

VIRTUELNA KOMUNIKACIJA U BUDUĆNOSTI

– UPOTREBA I ZLOUPOTREBA

Mr Tanja Tatomirović, komunikolog

Rezime: Budućnost komuniciranja zasnovanog na informacionoj tehnologiji je neizvesna, jer su mogućnosti nemerljive, a brzina razvoja nepoznata. Posledice takvog razvoja društvo oseća već sada, samo petnaestak godina od ekspanzije informaciono-komunikacione tehnologije. Među svim nepoznanicama je i pravac delovanja hakera, jer je nepoznat pravac etičke kontrole informacionog društva – sloboda ili život pod kontrolom? Imajući takve, novonastale, okolnosti u vidu, Ujedinjene nacije su odlukom Generalne skupštine pokušale da regulišu ove rezultate i tendencije razvoja, te organizuju Svetski samit o informacionom društvu World Summit on Information Society ili WSIS.

Ključne reči: *Internet, virtuelno komuniciranje, hakeri, hakerska kultura, antiteroristički zakon, WSIS, informaciono društvo*

Internet je neformalan i otvoren medij, globalno dostupan, jednostavan za korišćenje. Njegova upotreba i interaktivnost kroz aktivno učešće korisnika u stvaranju njegovog sadržaja, navode na mišljenje da ne postoji demokratičniji medij.

U isto vreme, međutim, postoje mišljenja da Internet poprima oblike anarhičnosti. Sloboda na Internetu tumači se i kao svakodnevna zloupotreba mreže od strane korisnika – pojedinaca i organizacija, koji svojim radnjama na Internetu nanose štetu, kako drugim korisnicima, tako i provajderima.

U Srbiji je trend porasta broja korisnika Interneta oko 70.000 novih korisnika svakih šest meseci. Broj osoba koji imaju pristup Internetu danas se može proceniti na sledeći način: *oko 600.000 domaćinstava ima pristup Internetu putem dial-up veze, oko 90.000 domaćinstava putem ADSL-a, oko 80.000 domaćinstava putem kablovskog modema i oko 10.000 domaćinstava putem bežičnih mreža.*¹

Širenje, oblikovanje, menjanje i razumevanje novog univerzuma posredovanog kompjuterskom komunikacijom neprekidno traje. Sagledavanje performansi hipertehnološke ere predstavlja višestruki izazov ne samo za praktičare, već i za teoretičare različitih naučnih disciplina. Danas gotovo nema nauke koja odoleva izazovima, mogućnostima i performansama *sajberkomunikacije*.

Internet je društvo hronične komunikacije². On zamagluje tradicionalne granice između interpersonalnih fenomena i fenomena masovne komunikacije, a takođe i rađa nove mogućnosti i rizike u načinima na koji ljudi stupaju u relacije jedni sa drugima³. Globalna mreža je za mnoge korisnike i teoretičare novi svet slobodnih asocijacija,

¹ Igor Jecl, direktor Direkcije za usluge kompanije Telekom Srbija, „Danas”, 23.juli 2007.

² Strangelove, M, “The Internet, electric gaia and the rise of the uncensored self. Computer-Mediated Communication Magazine, 1 (5)., 1994. ” <http://sunsite.unc.edu/cmc/mag/1994/sep/self.html>

³ Lea, M., & Spears, R., “Love at first byte? Building personal relationships over computer networks”, 1995.

otvorene i permanentne komunikacije, svet *neopterećen dosadašnjim principima* savremene kulture civilizovanog sveta.

Plaćanje računa, naručivanje robe, rezervacija avio-karata, komunikacija sa prijateljima ili poslovnim partnerima, igranje mrežnih igara,... sa bilo kog mesta i u bilo koje vreme su oblici komunikacije u savremenom društvu.

Svako od nas može namerno ili slučajno da pokuša da pristupi bilo kom drugom računaru na Internetu. Podaci koje čuvamo na našim računarima u vidu e-mail poruka, brojeva kreditnih kartica, planova proizvodnje, cenovnika usluga ili robe i sl, predstavljaju izazov velikom broju potencijalnih napadača, od hobista koji upadaju u tuđe sisteme iz zabave, do profesionalnih hakera koji koriste najnovije tehnologije u cilju industrijske špijunaže, ucenjivanja ili drugih kriminalnih aktivnosti.

Privatnost na Internetu je samo delimična. Postoje tehnički načini koji omogućavaju da gotovo svaka poruka koja se prenosi bude *“uhvaćena”*, *“pročitana”* ili *“dešifrovana”*⁴. Svaki korisnik može biti svačiji špijun, a mnoge web stranice imaju programe koji prikupljaju podatke o korisnicima.

Zloupotrebe na Internetu mogu se odnositi na najrazličitije informacije, kao npr. informacije u velikim bazama podataka, informacije o ostvarenom saobraćaju preko Interneta i mobilnog telefona, neovlašćeno korišćenje i upad u baze podataka (izdate lične karte, kriminalističke evidencije, bankovni računi, zdravstveni kartoni, personalni dosijei), neovlašćena izmena ili brisanje podataka, gubljenje podataka iz nehata, prisluškivanje, krađa ličnih podataka, krađa brojeva platnih kartica, prevare prilikom kupovine, primanje neželjenih sadržaja na e-mail – „spam“ (*pornografija, pedofilija, reklame, ...*)...

Virtuelni sukobi

Bez obzira na činjenicu da se sajber-prostor pojavljuje kao neka vrsta samoregulativnog sistema, on zavisi od realne infrastrukture, pa time i od realnih odnosa moći onih koji su delom strukture ušli u ovaj prostor ili bivaju u njemu.

Svaka nova tehnologija predstavlja potencijalnu metu za sajber-teroriste. Uloga Interneta nije zanemarljiva u pripremama za rat. I američki predsednik Buš potpisao je tajnu direktivu Vladi da osmisli kada i kako bi SAD trebalo da lansiraju sajber-napade na neprijateljske mreže. Sajber-ratovanje je neizbežna strategija svake ozbiljnije Vlade, jer u virtuelnom ratu (kao i u pravom) napad često predstavlja najbolju vrstu odbrane.

Ratovi se sve češće sa bojišta sele u virtuelni svet informacija, pa su sajber sukobi, iako ne očigledni, veoma rasprostranjeni i, sa napredovanjem tehnike, sve ozbiljniji.

Konvencionalne ratove vode poznati akteri s jasno definisanim obeležjima, ideologijom i ciljevima. Takvi ratovi, bilo kog obima i trajanja, medijski su praćeni i poznati javnosti. Oni su pitanje života i smrti, slike sa bojišta su dramatične, mediji redovno podsećaju na ljudsku surovost i žrtve.

Virtuelni ratovi su uglavnom ignorisani, primećeni, u većini slušajeva, samo od onih koji imaju profesionalne interese na polju koje je pogođeno takvim ratom. Virtuelni ratnici ratuju bez prolivanja krvi, sa isključivom političkom i ekonomskom komponentom, uz česte psihološke motive grupa ili pojedinaca. Umesto ukopanih vojski

⁴ Nikola Marković (2008), *“Internet i privatnost”*, prezentacija sa predavanja na FPN, 14.april 2008., Beograd

nakrvavim iscrpljujućim bojištima, ratuju male, izuzetno mobilne i tehnološki obrazovane snage naoružane informacijama. Pobjednik je ona strana koja uspeva da brže analizira i eksploatiše informacije. Dominacija u svetu tehnologije postala je preduslov za pobjedu. Ratnici u informacionom ratovanju danas su države, vojske, teroristi, industrijski konkurenti, hakeri.

Sam predsednik SAD izjavio je povodom debate o drastičnom povećanju američkog vojnog budžeta da je sledeći mogući masivni sukob sa teroristima i drugim neprijateljima Amerike na - elektronskom, a ne pustinjskom ili kakvom drugom terenu.

Hakeri i hakerska kultura

Napadačem se smatra svako lice koje neautorizovano pokuša da pristupi podacima, sistemima ili infrastrukturi. Termin haker definiše osobu koja proučava informacione tehnologije u cilju ovladavanja novim znanjima⁵.

Krakerom se nazivaju lica koja ta ista znanja koriste da bi vršila neautorizovan pristup mreži, sistemu ili podacima. S obzirom na to da je termin haker, iako delimično netačan, kod nas odomaćen, nadalje će biti korišćen kao sinonim za upadača.

Hakeri su sve obrazovaniji i cenjeniji, ali su i sve više u funkciji država ili velikih kompanija.

Hakerska kultura je zapravo labavo povezana mreža subkultura koje su ipak potpuno svesne da poseduju i da dele izvesno zajedničko iskustvo, korene i vrednosti. Ta kultura ima svoje sopstvene mitove, heroje, probisvete, folk-epiku, pošalice, tabue i snove. Pošto su hakeri kao grupa posebno kreativne osobe koje sebe ponekad određuju odbacivanjem „normalnih“ vrednosti i navika, oni poseduju neobično bogate i samosvojne tradicije za jednu međunarodnu kulturu koja postoji manje od 40 godina.⁶

Hakerska podkultura razvija se početkom 60-ih godina prošlog veka paralelno sa razvojem tehnoloških inovacija. U okviru hakerske podkulture nastao je i novi način izražavanja karakterističan samo za pripadnike ove kulturne grupe. Njegova funkcija je prvenstveno da isključi iz komunikacije sve one koji ne pripadaju ovoj kulturi, ali i da naglasi postojanje hakerske kulture u realnosti.

Komunikacija među pripadnicima hakerske kulture imaju ogromni uticaj na komunikaciju u svakodnevnom životu. U današnjem svetu tehnologija je ušla u sve pore društva, pa je tako *litspik* neprimetno postao deo svakodnevnog opštenja među ljudima koji nemaju direktne veze sa stvaranjem tehnologije, nego su isključivo njeni korisnici.

Neki od stavova hakera, preuzeti sa Interneta:

- 1. Svet je pun fascinantnih problema koji čekaju da budu rešeni.*
- 2. Probleme ne treba rešavati dva puta.*
- 3. Dosada i besposličarenje su zli.*
- 4. Sloboda je dobra.*
- 5. Sam stav nije zamena za stručnost.*

Ključna vrednost oko koje se formira hakerska kultura je *znanje*. Status pojedinca u hakerskom društvu određen je znanjem koje preda drugima.

⁵ „PSS magazin za bezbednost“, Beograd, 22.april 2008

⁶ Slobodan Lazarević, „Hakerski rečnik“, Solaris, Beograd, 2007.

Bilo da je reč o proučavanju zatvorenih tehnoloških uređaja, o programerskom radu na stvaranju slobodnog softvera ili o provaljivanju u informacijske sisteme koji upravljaju procesima u savremenom društvu, hakovanje uvek polazi od shvatanja da su tehnologije *oruđe društvene kontrole* i da je u društvu kojim dominiraju tehnologije *znanje* o funkcionisanju tehnologija i *kontrola* nad tehnološkim razvojem pitanje političke slobode.⁷

Grupa hakera izvela je 1998.godine žestok napad na Pentagon. Tada su hakeri kontrolisali preko 200 veoma osetljivih kompjuterskih sistema američke armije. Država je preduzela vojnu kontraakciju protiv hakera, koji su hapšeni širom S.A.D.

Tokom 2001. i 2002. godine napadi hakera su nastavljeni. Haker "Solo" je izvršio preko 100 napada na Pentagon, NASA i vojne američke mreže.

Krajem 2002. godine na hakovanim sajtovima FBI, CIA, Pentagon-a ostavljane su antiratne poruke.

Dva Arapina, braća Badir, izvršili su jedinstven hakerski podvig novembra 1999. godine. Virtuelnim ratom doprineli su konvencionalnom ratovanju - blokirali su telefonske linije izraelske armije da bi nakon toga dopustili Palestincima sa Zapadne obale i Gaze da ih koriste za međunarodne pozive na račun izraelske armije.

Poznata uzbuna digla se 1998.godine, kada je utvrđeno da NSA – američka Nacionalna agencija za bezbednost koristi svoje satelite za ilegalno prisluškivanje građana, firmi, državnika u okviru akcije "Ešalon". Ovakvo kršenje građanskih prava je išlo do te mere da je NSA informacije prikupljene od stranih firmi prosleđivala konkurentskim američkim korporacijama.

Najveća kampanja protiv hakera vođena je upravo paralelno sa državnim ilegalnim akcijama prisluškivanja. Hakeri su zato pokrenuli akciju pod nazivom "*Dan obaranja Ešalona*".

U proleće 1999. hakeri su uspeli da "kidnapuju" britanski vojni špijunski satelit „Skynet 4" (veoma važan za NATO u trenutku bombardovanja Jugoslavije). Stav vojske bio je da hakeri neće znati šta da rade s njim, ali su ga oni veoma uspešno programirali i držali pod kontrolom neko vreme.

Za vreme NATO agresije na SR Jugoslaviju mediji su izveštavali o uspesima hakerskog tima "*Crna ruka*". Nakon rušenja sajta „OVK" i nekoliko drugih sajtova, članice NATO su zapretila da će isključiti čitav yu domen na Internetu. "*Crna ruka*" je nestala sa virtuelne scene, ali su nakon bombardovanja kineske ambasade mnogo krupnije akcije izveli kineski i ruski hakeri.

Kevin Mitnik – zvani *KONDOR*, državljanin SAD, ušao je u Ginisovu knjigu kao najozloglašeniiji haker. Vlast je tvrdila da on predstavlja opasnost po društvo, jer i „*preko zatvorske govornice može da lansira nuklearni projektil*".

Mitnik hakuje sredinom 80-ih servere Pentagona i Vazduhoplovne komande Severne Amerike, nastavlja sa upadima na servere "Pacifik bela" (*odakle uzima fajl sa kreditnim karticama svih korisnika, „čisto da ih opomene"*) "Fudžitsua", "Novela", NEC-a", NSA i dr. Tokom 1986. i 1987. godine *Mitnik* vodi veliku bitku protiv korporacija i giganta "Digitala", koji je kumovao tzv. *antihakerskom zakonodavstvu*. Njegovo suđenje postaje medijski linč sa gomilom nelogičnih optužbi, pa izlazi iz pritvora 1989. Njegova meta postaje i Federalna služba bezbednosti (FBI), te ga vladini agenti u nedostatku dokaza iste godine hapse zbog kršenja uslovne slobode. *Mitnik* beži i tri naredne godine

⁷ Izložba "SYSTEM.HACK", Zagreb, 14.jun 2006. i postavke po svetu

vodi se trka između njega i FBI. Posle mnogih akcija i suđenja, pušten je na uslovnu slobodu, uz zabranu korišćenja kompjutera i telefona.

Britancu Geriju Mekinonu se upravo sudi, jer je upao neovlašćeno u stotinu najskrivenijih kompjutera Pentagona i Američke svemirske agencije (NASA). Britanac je priznao da je izvršio na desetine napada, ali da mu je cilj bio da pokaže da „*Amerikanci kriju dokaze o postojanju vanzemaljaca - NLO*“. On je pred sudom u severnom Londonu izjavio da je „*samo želeo da pokaže slabosti u vojnim mrežama SAD*“.

Regulativa i budućnost

Internet, mobilni telefoni i druga savremena sredstva komuniciranja postali su neizbežni deo savremenog društva. Život se u poslednjoj deceniji XX veka izmenio zahvaljujući, između ostalog, i izuzetnom tehnološkom napretku.

Imajući takve, novonastale, okolnosti u vidu, Ujedinjene nacije su odlukom Generalne skupštine⁸ pokušale da regulišu ove rezultate i tendencije razvoja, te organizuju Svetski samit o informacionom društvu (*World Summit on Information Society* ili *WSIS*⁹).

U prvoj fazi u Ženevi (2003.godine) usvojena je Deklaracija o principima informatičkog društva, kao i Akcioni plan delovanja. Na drugom samitu u Tunisu (2005.godine) učesnici su razmatrali kako se realizuju akcioni planovi, a usvojena je i agenda za narednih deset godina, što je i krajnji cilj ovog samita.

Samit je i nastao zbog potrebe da se definišu problemi sa kojima se savremeno društvo susreće, kao i planovi za funkcionisanje i regulativu novog, informacionog društva. Krajnji cilj Akcionog plana WSIS-a je da 50% populacije ima pristup informacionim i kompjuterskim tehnologijama. Kao i u mnogim drugim segmentima funkcionisanja društva, siromaštvo je i ovde najveći svetski problem i u novom, informacionom društvu pojavljuje se kao „digital divide“ (*digitalni, tehnološki jaz*).

Podaci govore da Internet koristi petina odraslog stanovništva u svetu¹⁰, što, samo po sebi, donosi mnogobrojne probleme koji se tiču pristupa Internetu, labavljenja granica između javnog i privatnog, pitanja autorskih prava i pravnih regulativa.

Promene u informacionom društvu su mnogo su brže nego druge društvene promene i zato je neophodno brže reagovanje zakonodavca i prilagođavanje regulative novonastalim situacijama. Ipak, postavlja se pitanje koliko takva zakonska regulativa zapravo ograničava prava pristupu informacijama i prava na slobodno izražavanje i nesmetano komuniciranje na Internetu.

U Velikoj Britaniji, u Zakon o terorizmu je dodat i član koji se odnosi na one koji ugrožavaju javne kompjuterske sisteme i koji će se, od sada, smatrati teroristima. U novom članu zakona se upotrebljava kovanica "*cyberterrorists*", ali nije precizno određeno kada će se neka akcija smatrati terorističkom, a kada ne. Definicija reči "terorista" je proširena, a hakerske grupe bi mogle, faktički, da se poistovete sa IRA-om, Al Kaidom ili Hezbolahom.

Nova dopuna zakona je naišla na neodobravanje i kritiku opozicionih partija u Velikoj Britaniji, dok u SAD borci za ljudska prava i građanske slobode pozivaju vladu SAD da preispita tzv. antiteroristički zakon (*korpus zakona koji predviđaju borbu protiv*

⁸ Odluka Generalne skupštine UN, broj 56/183

⁹ <http://www.wsis-cs.org>

¹⁰ podaci sa <http://www.comscore.com>

različitih vrsta terorizama, kao npr. Patriot Act) koji, takođe, hakere označava kao teroriste.

Jedno od najkontroverznijih pitanja na Internetu je pitanje prostornog važenja nacionalnih zakonodavstava i mesne nadležnosti nacionalnih sudova.

Vlada Hongkonga razmatra mogućnost da usvoji zakon kojim bi se mogao goniti strani sajt koji nudi on-line kockanje građanima te kineske pokrajine.

Sud u Đenovi je nedavno osudio operatera jednog neitalijanskog web sajta za krivično delo klevete.

Francuski sudija je naložio Yahoo-u da prestane sa oglašavanjem za prodaju nacističkog propagandnog materijala, jer je to u suprotnosti sa francuskim pravom.

Zamenici ministara Saveta Evrope su 28. maja 2003. godine usvojili *Deklaraciju o slobodi komunikacije putem Interneta* i *Preporuku o digitalnom emitovanju*. Deklaracija i Preporuka su pripremljene pod pokroviteljstvom Upravnog odbora za mas-medije (CDMM).

U poslednjih nekoliko godina, neke vlade su pokazale tendenciju ka ograničavanju i kontroli pristupa Internetu na način koji nije u skladu sa međunarodnim normama slobode izražavanja i pristupu informacijama.

Upravni odbor za mas-medije Saveta Evrope je odlučio da pripremi Deklaraciju kojom se oštro osuđuje takva praksa, posebno ukoliko je politički motivisana. Deklaracija se bavi onim aspektima Interneta u kojima je sloboda izražavanja i pristupa informacijama posebno ugrožena: *uklanjanje barijera za učestvovanje pojedinaca u informacionom društvu, sloboda davanja usluga putem Interneta, odgovornost posrednika, kao i anonimnost*.

Zvanične tendencije u Evropi još pre pet godina (a pet godina je u virtuelnom društvu čitav vek za mogući razvoj) bile su da se pristup Internetu i digitalnim mrežama mora stimulisati. OEBS je smatrao da se barijere na svim nivoima moraju eliminisati, bilo da su tehničke, strukturalne ili obrazovne prirode.¹¹

U grupama orijentisanim ka očuvanju i unapređenju mrežnih sloboda može se uočiti tvrdnja da će glavne "žrtve" pravnog ograničavanja viruelne komunikacije biti upravo sloboda govora, mogućnost samostalnog promišljanja i zasnivanja ličnih i kolektivnih stavova.

Organizacija za zaštitu ljudskih sloboda Amnesty International¹² kritikovala je neke Internet provajdere i kompanije koje su u nekim zemljama dozvolile kontrolu sadržaja i pristupa Internetu od strane državnih organa. Ova organizacija smatra da je u pitanju „erozija slobode na mreži“.

Smatra se i da, iako je mreža globalna, primena novih tehnologija i informaciono društvo ne bi trebali da utiču na smanjenje kulturnih i nacionalnih različitosti u budućnosti. Svetski samit o informacionom društvu očekuje da zemlje potpisnice učine sve kako bi očuvale kulturno i istorijsko nasleđe.

Prema WSIS-u, države su dužne i da obezbede sigurnost korišćenja informaciono-komunikacionih tehnologija, kao i da otklone mogućnost zloupotreba i da ih sankcionišu ako do njih dođe. U isto vreme, ipak, neophodno je da društvo bude svesno potrebe za usvajanjem novih tendencija koje se tiču segmenata koji nisu postojali pre razvoja

¹¹ OEBS, *Preporuke o slobodi medija i Internetu*, Amsterdam, 14.jun 2003.

¹² <http://www.amnesty.org>

informaciono-komunikacionih tehnologija. Etičke i moralne vrednosti trebale bi da se primene i u domenu ovakvog načina komuniciranja.

U dosadašnjem razvoju, informaciono-komunikacione tehnologije donele su ogromne promene u razvoju društva.

Budućnost i razvoj tehnologije nekada su prikazivani kao mogućnost čoveka da leti ili osvaja svemir. Niko nije mogao sa sigurnošću tvrditi da će nova informaciono-komunikaciona tehnologija biti ta koja će prevladati, kao nešto što nije diktirano iz jednog centra.

Globalna povezanost, preko Interneta, novi je faktor ekonomskog i političkog razvoja čitavog društva. Bezuslovno grabljenje napred kada je informaciona tehnologija u pitanju marginalizovala je i samu filozofiju, kao srž ljudske mudrosti i svela je na marginu ljudskog znanja.

Države, organizacije, kompanije i pojedinci mogu imati skrivene i šifrovane podatke, ali ni takvo čuvanje informacija u današnjem društvu nije garantovano.

Sve opasnosti vezane za virtuelno komuniciranje vrebaju na različitim poljima – političkom, ekonomskom, tehničko-tehnološkom i privatnom, a ipak se društvo sve više „seli“ u informacione sisteme, na mrežu, koja je podložna napadima i pomenutim opasnostima.

Iako izloženi opasnostima, za ove sisteme se ne traži alternativa, već se sve više sredstava ulaže u stvaranje „apsolutno sigurnih“ sistema, koji ne bi bili ugroženi od strane hakera.

A hakeri? Sve što je u digitalnoj formi u domenu je hakerske zajednice i njene akcije. Digitalni svet niko ne poznaje bolje od hakera. Kao takvi, oni su od izuzetnog značaja za budućnost zdravog razvoja društva. Oni su, lišeni interesa državne kontrole i interesa velikih kompanija, jedina alternativa sve kontrolisanoj društvenoj zajednici, reklo bi se. U mogućnosti su da, u budućnosti, ponude potpuno „rušenje“ postojećeg poretka, ali time čine svojevrsnu ravnotežu ili, čak, kontrolišu društvene tokove regulisane od strane države.

Nesporno je da zloupotrebu virtuelnog komuniciranja treba zakonski uobličiti, ali je, isto tako, pozitivno imati i „drugu stranu“, čije postojanje je bitno zbog iniciranja razmene znanja i podsticanja napretka informaciono-komunikacionih tehnologija.

Države će biti ugrožene na taj način što će gubiti svoju moć nadgledanja, kontrole i moći, ali će inventivnost hakera i u budućnosti uticati na sve brži informaciono-komunikacioni i svaki drugi razvoj društva.

Hakere ne može niko uništiti. Za nekoga – oni su kriminalci, za nekoga slobodni duh virtuelne komunikacije. Svakako se mogu gledati i kao izvor problema, ali i kao potencijalno rešenje.

Neizvesna je budućnost komuniciranja zasnovanog na informacionoj tehnologiji, jer su mogućnosti nemerljive, a brzina razvoja nepoznata. Posledice takvog razvoja društvo oseća već sada, samo petnaestak godina od ekspanzije informaciono-komunikacione tehnologije.

Među svim nepoznanicama je i pravac delovanja hakera, jer je nepoznat pravac etičke kontrole informacionog društva - sloboda ili život pod kontrolom?

LITERATURA:

1. *Strangelove, M.* (1994), "The Internet, electric gaia and the rise of the uncensored self. *Computer-Mediated Communication Magazine*, 1 (5)." <http://sunsite.unc.edu/cmc/mag/1994/sep/self.html>
2. *Slobodan Lazarević* (2003), "Hakerski rečnik"
3. *Lea, M., & Spears, R.* (1995). "Love at first byte? Building personal relationships over computer networks"
4. *MacKinnon, R.* (1997), "Journal of Computer Mediated Communication, 2 (4)." Available: <http://www.ascusc.org/jcmc/vol2/issue4/mackinnon.html>
5. *Miroljub Radojković, Mirko Miletić* (2006), "Komuniciranje, mediji i društvo"
6. *Nikola Marković* (2008), "Internet i privatnost", prezentacija sa predavanja na FPN