Žaklina SPALEVIĆ,
Miroslav VRHOVŠEK,
Milovan JOVANOVIĆ*

UDK: 004.738.5:343.9.02

RAČUNARSKE MREŽE KAO LOGISTIČKA PODRŠKA TERORISTIČKIH I KRIMINALNIH ORGANIZACIJA

Sažetak: Činjenica je da su i terorizam i Internet značajni globalni fenomeni koji oblikuju razne aspekte svetske politike. Zbog svoje globalne zastupljenosti i bogatog višejezičkog konteksta, Internet ima potencijal da utiče na različite načine na razne tipove politike i društvenih odnosa. Za razliku od tradicionalnih masovnih medija, otvorena arhitektura Interneta ograničava napore Vlada zemalja sveta da regulišu Internet aktivnosti, pa ovo obezbeđuje korisnicima ogromnu slobodu i prostor da oblikuju Internet na svoj način. Teroristi danas znaju da veoma pametno koriste tradicionalne masovne medije, a takođe prepoznaju i vrednost direktnih komunikacionih kanala. Ukoliko teroristi žele da pošalju poruku, sada imaju šansu da to urade bez bombaških akcija i ubistava. Reči su jeftinije od života. Javnost ne vidi teror ako vidi da terorista govori na televiziji ili na Internetu, ali je uplašena ako vidi žrtve terorističkih napada, a ne vidi teroriste. S druge strane, državni akteri i pojedinci pokušavaju da obuzdaju pojavu terorističkih materijala na Internetu. Autoritarne Vlade su imale određene uspehe u korišćenju tehnologija koje ograničavaju svoje građane da pristupaju određenim sajtovima. Postoji nekoliko restriktivnih opcija u demokratskim zemljama, gde, iako su usvojeni novi restriktivni zakoni u brojnim pravosudnim organima i dalje nije jasno da li će oni biti efikasni kao raniji pokušaji kontrole, npr. kontrolisanja cyber mržnje. U pogledu terorističkih Web sajtova i njihovih uklanjanja, privatne institucije u saradnji sa Internet

* Žaklina Spalević, Pravni fakultet za privredu i pravosuđe, Novi Sad, e-mail: zaklinaspalevic@mail.com.
Miroslav Vrhovšek, Univerzitet Privredna Akademija, Novi Sad, e-mail: vmiroslav@eunet.rs
Milovan Jovanović, diplomirani politikolog, e-mail: miki80miki@gmail.com.

provajderima su mnogo uspešnije, međutim, aktivnosti pojedinačnih aktivista ozbiljno narušavaju slobodu govora i one koji trebaju da donose odluke o tim ograničenjima. Takva nastojanja mogu nas zapravo podstaknuti da dobro razmislimo o zakonodavstvu, ne samo u smislu postavljanja kontrole, već i u pisanju robustnih zakona o radikalnim političkim govorima.

Ključne reči: Internet, kontrola Internet sadržaja, Internet uprava, zakonodavna politika, cyber teroristi.

Uvod

Novi razvoj i dostignuća u telekomunikacijama, naprednim ekspertnim sistemima i *inteligentnim* programskim rešenjima doveo je do velikih promena u životu i komunikaciji među ljudima. Virtuelni čovekov svet postaje sve važniji deo života i delovanja pojedinaca, njihovih organizacija i savremenih društvenih zajednica. Stvara ga i stalno unapređenje, progresivan razvoj informacionih tehnologija.

Internet je nametnuo globalnu promenu u brzini i načinu komunikacija, unevši važan uticaj na kvalitet života "običnog čoveka".Taj uticaj vidljiv je u svim sferama društvenog života,odnosno svim poljima našeg životnog okruženja.Pozitivne i korisne novine savremenih informacionih i kompjuterskih tehnologija,donele su i niz problema vezanih za pojavu i ekspanziju različitih oblika kompjuterskog kriminaliteta.[1]

Sadašnje stanje u oblasti Interneta je primamljivo za razne vrste kriminalnih radnji informaciono-tehnički obučenih lica koja na protivzakonit način stiču materijalnu korist i ujedno predstavljaju širu društvenu opasnost protiv koje države, među kojima i naša u težnji da koriste nove tehnologije u razvoju tržišta, moraju da razvijaju legitiman zaštitni okvir poslovanja. Neki autori govore o ranjivosti informatičkog društva i o potrebi da se ona otkloni, koliko je to moguće.

Visok stepen razvoja računarske tehnike i informacionih tehnologija je doveo do novih pojavnih oblika kriminala. Cyber kriminalitet sa sobom donosi veliku društvenu opasnost tako da se kao odgovor na to pojavljuju novi zakoni kojima se ovi postupci sankcionišu kao krivična dela. Oblast Internet komunikacija je u velikim delu pravno neregulisan, jer adekvatne zakonske regulative nema. Efikasnom pravnom zaštitom sprečila bi se situacija u kojoj

[1] Željko Bjelajac, Cyber crime and Internet pedophilia as an important international phenomenon, „Western Balkans: From Stabilization to Integration“, The Institute for International Politics and Economics, Belgrade, 2012, str. 4370456.

širenje polja primene računara kroz elektronsko bankarstvo, elektronsku trgovinu i elektronsku upravu povećava rizik za nastanak cyber kriminala, a posebno cyber terorizma.[2]

Ovim problemom se danas ozbiljno bave Evropska Unija, Savet Evrope, G8, Interpol i Ujedinjene Nacije. Zaštitna funkcija vrednosti se, pre svega, u državi ostvaruje putem krivično pravne zaštite kroz generalnu i specijalnu prevenciju.

Internet – globalna računarska mreža

Internet je postojeća virtuelna mreža kreirana od drugih *internetworking* mreža koje su povezane TCP/IP protokolom ili drugim vidovima otvorenog pristupa, jer je on javna mreža svima dostupna. Internet nije entitet, već komunikaciona infrastruktura. Internet je mreža *svih* mreža koje međusobno komuniciraju.

Nastao je početkom 90-tih godina spajanjem regionalnih mreža. Tu se javlja pravni problem nadležnosti s obzirom na geografski raspored servera na Internetu koji se nalaze širom sveta. Pre nego što se uopšte postavi pitanje ko je nadležan za događaj koji se desio na Internetu, potrebno je odgovoriti na pitanje gde se događaj koji se odigrao u virtuelnom svetu Interneta odigrao u fizičkom realnom svetu. Problem koji postoji na Internetu, a koji takođe pogoduje cyber kriminalitetu je problem identiteta. Naime, teško je na Internetu utvrditi nečiji pravi identitet (*On the Internet nobody knows you are a dog*, je tekst ispod čuvene karikature objavljene u u *Newyorker*-u, 5. jula 1993. godine, na kojoj je naslikan pas koji surfuje Internetom). Pitanje identiteta se danas rešava elektronskim potpisom i raznim sistemima identifikacije (smart karticama, biometrikom) i to samo donekle, za određene korisnike i određene potrebe, dok u ostalom delu ovaj problem i dalje ostaje nerešen. Stari vidovi trgovine i drugih delatnosti se nalaze u novim, još uvek nesigurnim i vrlo sofisticiranim elektronskim okvirima Interneta. Zaključivanje ugovora putem Interneta, koje je sve češće, praćeno je elementima identifikacije. Postoji i problem i teškoća privatnosti na Internetu koji takođe pogoduju cyber kriminalitetu.

Sve ovo *pravo* postavlja pred velike izazove koji se ogledaju u tome da se u virtuelnom svetu javljaju neke situacije koje su nepoznate u fizičkom svetu i da za njih ne postoje izgrađena pravna rešenja za te situacije. Zatim, javljaju se

[2] Ivana Damjanović, "Postoji li sajberterorizam?", *Politička revija*, vol. 8, br. 1, str. 237–253, 2009.

problemi u smislu toga da je virtuelni svet digitalan i da su u njemu neke akcije koje su u fizičkom svetu zavisne od volje fizičkih i pravnih lica ovde automatske i da je u toj situaciji vrlo često teško otkriti ko je odgovoran i da li je odgovoran, a što je primarno kod utvrđivanja građanske ili krivične odgovornosti.

Izazov je u tome da se bezopasne i uobičajene Internet transakcije obavljaju preko teritorija više zemalja i njihovih pravnih sistema. To dovodi do situacija mnogostrukih sukoba nadležnosti što za predmet ima u građanskopravnoj materiji posebna i složena disciplina međunarodnog privatnog prava. Rešenje za ovaj problem mogu biti međunarodne konvencije, gde se opet postavlja problem unifikacije ili harmonizacije vrlo različitih pravnih sistema, sukoba interesa država koji obuhvataju i različite nacionalne standarde i tradicije, ali i mnogo veće sukobe interesa moćnih interesnih grupa koje, pre svega, obrazuju velike multinacionalne kompanije.

Internet uprava

Kontrola sadržaja na Inernetu, pre svega na polju otkrivanja terorizma je neophodna. Vlade zemalja moraju imati glavnu ulogu u kontroli sadržaja na Internetu, tako što one određuju šta treba, a šta ne treba kontrolisati i na koji način. Neke grupe ili pojedinci, kao što su hakeri, ometaju prisustvo brojnih terorističkih organizacija na Internetu. Praktično rečeno, i zakonska kontrola sadržaja i privatna inicijativa zahtevaju učešće privatnih kompanija, naročito Internet provajdera i kompanija koje nude usluge pretraživanja sadržaja na Internetu, na koje država i privatne organizacije vrše pritisak da regulišu sadržaj terorističkih organizacija. Ovde je uzeta u obzir i dostupnost odgovarajuće tehnologije za kontrolu sadržaja.

Opšti pristup politike kontrole sadržaja ima tri tačke gledišta, a to su: ljudska prava (sloboda izražavanja i prava na komunikaciju), Vlada (zakonska kontrola sadržaja) i tehnologija (alati za kontrolu sadržaja).

Sloboda izražavanja i pravo da korisnik može da potražuje, dobija i saopštava informacije predstavljaju osnovna prava, prema članu 19. Univerzalne Deklaracije Ujedinjenih Nacija o ljudskim pravima (1948). Na drugoj strani, pomenuta deklaracija ukazuje na to da sloboda izražavanja ograničava tu slobodu u skladu sa moralom, javnim redom i opštim dobrom (član 29). Prema tome, i diskusija implementacije člana 29. mora biti stavljena u kontekst uspostavljanja balansa između prethodno navedenih interesa. Ovaj dvosmislen međunarodni režim otvara vrata brojnim mogućnostima za različite interpretacije normi koje se odnose na pravo govora.

Kontrola sadržaja je ograničena slobodom govora i interesima ograničenja slobode izražavanja. Kontrola govora na Internetu je u suprotnosti sa Prvim Amandmanom Američkog zakona u kome se garantuje sloboda izražavanja, čak i pravo javnog iskazivanja mržnje i sličnih materijala. Postizanje odgovarajućeg balansa između kontrole sadržaja i slobode izražavanja predstavlja veliki izazov. S obzirom na to, Američki kongres teži sprovođenju strožije kontrole sadržaja, posebno nakon 11. septembra 2001. godine, dok Američki vrhovni sud podržava zaštitu Prvog Amandmana. Sloboda izražavanja najvećim delom određuje poziciju SAD-a u međunarodnim debatama na temu Internet uprave. Sve dok je SAD potpisnik Konvencije o cyber kriminalu, ograđena je od potpisivanja Dodatnog Protokola koji se odnosi na kriminalističke radnje rasističke i ksenofobične prirode koje se obavljaju preko kompjuterskih sistema. Drugačije rečeno, dok je Dodatni Protokol potpisan od strane Vlada zemalja Evropske unije i drugih zemalja potpisnica, gde je moguće dodavati druge statute o kriminalu mržnje, prema kojima se terorističke grupe i njihovi pomagači mogu sudski goniti, iste legalne opcije ne postoje u zakonodavstvu SAD-a.[3]

Iz tog razloga su Internet stranice brojnih terorističkih grupa smeštene u SAD-u. Na primer, Internet provajder Konektikata je nudio servise izmeštanja i virtuelnog hostinga za Web sajt organizacije *Hamas* u centru podataka u Konektikatu i Čikagu. Dok su Web sajtovi *Hamasa* bili predmet posmatranja nakon 11. septembra 2001. godine, slične Web stranice su već nadzirane pre ovog događaja.

Tokom 1997. godine pojavila se kontraverzna situacija kada je otkriveno da je Državni Univerzitet u Njujorku (SUNY) hostovao Web sajt Revolucionarne Armije Kolumbije (FARC), a Web sajt Revolucionarnog pokreta solidarnosti *Tupak Amaru*-a je hostovan na Univerzitetu u Kaliforniji u San Dijegu. SUNY je zvanično ugasio Web sajt FARC-a, dok je u San Dijegu zvanično odlučeno da zbog slobode govora ostane na serveru Web sajt *Tupak Amaru*-a još nekoliko godina.[4]

Države imaju pristup brojnim tehnologijama uz pomoć kojih je moguće disidentima zabraniti i ograničiti korišćenje Interneta. Uspešno korišćenje

[3] Giovanna Bono, "The Impact of 11 September 2001 and the '*War on Terror'* on European Foreign and Security Policy: Key Issues and Debates", *Studia Diplomatica*, vol. LIX, no. 1, 2006.

[4] Mark Rodžers,"Psihologija sajber-terorizma", *Bezbednost*, Beograd, vol. 46, br. 1, str. 126–132, 2004.

Interneta za potrebe regrutovanja novih članova terorističke organizacije i drugi tipovi političkih akcija zasnovani su na pretpostavci da korisnici imaju pristup Internetu putem kojeg razmenjuju poruke. Prema tome, države mogu ograničiti njihovu efikasnost ograničavanjem pristupa Internetu korisnicima, bilo da aktivno cenzurišu sadržaj na Internetu, bilo da kontrolišu infrastrukturu Interneta ili da kombinuju prethodno navedena ograničenja. Zajednički element prema kome se obavlja filtriranje sadržaja predstavlja indeks Web sajtova koji su blokirani za pristup. Ukoliko se Web sajt nalazi na ovoj listi, pristup korisniku neće biti dozvoljen.

Tehnički rečeno, filtriranje se vrši pomoću IP protokola za rutiranje, proksi servera i DNS preusmeravanja. Filtriranje sadržaja se obavlja u mnogim zemljama, kao što su Kina, Saudijska Arabija i Singapur, dok druge zemlje koriste cenzurisanje. Na primer, Australija ima sistem filtriranja za specifične nacionalne Web stranice, dok Nemačka pokrajina Severna Rajna-Vestfalia zahteva od Internet provajdera da uglavnom filtriraju pristup Neo-Nacističkim sajtovima.

U analizama o Internet upravi, jedan od ključnih razloga rasprave je bila da decentralizovana priroda Interneta čini pokušaje na primeni prekomerne cenzure. To je u svakom pogledu netačno, jer Internet uključuje brojne tehnike i tehnologije koje obezbeđuju efikasnu kontrolu. Sa tehnološke tačke gledišta mehanizme kontrole je moguće izbeći. U državama gde Vlade upravljaju kontrolom sadržaja tehnički iskusni korisnici nalaze načine da zaobiđu takve kontrole. Još uvek je teško identifikovati ko se tačno nalazi iza nekog računara, ali je sasvim jasno kako se identifikuje Internet provajder preko koga je korisnik pristupio Internetu. Širok spektar novijih zakona zahtevaju od Internet provajdera da identifikuju svoje korisnike i ako se zahteva, da se obezbede potrebne informacije nadležnim organima o samim korisnicima. Brojne Vlade imaju takođe planove o nadgledanju korisnika koji pristupaju Internetu sa javnih mesta, naročito iz Internet kafea. Pojačani monitoring na javnim mestima sada je zastupljen u Indiji, Italiji, Tajlandu i drugim zemljama, a razlog tome je nacionalna sigurnost.

Što je više Internet zastupljen u svetu, manje će biti jedinstveno upravljanje njime. Na primer, sa mogućnošću da se geografski lociraju Internet korisnici i njihove transakcije, kompleksna pitanja o pravnoj nadležnosti se mogu rešiti mnogo lakše putem postojećih zakona.

Jedno tehnološko rešenje je geografska lokacija softvera koja identifikuje lokacije računara i filtrira pristup određenim Internet sadržajima u skladu sa

nacionalnim poreklom računara. Slučaj *Yahoo!* je veoma važan po ovom pitanju i to od kada je grupa eksperata otkrila da je u 90% slučajeva *Yahoo!* mogao da odredi da li se nekim Web sajtovima, koji reklamiraju Nacističke suvenire, pristupalo iz Francuske. Ova tehnološka procena je pomogla sudu da donese konačnu odluku.

Kompanije koje imaju softver za Geografsku lokaciju korisnika tvrde da trenutno mogu, bez greške, da identifikuju zemlju porekla i grad iz koga se pristupilo Internetu u 85% slučajeva, naročito ako je grad veliki. Prema tome, takav softver može pomoći Internet provajderima da filtriraju pristup Internetu prema nacionalnim pripadnostima i da izbegnu sudske slučajeve u stranim pravosuđima.

Kontrola sadržaja na Internetu u cilju sprečavanja terorizma

Postoje tri tipa Internet sadržaja o kojima se raspravlja.

Prvi tip se sastoji od sadržaja gde postoji globalna saglasnost po pitanju kontrole. Kontrola širenja dečje pornografije putem Interneta je oblast za koju trenutno postoji najveća saglasnost, dok su navođenje na terorističke radnje i organizacije istih zabranjene međunarodnim zakonom, gde, iako postoji opšta saglasnost o uklanjanju ovog sadržaja sa Interneta, postoje i određena neslaganja. Razlog ovome je to što ne postoji globalno prihvaćena definicija terorizma, što otežava stvar. Saglasnost povodom toga je ipak moguće postići za razliku od stvaranja podrške u borbi protiv terorizma u bilo kojoj njenoj instanci.

U pogledu kontrole, drugi tip sadržaja o kojem se diskutuje predstavlja sadržaj koji može biti osetljiv za određene zemlje, regione ili etničke grupe iz razloga određenih religijskih ili kulturnih vrednosti. Većina sudskih Internet slučajeva se odnosi na ovaj tip sadržaja. Nemačka ima visoko razvijenu pravnu nauku u ovoj oblasti i ima iskustva iz mnogih slučajeva protiv odgovornih za hostovanje Web sajtova koji imaju Nacistički sadržaj. U Francuskoj je korisnicima Interneta zabranjen pristup jednom delu Yahoo.com Web sajta u kome se prodaju nacistički suveniri. Većina kontrole sadržaja u Aziji i Bliskom Istoku je opravdana iz razloga zaštite kulturnih vrednosti. U ovu zabranu spada: zabrana pristupa pornografskim i sajtovima za kockanje.

Na kraju, imamo treći tip sadržaja o kojem se često diskutuje, a koji sadrži politički i ideološki osetljive materijale koje je moguće cenzurisati. Ovde postoji dilema između realnog i cyber sveta. Postojeća pravila o slobodi govora, koja postoje u stvarnom svetu, mogu se implementirati i na Internetu.

Ovo je najbolje objašnjeno unutar Evropskog konteksta gde npr. okvir za donošenje odluka Saveta Evropske unije o borbi protiv rasizma i ksenofobije određuje da sve što je ilegalno u realnom svetu je ilegalno i u virtuelnom.

Prema tome, jedan od argumenata istaknut od strane onih koji veruju da Internet treba da ima specifično zakonodavstvo, skrojeno prema njegovim specifičnim karakteristikama je da kvantitet (npr. intenzitet u komunikacijama, broj poruka, itd.) pravi razliku u kvalitetu. Prema tome, problem govora mržnje i terorizma nije u tome da nema regulative protiv kojih je ona propisana, već u tome da širenje Interneta pravi razliku između širenja mržnje i terorizma putem Interneta i njenih ekvivalenata u realnom svetu. U osnovi, većina pojedinaca je izložena ovom tipu govora mržnje pa je teško primeniti postojeća pravila.

Shodno iznetom, razlike koje unosi Internet odnose se uglavnom na probleme primene pravila nego na sama pravila.

Pravna regulativa na polju kontrole sadržaja na Internetu

Zakonski vakuum na polju politike kontrole sadržaja, koji karakteriše prvo pojavljivanje i korišćenje Interneta, obezbeđuje Vladama zemalja Sveta visok nivo diskrecije u kontroli sadržaja. Regulativa na nacionalnom nivou može obezbediti bolju zaštitu ljudskih prava i ponekad otkloniti nedoumice uloge Internet provajdera, ali takvi zakoni mogu, takođe, pokazati visoko neslaganje. Prethodnih godina, mnoge zemlje su po prvi put uvele zakonodavnu politiku kontrole Internet sadržaja. Neki od ovih zakona je uveden kao rezultat porasta korišćenja Interneta i potreba da se zaštite interesi građana, pa je prema tome veliki broj zakona brzo donet nakon 11. septembra 2001. godine zbog rizika po nacionalnu bezbednost.

Odmah nakon događaja od 11. septembra FBI je zvanično zatvorio stotine, ako ne i hiljade Internet sajtova u Sjedinjenim Američkim Državama. Na primer, nekoliko radikalnih Internet radio stanica, kao što su *IRA Radio, Al Lewis Live* i *Our Americas* na Internet provajderu u Indiani je bilo ukinuto nakon 11. septembra, kada ih je FBI upozorio da će im oduzeti sredstva za promovisanje terorizma. Međutim, iz razloga što ovi sajtovi, koji su bili ugašeni, nisu direktno podsticali nasilje i prikupljanje novca, nisu se složili sa zakonom Sjedinjenih Američkih Država i veći broj njih je pokrenut ubrzo nakon što su ugašeni.[5]

[5] Maura Conway, "Reality bytes: Terrorist use of Internet", *First Monday*, Iss. 7,_11. 2002. Izvor: http://outreach.lib.uic.edu/issues/issue7_ 11/conway/index.html; datum pregleda: 10. 10. 2011.

Od svih zakona donetih nakon 11. septembra, najvažniji po pitanju Internet uprave je *USA PATRIOT* akt o događaju iz 2001. godine koji proglašava nelegalnim savetovanje ili pomaganje terorista čak i putem Internet sajtova. Slučaj *Babar Ahmada* je interesantan u tom pogledu. *Ahmad,* inače Britanski državljanin, osnivač dva čuvena sajta o džihadu, *azzam.com* i *qoqaz.net*, koji su hostovani u Sjedinjenim Američkim Državama, bio je okrivljen za prikupljanje novca za Islamističke militante u Čečeniji i Avganistanu. Vlada Velike Britanije je prihvatila da se *Ahmad* izruči SAD-u, gde se nalazio na odsluženju kazne zbog korišćenja Interneta u terorističke svrhe. *Ahmad* nije okrivljen samo za prikupljanje finansijskih sredstava, već i za podsticanje Muslimana na "korišćenje svih raspoloživih sredstava za izvođenje vojnih i fizičkih treninga za sveti rat i davanje jasnih instrukcija kako se prikupljaju i usmeravaju novčana sredstva nasilnim fundamentalističkim organizacijama, putem organizacije dobrotvornih akcija".[6]

Slične optužnice za koje treba da bude optužen *Ahmad*, donete su i protiv drugih, pre svega, državljana Sjedinjenih Američkih Država. Međutim, zbog visokog nivoa zaštite slobode govora u SAD-u, najmanje dva optužena su oslobođena bez optužbi, a to su: *Sami Omas al-Hussayen*, doktorant računarskih nauka na Univrzitetu Ajdaho, koji je osnovao i održavao radikalni Web sajt i *Sami Amin al-Arian,* profesor na Univerzitetu Južna Florida koji je bio optužen za objavljivanje članaka o nasilju koji su izvršili pripadnici Palestinskog Islamskog Džihada. Sudski proces *Ahmad Babara* će služiti kao još jedan test Akta *USA PATRIOT*. Očigledno je da će *Ahmadov* slučaj biti predmet posmatranja zbog njegovog govora o terorizmu na Internetu u SAD-u.[7]

Bombaški napad od 7. jula 2005. godine podstakao je Britansku Vladu da učestvuje u borbi protiv terorističkih Web sajtova van Velike Britanije. Odmah nakon ovog napada, Sekretar unutrašnjih poslova u Britanskoj Vladi, *Arthur Clarke,* je u parlamentarnom govoru ukazao na potrebu da moć države kontroliše "one koji podstiču terorizam ili traže od drugih da podrže terorističke akte". U pomenutom govoru *Clarke* je posebno naglasio da "osnivanje Web sajtova" ili "pisanje članaka u cilju podsticanja terorizma" predstavljaju aktivnosti koje treba da budu pod kontrolom ove "nove moći". Predlog zakona

[6] Krunoslav Antoliš "Prerequisites for Systematic Fighting Terrorism", *Croatian International Relations Review*, Vol. XI, No. 40/41, 2005., 121–125, July-December 2005, Zagreb, Croatia.

[7] Dorothy Denning, "Is cyber terror next?", Social Science Research Council, New York Izvor: http://www.ssrc. org/sept11/essays/denning. Htm, datum pregleda 25.10.2011.

o prevenciji terorizma iz 2005. godine bio je blizu da se ne usvoji u Vestminsteru oktobra 2005. godine. Naime, opozicija je zahtevala dve stvari: prvi predlog je bio da nove policijske snage treba da zadrže osumnjičene do 90 dana bez optužnice, a drugi predlog je bio da se kazni "ohrabrivanje" ili "glorifikacija terorizma". Što se tiče "glorifikacije terorizma", takva mera bi trebalo da jasno kriminalizuje osnivanje, održavanje i hostovanje brojnih Web sajtova koji trenutno postoje u Velikoj Britaniji.

Glavna kritika je ta da ova odredba može ugušiti legitimne političke govore. Nekoliko drugih mera uključenih u ovom predlogu zakona, koje mogu sankcionisati korišćenje Interneta u svrhe terorizma, kao što je delo pripremanja terorističkih akcija i obuka terorista, su nesporno prošle u parlamentarnim debatama. Ovaj predlog zakona je stupio na snagu i nazvan je Teroristički Akt 2006.

Na međunarodnom nivou, glavne inicijative za kontrolu sadržaja preuzimaju evropske zemlje koje imaju jako zakonodavstvo u oblasti govora mržnje, pa kroz evropske regionalne institucije pokušavaju da nametnu ista pravila i u cyber prostoru. Ključni međunarodni zakonski instrument po pitanju kontrole sadržaja je Dodatni Protokol Sporazuma o cyber kriminalu Saveta Evrope.

Protokol definiše različite tipove govora mržnje koje treba zabraniti na Internetu, uključujući rasističke i ksenofobične materijale, opravdavanje genocida i zločina protiv čovečnosti. OSCE organizacija je takođe aktivna po ovom pitanju. Juna 2003. godine na OSCE konferenciji o "Slobodi Medija i Interneta" u Amsterdamu, usvojene su preporuke o "Slobodi Medija i Interneta", koje promovišu slobodu izražavanja i težnju da se smanji cenzura na Internetu. Juna 2004. godine OSCE je organizovala sastanak na kojem se razgovaralo o odnosima između rasističke, ksenofobične i anti-semitske propagande na Internetu i zločinima mržnje. Fokus ovog događaja bili su zloupotreba Interneta i sloboda izražavanja. Pomenuti događaji obezbeđuju širi akademski i politički pogled na ove aspekte kontrole sadržaja.[8]

Na više praktičnom nivou, u maju 2007. godine ambasadori zemalja Evropske unije su se složili da *online* portal poznat kao *Check the Web*, kancelarije Evropske Policije (Europol), treba da ojača dalju borbu protiv terorizma. Web sajt omogućava zemljama članicama Evropske unije da prikupljaju podatke o Islamističkoj propagandi i čet sadržaju preko Interneta. *Check the Web* je jedino dostupan organima zakona i ekspertima, ali

[8] M. Pisarić, "Stanje i tendencije u suprotstavljanju kompjuterskom kriminalu na evropskom nivou", *Zbornik radova Pravnog fakulteta*, Novi Sad, vol. 45, br. 1, str. 487–505, 2011.

"Bezbedniji Akcioni Plan Interneta" je rezultirao u osnivanju Evropske mreže "vruće linije", poznatije kao *Inhope*, čiji je cilj obaveštavanje o nelegalnom sadržaju od strane javnosti. Danas je na Internetu najviše zastupljen nelegalni sadržaj pedofilije i dečje pornografije.

Donošenje zakona o terorističkom sadržaju na Internetu je domen Vlada zemalja. Međutim, zbog prirode Interneta, privatne kompanije i grupe nisu daleko od toga da se i oni uključe u donošenje zakona. Glavni fokus je na članovima koji nisu državni organi i njihovim naporima iskorenjivanja terorističkog materijala na Internetu. Dve grupe koje su fokusirane na ovome su: Kompanije za pretragu Internet sadržaja i haktivisti.

Monitoring terorističkih Web sajtova

Postoje značajne razlike između raspoloživosti i dostupnosti materijala na Internetu. Činjenica da je određeni sadržaj raspoloživ na Internetu ne znači da je on lako dostupan velikom broju korisnika. Most između krajnjeg korisnika i Web sadržaja je obično mašina za pretragu sadržaja. Međutim, ukoliko se određeni Web sajt ne može naći na *Google*-u ili na drugim glavnim pretraživačkim sajtovima, njegova vidljivost je ozbiljno smanjena. Kod Nemačke i Francuske verzije *Google*-a npr. nije moguće pretraživati ili nalaziti Web sajtove sa Nacističkim materijalom. Ovo pokazuje da postoji određeni nivo samo-cenzure na delu *Google*-a kako bi se izbegli mogući sudski procesi. U pogledu terorističkih Web sajtova, nakon 11. septembra 2001. godine brojne Internet kompanije volonterski brišu sajtove koji su shvaćeni kao teroristički. Na primer, *Yahoo!* je uklonio na desetine sajtova koji se nalaze u Web prstenu Džihada, udruženih 55 Web sajtova o Džihadu, dok je *European Lycos* (Panevropska mreža Web sajtova) osnovao tim od 20 ljudi koji treba da nadgledaju pomenute Web sajtove u slučaju nelegalnih aktivnosti i da uklanjaju terorističke sadržaje. Međutim, takve mere kontrole mogu se okarakterisati kao političke, te se mogu naći na udaru zaštitnika ljudskih sloboda.[9]

Događaji od 11. septembra 2001. godine podstakli su brojne privatne kompanije i pojedince da na Internetu nalaze i ruše terorističke Web sajtove. Računarski hakeri su imali određenu ulogu u ovoj vrsti aktivnosti. Ubrzo nakon napada, grupa koja sebe naziva "Dispečeri", objavila je da će uništiti Web servere i Internet pristup u Avganistanu i drugim zemljama koje podržavaju

[9] Michael Posner, "America already is in a cyber war, analyst says", 2007. Izvor: http://www.govexec.com/story_page.cfm?articleid= 8667, datum pregleda 25.10.2011.

terorizam. Ova grupa je srušila hiljade Web sajtova i pokrenula napade Distribuiranih Odbijanja Servisa (DDoS) protiv meta od Iranskog ministarstva unutrašnjih poslova do Predsedničke palate u Avganistanu.

Međutim, ne pružaju sve hakerske grupe podršku takozvanom hakerskom ratu. Nemačka grupa hakera, *Chaos Computer Club,* je pozvala sve hakere koji su uzeli zakon u svoje ruke da prekinu započete akcije. Jedan od razloga sprečavanja eskalacije napada može biti da su mnogi hakeri bili oprezni po pitanju negativne asocijacije sa terorističkim napadom od 11. septembra, pa su obuzdali svoje aktivnosti. Za teroriste nikada nije bilo jednostavnije krstariti Internetom, čak jednostavnije i lakše nego pre 11.septembra.

Početne stranice sajtova su bile predmet naizmeničnih DDos i drugih hakerskih napada, a takođe su bili i napadi na Internet provajdere što je prouzrokovalo brojne probleme. Na primer, 1997. godine desio se napad bombardovanjem elektronskom poštom koji je bio usmeren protiv Instituta za Globalne Komunikacije (IGC), Internet provajdera u San Francisku, koji je hostovao Web stranice Baskijske separatističke grupe ETA. Napad protiv IGC-a je počeo nakon eskalacije terorističkih aktivnosti vojnog krila ETA na severu Španije. Protestanti su želeli da ugase sajt sa Interneta, pa ga je IGC najzad uklonio sa servera, ali je pre toga sačuvana kopija sajta omogućavajući drugima da postave *mirror* sajtove, te su se isti pojavili na desetinama servera na tri kontinenta.[10]

Od 11. septembra 2001. godine osnovane su brojne zvanične Web organizacije za potrebe nadgledanja terorističkih Web sajtova. Najpoznatiji od ovih tipova sajtova je Web sajt *Internet Haganah*. Takođe, poznati sajt Vašingtona DC-a (*District of Columbia*) je *Search for International Terrorist Entities* (*SITE*), koji je kao *Internet Haganah* fokusiran na Islamističke terorističke grupe. Klijenti koji plaćaju i koriste usluge *SITE*-a su: FBI, državna bezbednost Sjedinjenih Američkih Država i brojne medijske organizacije. Jedan od osnivača i direktor *SITE*-a, *Rita Katz* je prokomentarisala: "U našu korist ide to da postoje neki teroristički sajtovi pokrenuti od strane kompanija u SAD-u. Ako se server nalazi u SAD-u, onda to ide u našu korist kada treba da vršimo nadgledanje aktivnosti." *Aeron Weisburd,* koji je osnovao *Internet Haganah,* kazao je da je njegov cilj da natera ekstremiste da se premeštaju sa jedne adrese na drugu: Naš cilj nije da ih ućutkamo,već da ih nateramo da se premeštaju i komuniciraju kako bi oni napravili grešku, a mi prikupili što više

[10] James A. Lewis, *Assessing the risks of cyber terrorism, cyber war and other cyber threats,* Center for Strategic and International Studies, Washington, 2002.

informacija o njima pri svakom njihovom koraku." Ako bude postojao dokaz o terorizmu na Internetu, *Internet Haganah* će kontaktirati hosting kompaniju i zahtevati od njih da uklone sajt sa njihovog servera. Ukoliko to bude uspešno obavljeno, *Internet Haganah* će zakupiti ime domena kako se adresa nikada više ne bi koristila. Od svog osnivanja 2003. godine, *Internet Haganah* je imao zasluge u gašenju više od 600 sajtova povezanih sa terorizmom.

Na osnovu iznetog dolazimo do zaključka da je počeo treći svetski rat u cyber svetu, odnosno eksplodirala je municija koja se ne čuje, ali uprkos tome odjekuje širom sveta. Inicijalna kapisla bio je *WikiLeaks* i njegov osnivač *Julian Paul Assange*. Posle poteza koordinisanih iz Vašingtona da se *WikiLeaks* onemogući uskraćivanjem servera na Amazonu, odbijanja transfera donacija od strane *Paypal*-a, *Viza*-e i *Mastercard*-a, zatim hapšenja *Assange*-a u Britaniji zbog veoma spornih optužbi za silovanje, u protivofanzivu je krenula "međunarodna cyber-gerila". Pod imenom *Anonimusi*, grupa hakera koji se okupljaju oko zloglasnog foruma *4chan*, otpočela je napad na kompanije koje su pod pritiskom američke vlade otkazale saradnju *WikiLeaks-u*.

U operaciji nazvanoj *Osveta, ratnici* koji *Assange*-a nazivaju političkim zatvorenikom, ali i ljudi koji su svojim ranijim akcijama pokazali da su veoma osetljivi na pokušaje kontrole Interneta od strane država i velikih korporacija, koriste jednostavno, ali moćno oružje, tzv. *bombardovanje* sajtova napadnutih institucija stalnim upitima koji ih onesposobljavaju za normalno korišćenje. Taj softver je poslednjih dana sa Interneta dovlačen tempom od hiljadu instalacija po satu, od čega je jedna trećina instalirana na računare u Sjedinjenim Američkim Državama. Mreža *BotNet*, inače, deluje kao džinovski robot, te niko ne mora da sedi ispred računara kada počne "bombardovanje". Meta su bili *Viza* i *Mastercard*, što je dovelo čak i do hapšenja 16-godišnjeg cyber ratnika u Holandiji, a mreži *Anonimusa* priključili su se i hakeri iz Srbije, jer je ovaj rat udružio sve na planeti, bez obzira na naciju, veru, boju kože ili politička opredeljenja.

Tvrdi se da je rat *Anonimusa* samo lagano zagrevanje za ono što može da se desi svetu, čiji bezbednosni i bankarski sistemi, snabdevanje energijom, saobraćaj i kretanje novca počivaju na upravljanju računarima. To industrijski razvijene zemlje čini ranjivima. Samo nekoliko klikova mišem i sve može, dokazuju hakeri, da se pretvori u haos. Vreme će pokazati kako će se ubuduće voditi cyber ratovi i ko će u njima biti pobednik, a najmoćnije države ozbiljno su shvatile, nimalo naivne, cyber pretnje.

Moć cyber terorista

Cyber ratnici postaju najznačajnija vojska najmoćnijih armija i država sveta. Da rat u virtuelnom prostoru nije mašta, dokazuje činjenica da su razvijene zemlje počele da formiraju cyber vojsku.

Naime, hakeri su kao normalna vojska, ona koja maršira oko nas ili u cyber prostoru, svejedno je, znači angažovani i plaćeni da to rade. Amerikanci su uveli poseban rod u svojoj vojsci koji se bavi cyber ratom, borbom na Internetu i to nije jedina cyber vojska u svetu. Postoje što zvanične, što nezvanične najave da će i druge zemlje uvesti takve jedinice u svojim armijama. Ruski hakeri mogu da se pohvale da su pobedili u prvom cyber ratu, jer je Rusija u sukobu protiv Gruzije u Južnoj Osetiji 2008. godine paralelno vodila vojni i cyber rat. Tvrdilo se da iza ovih napada hakera stoji Rusija kao država, međutim, to nije dokazano. Obaranjem gruzijskih sajtova, a zatim potpunim presecanjem infrastrukture, hakeri iz Rusije su onemogućili vladi i predsedniku Gruzije da komuniciraju sa svojim narodom i sa svetom. To je prvi put u istoriji čovečanstva da je jedna zemlja koristila modernu tehnologiju u ratovanju. Pretpostavlja se da Rusija i Kina, koje su uspele da skrenu i "progutaju" 18 minuta Internet saobraćaja koji im nije odgovarao već imaju više hiljada cyber ratnika.

Nemačka i Engleska su najavile oštru borbu sa cyber terorizmom. Nemačke rupe u informacionoj infrastrukturi učinile su da je ona za cyber ratnike postala lak plen. To se videlo maja 2007. godine kada su strani hakeri prodrli u centralu nemačke vlade i službenicima poslali falsifikovana elektronska pisma.

Kada su otvorili zakačena dokumenta, u njihove računare je neprimetno učitan program štetočina. To je hakerima omogućilo da uđu u informacionu mrežu vlade. Rupa je primećena tek posle nekoliko nedelja, a trag hakera vodio je u Kinu. *Sandro Gaycken,* jedan od vodećih IT stručnjaka savremenog sveta, ukazuje da Nemačka nije jedina zemlja koja je počela da se sprema za moderan način ratovanja, odnosno za ratovanje preko kompjutera. Mnoge druge svetske vlade, takođe su kao ključni deo ratovanja u budućnosti prepoznale uništavanje računarskih sistema ili ometanje elektronskog poslovanja u nekoj državi, poput smetnji rada vlade, banaka i platnih sistema, ali i nuklearnih postrojenja. *Gaycken* ukazuje da se više ne moraju kupovati tenkovi i skupo vojno naoružanje i tehnologije, već da je dovoljan samo "dobar personal". Šta je moguće postići sa dobrim personalom, "videlo se" kada su se *Simensovi* računari širom sveta našli na meti računarskog crva *Staksnet*. Slično je bilo i sa iranskom nuklearnom elektranom *Bušer. Staksnet* je bio vrlo zahtevno programiran, međutim, niko ne

zna ko je "crva" pustio u svet. Glasine kažu da je to bila izraelska tajna služba sa namerom da sabotira iranski atomski program, ali za to još uvek nema dokaza.

Stručnjaci tvrde da ako neko hoće da privredno oslabi Zapad, može da izvodi male, fine, diskretne sabotaže, manipulacije na berzi, da ometa rad proizvodnih pogona i tako izvede niz malih pakosti koje uvek izgledaju kao nezgode ili propusti koji možda i neće biti primećeni. Međutim, za teroriste je virtuelni svet još uvek prevelik zalogaj, jer da bi prouzrokovali značajnu štetu moraju angažovati mnogo kompetentnih programera. Pojedinačne terorističke ćelije to ne mogu. Uprkos tome, signal za prestanak opasnosti ne sme biti dat, a boreći se za slobodu Interneta *Anonimusi* su na delu dokazali kolika je moć cyber ratnika.[11]

S druge strane kriminalci lutaju elektronskim mrežama, uz pomoć visoko razvijenih tehnologija „peru" velike količine novca i kao neka nevidljiva ogromna snaga povlače točak civilizacije unazad degradirajući dosadašnja epohalna dostignuća.[12]

Zaključak

Činjenica je da su pojava modernih računara i korisničkih programa za najširu upotrebu promenili živote ljudi širom sveta. Računari se koriste za drastično ubrzavanje osnovnih kancelarijskih poslova, ali i za složena projektovanja, baze podataka, komunikaciju, informisanje, edukaciju i zabavu. Pomenuti razvoj računara propratio je i razvoj računarskih mreža, odnosno računarskih sistema, od kojih je svakako najpoznatija tzv. svetska mreža Internet. Uporedo sa ovakvim progresom razvijala se i ideja o korišćenju novih tehnologija u protivpravne svrhe.

Očigledno je da je cyber kriminal postao svakodnevnica, a neverovatan razvoj tehnologija uslovio je i neverovatnu diferencijaciju vrsta nedozvoljenih dela koja se njegovim korišćenjem mogu izvršiti i to počev od onih naivnih i bezopasnih koja se uglavnom vezuju za reklamiranje različitih proizvoda do veoma opasnih ponašanja koja spadaju među teška, ponekad čak i najteža krivična dela u mnogim nacionalnim zakonodavstvima. Naime, život je daleko ispred mogućnosti zakonodavca da inkriminiše sve potencijalno opasne

[11] Boško Rodić, Dejan Vuletić, "Sposobnost opstanka informacionih sistema", *Vojnotehnički glasnik*, vol. 53, br. 2, str. 168–177, 2005.

[12] Željko Bjelajac, „Organizovani kriminal vs. Srbija, Pravni fakultet za privredu i pravosuđe u Novom Sadu", „DTA" Beograd, Beograd, 2008, str. 9.

društvene pojave koje su vezane za savremene tehnologije. S obzirom da se broj dela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije cyber kriminala uvećava gotovo svakodnevno, klasifikacija takvih ponašanja je vrlo teška. S jedne strane, klasifikacija je teška zato što se ne mogu utvrditi kriterijumi koji će određena dela svrstati isključivo u jednu kategoriju, dok s druge strane pojave novih načina zloupotrebe nužno iziskuju i proširenje sačinjene liste kriterijuma.

Za razliku od stvarnog, virtuelni svet ne poznaje vremenska i prostorna ograničenja, podložan je stalnim promenama i tehnološkim inovacijama, a zakonska regulativa je ograničenog dometa budući da takve nagle promene "pravo" ne može unapred predvideti i ograničiti. Preterana zakonska ograničenja, osim sprečavanja nepoželjnog, mogu i sputavati i onemogućiti željeni informacioni razvoj i slobodnu razmenu podataka. Na taj način, stalne tehnološke inovacije, raznolikost i dinamičnost tog promenljivog sveta neočekivano i lako pretvaraju propisana ograničenja u suvišne, pa i štetne mere.

Literatura

1. Antoliš Krunoslav, "Prerequisites for Systematic Fighting Terrorism", *Croatian International Relations Review*, Vol. XI, No. 40/41, 2005., 121–125, Zagreb, Croatia, July–December 2005.
2. Bjelajac Željko, Cyber crime and Internet pedophilia as an important international phenomenon, „Western Balkans: From Stabilization to Integration", The Institute for International Politics and Economics, Belgrade, 2012, str. 437–456.
3. Bjelajac Željko, „Organizovani kriminal vs. Srbija, Pravni fakultet za privredu i pravosuđe u Novom Sadu", „DTA" Beograd, Beograd, 2008.
4. Bono Giovanna, "The Impact of 11 September 2001 and the 'War on Terror' on European Foreign and Security Policy: Key Issues and Debates", *Studia Diplomatica*, vol. LIX, No. 1, 2006.
5. Conway, Maura, "*Reality bytes: Terrorist use of Internet*", *First Monday*, Iss. 7,_11. 2002. Izvor: http://outreach.lib.uic.edu/issues/issue7_11/conway/index.html; datum pregleda: 10. 10. 2011.
6. Damjanović, Ivana "Postoji li sajberterorizam?", *Politička revija*, vol. 8, br. 1, str. 237–253, 2009.
7. Denning Dorothy, "Is cyber terror next?", Social Science Research Council, New York, Izvor: http://www.ssrc. org/sept11/essays/denning. htm, datum pregleda 25.10.2011.

8. Lewis, James A.,"*Assessing the risks of cyber terrorism, cyber war and other cyber threats*", Center for Strategic and International Studies, Washington,2002.
9. Pisarić M.,"Stanje i tendencije u suprotstavljanju kompjuterskom kriminalu na evropskom nivou", *Zbornik radova Pravnog fakulteta*, Novi Sad, vol. 45, br. 1, str. 487-505, 2011.
10. Posner, Michael, "*America already is in a cyber war, analyst says*", 2007. Izvor: http://www.govexec.com/story_page.cfm?articleid= 8667, datum pregleda 25.10.2011.
11. Rodić, Boško, Vuletić, Dejan, "Sposobnost opstanka informacionih sistema", *Vojnotehnički glasnik*, vol. 53, br. 2, str. 168-177, 2005.
12. Rodžers Mark,"Psihologija sajber-terorizma", *Bezbednost*, Beograd, vol. 46, br. 1, str. 126–132, 2004.

Žaklina Spalević, Miroslav Vrhovšek, Milovan Jovanović*

COMPUTER NETWORK AS LOGISTIC SUPPORT TERRORIST AND CRIMINAL ORGANIZATION

Summary: The fact is that the Internet and terrorism and a significant global phenomena that shape the various aspects of world politics. Because of its global presence and extensive multilingual context, it has the potential to impact differently on different types of politics and social relations. Unlike traditional mass media, the Internet's open architecture limits the efforts of the Governments of the world to regulate Internet activity, and this provides customers with enormous freedom and space to shape the Internet in their own way. The terrorists now know that a very clever use of traditional mass media, and also recognize the value of direct communication channels. If terrorists want to send a message, they now have a chance to do it without action bombings and assassinations. Words are cheaper than life. The public does not see if you see the terror that terrorists speak on television or the Internet, but if you see the frightened victims of terrorist attacks, and not see the terrorists. On the other hand, state actors and individuals are trying to curb the occurrence of terrorist material on the Internet. Authoritarian governments have had some success in using technology to restrict its citizens from accessing certain sites. There are a number of restrictive options in democratic countries, where,

* Žaklina SPALEVIĆ, The Law Faculty of Economics and Justice, Novi Sad, e-mail: zaklinaspalevic@mail.com.
Miroslav VRHOVŠEK, University Business Academy, Novi Sad, e-mail: vmiroslav@eunet.rs
Milovan JOVANOVIĆ, e-mail: miki80miki@gmail.com.

although they adopted new restrictive laws in a number of judicial authorities is still not clear whether they will be effective as earlier attempts to control, for example controlling cyber hate. In terms of terrorist Web sites and their removal, private institutions, in cooperation with Internet service providers are much more successful, however, the activity of individual activists seriously undermine freedom of speech and those who need to make decisions about these restrictions. Such efforts may actually encourage us to think carefully about the legislation, not only in terms of setting up control, but also in writing robust law of radical political speeches.

Keywords: Internet, Control Internet Content, Internet Governance, Legislative Policy, Cyber Terrorists.