štete protivniku.

Insajderi najčešće poznaju sistem žrtve, pa mogu lako i pristupiti. U Americi, prema informacijama federalnog biroa, najčešće se dešavaju napadi sa strane, izvan države. S obzirom na to da je vrijeme u kojem postoje prikriveni i otvoreni konflikti formiraju se grupe za terorizam koje imaju kapacitete za sajber napad. Za sada ih nema u većem broju, ali će ih u budućnosti biti više. Na podzemnoj sceni tržišta su botnet operateri koji, u stvari, predstavljaju hakere koji zahvataju sve veći broj računara, preko kojih vrše pripreme za nove napade. Sve to predstavlja prevare i spamovanje. Spamovanje podrazumeva slanje spama (elektronska pošta), a fišeri su pojedinci ili male grupe koje izvršavaju kazne identiteta, pa tako stiču velike količine nezakonito zarađenog novca. Koristeći spam, odnosno softver za špijunažu, realizuju svoje namjere. Oni šalju lažne informacije, a njihov cilj je da prodaju svoje proizvode, vrše distribuciju zlonamjernog softvera, vršeći na taj način napade na razne organizacije. Posebnu prijetnju u ovom vidu kriminaliteta predstavljaju pedofili koji uz pomoć interneta šire dječju pornografiju, pomoću internet pričaonica. „United States Government Accountability office, 2009., P.G.; Wulf&Jones, 2009.; 943; Golumbic, 2007".

Jedna od najvećih prijetnji u svijetu predstavlja sajber terorizam koji je danas u velikoj ekspanziji . Ovdje podrazumijevamo napade na informacije računarskih sistema, raznih programa i podataka. Po Vuletiću sajber terorizam je „kriminalni akt izvršen kroz računare rezultujući u nasilju, smrti i/ili destrukciji, stvarajući teror radi ubjeđivanja vlade da promjeni svoju politiku" (Vuletić, 2012a:27).

U vrijeme velikih tehnoloških razlika, naročito između razvijenih i jakih industrijskih zemalja i nerazvijenih i siromašnih zemalja, kad ne postoji mogućnost vođenja rata protiv mnogo superiornijeg suparnika, nastaju sajber ratovi koji sa sajber terorizmom predstavljaju alternativu. Svoje namjere ovi teroristi ostvaruju pomoću takozvanih Logic bombs) Trojan horses, Worms , uz pomoć različitih virusa itd. (Zirojević-Fatić, 2011.:419). Treba istaći i sabotaže uz upotrebu kompjuterskih tehnologija, upad u računare nuklearnih elektrana, ometanje i isključivanje velikih elektronskih sistema, blokiranje kompjuterskih mreža itd.(Matusitz, 2008:186). Koristeći ove metode, na različitim softverima, ovi akteri mogu sabotirati rad na berzama, ometati avio-saobraćaj, odnosno avio-kontrolu, uticati na promjenu pritiska u gasovodima, kao i ometati državne organe i nanositi štetu institucijama. Sajber terorizam se po načinu sprovođenja razlikuje od standardnih oblika terorizma. Privlačniji je za teroriste, jer se vrši bez upotrebe oružja. Ovaj vid terorizma je mnogo i ekonomičniji, jer je lakše pronaći hakera, platiti i izvršiti zadatak pomoću njega, za razliku od konvencijalnih terorista koje treba pripremiti, obučiti, itd., što iziskuje velika sredstva, kao i rizik od otkrivanja i dovođenja pred lice pravde. Na ovaj način izbjegavaju se samoubilačke misije, a privlači se veća medijska pažnja zahvaljujući načinu izvršenja (Berner, 2003:3).

U svijetu postoje mnoge organizacije koje odgovaraju na ove sajber prijetnje. To su: Apec-Tel, Enisa, Nato koordinacioni centar posebne sajber odbrane CCDCOE, ARSEAN, OECD, OAS tim za reagovanje na kompjuterske incidente (SIRT), forum za upravljanje internetom (IGF), međunarodna telekomunikaciona unija (ITU) itd. Pored navedenih organizacija postoje i nevladine organizacije: Human Rights Watch-a, Amnesty International-a, Reporteri bez granica itd. Od industrijskih organizacija najpoznatije su: konzorcijum za podsticanje bezbjednosti na internetu (ICASI), organizacije koje se bave bezbjednošću na aerodromima anti-fišing radna grupa (APWG). U upravama policija balkanskih država postoje odeljenja koja se bave sajber kriminalom. U suštini, sajber prijetnje će predstavljati opasnost koja će aktivirati bezbjednosne službe na što predanijem radu u spriječavanju, otkrivanju i procesuiranju ovih oblika krivičnih djela.

Pravna regulativa, borba protiv sajber kriminala u svijetu

Sajber kriminal se sprovodi uz pomoć tzv. sajber stručnjaka koji su obučeni i pripremljeni za te aktivnosti, Nasuprot njima treba da postoje veoma stručni profesionalci u državnim službama. Pored toga, postoji i potreba za što boljom pravnom regulativom, što doprinosi efikasnijem radu, preventivnom djelovanju i spriječavanju u vršenju ovog vida kriminala. U svijetu danas postoji konvencija o sajber kriminalitetu Savjeta Evrope, gdje su regulisani međunarodnopravni okviri borbe protiv sajber terorizma. Ovu konvenciju su u dužem periodu pripremale članice Savjeta Evrope, ali i druge države van Evrope, kao što su: Australija, Japan, Kanada, SAD, Dominikanska republika, Mauricijus i Južnoafrička republika. Do 2013. godine 52 zemlje potpisale su ovu konvenciju pomoću koje rešavaju ovaj problem na globalnom nivou, djelujući u otkrivanju i procesuiranju sajber kriminala pred krivičnim sudovima. Ova konvencija ima širok spektar tumačenja. Ona obavezuje države da utvrde krivičnu odgovornost, kako za saučesništvo i podstrekivanje, tako i za pokušaj izvršenja krivičnog djela. Takođe, insistira se na usaglašavanju zakona u državama članicama sa tom konvencijom, kao i za davanje širih ovlašćenja državnim organima u zemljama članicama radi što efikasnijeg rada. Konvencija je sastavljena od četiri dijela. U prvom dijelu najviše se razmatra terminologija, u drugom se navodi šta treba da bude preduzeto na domaćem nivou država članica (domaće materijalno pravo i krivično procesno pravo); u trećem dijelu navode se načini i oblici međunarodne saradnje, a u četvrtom se nalaze završne odredbe. Konvencijom su predviđena sledeća krivična djela: neovlašćeni pristup, neovlašćeno presretanje, ometanje toka podataka, ometanje računarskog sistema, zloupotreba uređaja, falsifikovanje počinjeno pomoću računara, prevara izvršena pomoću računara, krivična djela protiv pornografije, krivična djela autorskih i srodnih prava.

U drugom dijelu konvencije navode se sledeće procesne odredbe: hitno čuvanje pohranjenih podataka, hitno čuvanje i djelimično otkrivanje podataka o saobraćaju, naredba za dostavljanje, pretraživanje i zaplena računarskih podataka, prikupljanje podataka o saobraćaju u realnom vremenu, presretanje podataka o saobraćaju.

Treća glava odnosi se na krivično-materijalnu saradnju, odnosno navodi se kada će se primjenjivati odredbe konvencije među zemljama članicama. Ovom konvencijom predviđa se i međudržavna saradnja i pristup računarskim podacima. Čak se predviđa i uspostavljanje mreže za hitno reagovanje u slučajevima saradnje među državama koje su pristupile primjeni konvencije. Kontakti u okviru mreže ostvaruju se preko ministarstava unutrašnjih poslova i javnih tužilaštava navedenih zemalja. Konvencijom u dijelu članova od 16 do 21 određeni su procesni pristupi u borbi protiv sajber kriminala, kao što su: hitno čuvanje pothranjenih računarskih podataka, hitno čuvanje i djelimično pohranjivanje odnosno otkrivanje podataka o saobraćaju, naredba o dostavljanju podataka, pretraga i zaplena pohranjenih računarskih podataka, prikupljanje podataka u realnom vremenu.

Sama konvencija može se kritikovati sa pristupa pravne logike. Znajući da je veliki dio država u svijetu tehnološki zaostao, a da je konvencija pisana pod uticajem razvijenih država, naročito SAD, većina država smatra da je to politički instrument u rukama velikih sila. Međutim, bez obzira na sve kritike, ona predstavlja najznačajniji međunarodnopravni okvir i uputstvo za suprotstavljanje rastućem sajber kriminalu (Polić, 2010) Avgusta 2013. godine doneta je direktiva 2013/40 EU kojom se mijenja odluka Savjeta Evrope 2005/222/JHA. Ona predstavlja sastavni dio „ACQUI COMMUNALITAIRE" –

zajedničkog okvira za zemlje koje su članice EU, a u vezi sa napadima na informacione sisteme. Ovom direktivom postavljaju se pravila u odnosu na definisanje krivičnih djela, kao i sankcije za njih, kao i saradnja između nadležnih organa. Donošenjem direktive Evropski parlament je vodio računa o sve izraženijem obliku napada na informatičke sisteme. Jedna od njih je upotreba „botnetova". Ovaj metod može koristiti više nivoa pri izvršenju krivičnog djela, gdje svaki predstavlja opasnost po državne interese. Direktiva uvodi krivičnu odgovornost za njihovo korišćenje. „Botnetovi su koordinirane grupe od nekoliko (desetina, stotina ili hiljada) personalnih računara ili čak novih generacija mobilnih telefona (smartphones) pri čemu su svi zaraženi istim malicioznim programom. Njihova moć, daljinski kontrolisana, može se rangirati od spemova i krađe identiteta po špijunaže i napada na kritične informacione strukture" (Vuletić, 2012b:240). Zbog veće društvene opasnosti direktiva propisuje veće sankcije za krivična djela koja su opasnija po društvo, pa imamo „elemente bića krivičnog djela neovlašćeni pristup informacionom sistemu, neovlašćeno ometanje sistema, neovlašćeno ometanje podataka, nekorišćenje sredstava za izvršenje ovih krivičnih djela" (Stamenković i dr. 2014:41). Direktiva u članovima 4 i 5 predviđa kazne od 5 godina u određenim slučajevima, i to: kada su ova krivična djela izvršena od strane kriminalne organizacije bez obzira na kaznu koja je propisana za kriminalnu organizaciju, ukoliko je nastala šteta usled krivičnog djela, ukoliko je izvršeno krivično djelo protiv informacionog sistema kod kritične infrastrukture. U članu 17 ove direktive Evropska komisija se obavezala da do 4. septembra 2017. podnese izvještaj Savjetu Evrope, kako bi se izvršila procjena primjene u državama potpisnicama ove konvencije. Koliko god se vršila primjena konvencije države članice je ne mogu u potpunosti kontrolisati, jer se ovaj vid kriminaliteta mijenja iz dana u dan, stvarajući nove metode za dejstva.

Zaključak

Borba protiv sajber kriminala zahtijeva upotrebu modernih tehničkih znanja, radi preventivnog djelovanja i spriječavanja hakera. Potrebno je izvršiti sinhronizaciju djelovanja, uskladiti zakone između država, djelovati na globalnom nivou, a države moraju imati jake obrazovne kadrove u ovoj sferi, kako bi se procedura otkrivanja, gonjenja i procesuiranja što bolje izvela. Svaka aktivnost u zemlji treba da bude organizovana tako da postoji saradnja između državnih organa i istovremeno djelovanje bezbjednosnih službi (obavještajne službe, policije, vojne obavještajne službe), kao i saradnja u javno-privatnom obliku. Bez obzira na Konvenciju, njene potpisnice ne mogu reagovati, jer saradnja na međudržavnom nivou nije baš sjajna, što otkrivanje krivičnih djela sajber kriminala čini otežanim, a službe sprečava da budu efikasnije. Posebnu teškoću predstavlja saradnja preduzeća i korporacija sa kriminalnim grupama i hakerima u sprovođenju industrijske špijunaže i sabotaže. Prijetnje hakera, terorista, fišera i spamera potpomognute su i pravnim prazninama, odnosno neregulisanom zakonskom regulativom. Ove nedostatke nije prevazišla ni Konvencija o sajber kriminalu, iako se na njoj dugo radilo. Ipak, dolazilo je do stalnih promjena, kako u zakonskoj regulativi, tako i do promjena i usavršavanja rada hakera. Sve to predstavlja usavršavanje i stvaranje uslova za što bolje i efikasnije djelovanje, kako u državama tako i na regionalnom i međunarodnom nivou organizovanja.

Literatura

[1] Berner, S. (2003) Cyber-terrorism: reality or paranoia? South African *Journal of Information Management*, Vol 5, No 1, p. 1-4 .

[2] Buckland, B., Schreier, F. & Winkler, T. (2010). *Demokratsko upravljanje*: izazovi Sajber bezbednosti, Beograd: Forum za bezbednost i demokratiju.

[3] Giles, J. (2010). *Benevolen Hackers Poke Holes in E-Banking*, http://www. newscientist.com/article/mg20527455.400-benevolent-hackers--poke-holes-in-ebanking.html, pristupljeno 04.02.2015.

[4] Golumbic, M. (2007). *Fighting Terror Online*: *The Convergence of Security, Technology and the Law*. New York: Springer.

[5] Ларьков, А. & Кесареева, Т. (1998). Экономическая прѐступность: характеристика и факторный анализ, (3), (125-130).

[6] Matusitz, J. (2008). Similarities between terrorist networks in antiquity and present-day cyberterrorist network. *Trends in Organized Crime*, Vo1.11 (2), 183-199.

[7] Ментюкова, М. А. & М.М. Дубровина, (2013.) Эволюция уголовной ответственности за доведение до самоубийства с использованием сети Интернет. *Журнал Вопросы современной науки и практики,* (44) 81-86.

[8] Mamić, D. (2012). D*ruštvene mreže kao omogućitelji društvene (ne) odgovornosti*, Zagreb: Fakultet elektronike i računarstva.

[9] Polić, V. (2010), Komparativna analiza kompjuterskog kriminala u zakonodavstvima Republike Srbije i nekih stranih zemalja http://www.singipedia.com/content/1066-Komparativna-analiza-kompjuterskog-kriminala-u-zakonodavstvima-Republike-Srbije-i-nekih-stranih-zemalja, pristupljeno 06.02. 2015.

[10] Rushkoff, D. (1996), *Media Virus*. New York: Ballantine Books.

[11] Stamenković, B, Balota, A, Pavličić, V, Paunović, B. i Backović, J. (2014). *Visokotehnološki kriminal: praktični vodič kroz savremeno krivično pravo i primjere iz prakse*, Podgorica: OSCE Misija u Crnoj Gori.

[12] United States Government Accountability Office (2009). *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk*. Washington DC: US GAO.

[13] Vuletić, D. (2012a). *Bezbednost u Sajber prostoru*, Beograd: Medija centar „Odbrana".

[14] Vuletić, D. (2012b). Napad na računarske sisteme, *Vojnotehnički glasnik*, Vol. 60, (1), 235-249.

[15] Wulf, W. & Jones, A. (2009). Reflections on Cybersecurity. *Science*, Vol. 326, (5955), 943-944.

[16] Zirojević-Fatić, M. (2011). Zloupotreba interneta u svrhe terorizma. *Međunarodni problemi*, Vol. 63, (3), 417-448.