Izvorni znanstveni članak
355.356(100-622NATO:497.1):004

Virtualni rat

MARINA MUČALO*
NIKŠA SVILIČIĆ**

Sažetak

Je li Wesley Clark, zapovjednik NATO-a, imao pravo kad je ustvrdio da je SR Jugoslaviju, umjesto akcije "Allied Force", trebalo elektronički izolirati?

Jugoslavenski *hackeri i crackeri* u potpunosti su iskoristili slobodu *cyber* prostora. U vrijeme NATO-ove intervencije objavili su prvi pravi "virtualni rat" svim zemljama koje su podržavale tu akciju, a osobito Sjedinjenim Državama. Obrušavajući se svim raspoloživim elektroničkim sredstvima na brojne službene stranice američkih institucija, apsolutno zloupotrebljavajući komunikacijske slobode na Netu, jugoslavenski su *hackeri* zapravo demonstrirali tek djelić mogućnosti nove e-sile. Ipak, posljedice običnih korisničkih djelovanja bile su toliko štetne da su natjerale međunarodnu zajednicu na oštro upozorenje Telekomu Srbije – isključit ćemo vas s Interneta!

Cilj ovoga rada ponajprije je evidentiranje jedne potpuno nove pojave na Internetu, prvoga organiziranog virtualnog rata koji se odvijao u *cyber* prostoru, u vrijeme kad su vođene i stvarne borbene akcije protiv SRJ. Završetak te akcije rezultirao je i "skidanjem" dokumenata s Neta, koji su sačuvani tek u arhivi autora ovog teksta. Dopunskih znanstvenih izvora nema, jer je ključni izvor ovoga rada bio Internet i novinski članci.

Iako zamišljen kao medij dostupan svima, Internet će u bliskoj budućnosti ponajprije morati biti obranjen i zaštićen zakonskim sredstvima. U protivnom, mogao bi jednostavno posustati pod naletom svih zlouporaba i bezbrojnih virusa koji se nalaze u svjetskom *cyber* prostoru. Treba očekivati, s obzirom na porast korisnika i usluga, da će uskoro početi stasavati i potpuno nova grana kaznenog zakonodavstva, računalni kriminal.

1. "Virtualni ratnici"

Izraz *hacker* dolazi od engleske riječi *to hack*, što znači zasjeći, proniknuti u nešto. Etablirao se početkom osamdesetih kad *hacking* nije imao toliko negativnih posljedica. Dapače, informatička ga je industrija donekle i podržavala, jer je popularizirao njezinu djelatnost. Bilo je to vrijeme romantičnih pogleda na dolazeću eru nove tehnologije. Međutim, romantika se vrlo brzo i ugasila.

* *Marina Mučalo*, vanjski suradnik Fakulteta političkih znanosti u Zagrebu na predmetima Radio i Radijski praktikum.

** *Nikša Sviličić*, asistent Fakulteta za organizaciju i informatiku u Varaždinu.

Kao rezultat sve jačih kriminalnih aktivnosti *hackinga*, kojemu je u stjecanju slave pomogala medijska i filmska industrija, danas sve zemlje europske zajednice imaju sankcioniran računalni kriminal. Tomu je ponajprije uzrok masovno korištenje toga načina komunikacije te goleme količine novca što svakodnevno "putuju" ili se izravno troše u *cyber*-prostoru.

Hacking ima brojne podjele prema određenim "specijalnostima". Ubrajaju se tu *insidersi*[1]*, codersi*[2]*, scriptkidds*[3]*, professionals*[4]*,* itd. Ipak, najbrojnija je grupacija *crackera*. Iako *hackeri* odbijaju svaku povezanost s njima i prave oštre granice između *hackinga* i *crackinga*, činjenica je da se bave sličnim poslom, ali s različitim motivima.

Slika 1: Isječak s objašnjenjem razlike hackera i crackera

Crackers and Hackers
(Whats the Difference?)

A Hacker:
A person who enjoys exploring the details of programmable systems and how to streach their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. -- The New Hackers Dictionary

A Cracker:
One who Breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker. -- The New Hackers Dictionary
See The Difference now??

IF YOU ARE A REPORTER PLEASE SAY CRACKER WHEN YOU ARE TALKING ABOUT CRACKERS BREAKING INTO BANK ACCOUNTS AND GETTING CREDIT CARD NUMBERS

Izvor: http://bvsd.k12.co.us/~clarkj/Hackers.html

Izraz *cracker* dolazi od engleske riječi *to crack*, što znači slomiti, skršiti. Najopasnija su grupacija u *hackingu*, jer se radi o znalcima koji su se specijalizirali za provaljivanje u sve vrste stranica. Točnije, nekada su im najveći izazov bile službene stranice američke vlade te stranice vojnih organizacija kojima su potom mijenjali sadržaj i na

[1] Osobe koje su najčešće "iznutra", otpušteni ili nezadovoljni djelatnici koji provaljuju na stranice svojih poslodavaca.

[2] Znalci koji razvijaju *hacking* metode, ali se ne služe njima u ilegalne svrhe, već obavljaju legalne poslove.

[3] Početnici koji provaljuju iz čiste zabave.

[4] Profesionalci su plaćenici koji provaljuju isključivo zato što su plaćeni za taj posao.

njima objavljivali, više ili manje, duhovite poruke. Na samomu početku svojih akcija, *crackeri* nisu stjecali nikakvu materijalnu korist. Dovoljna im je bila *cyber*-slava i spoznaja da su uspjeli upasti, "preurediti" ili uništiti nečiju stranicu. Međutim, s vremenom su se pojavljivali i slučajevi izravnog protupravnog stjecanja materijalne koristi, kao, primjerice, slučaj ruskog *hackera* Vladimira Levina koji je 1994. godine, preko računalnog sustava, upao u newyorško "Citibank" i otuđio deset milijuna dolara. Uhićen je 1995. godine, na londonskom aerodromu Heathrow i osuđen na zatvorsku kaznu. Krakerstvo se počelo pretvarati u vještinu otimanja novca, što je zahtijevalo i hitnu reakciju sigurnosnih službi svih razvijenih zemalja.

Sad već daleke 1989. godine, kad još nije bilo govora o sankcioniranju upada na tuđe stranice, u Amsterdamu je upriličeno prvo svjetsko okupljanje *hackera*[5]. Okupilo se oko dvjestotinjak sudionika iz cijelog svijeta, dok je s onima koji nisu bili nazočni jednostavno uspostavljena *on-line* veza. Sudionici su tri dana razmjenjivali iskustva, prozvali svoje okupljanje "Informatičkom burzom" i zaključili da svakako treba nastaviti borbu protiv "centralizacije informacija u svijetu."

Bio je to tek jedan od brojnih skupova sličnih računalnih znalaca. Međutim, mladenačko je zanesenjaštvo rezultiralo vještinom koja može odvesti u zatvor. Zasad je najpoznatiji slučaj, sad već legendarnog, *hackera* Kevina Mitnicka[6]. Nakon tjeralice ("obične" i elektronske), FBI ga je 1995. godine i uhitio uz pomoć jednog *hackerskog* znalca, Tsotomuo Shimomure. Mitnicku je suđeno zbog prijevara, nezakonitog posjedovanja elektroničkih uređaja, oštećivanja računala i presretanja elektronske pošte. Optužba je imala 25 točaka. Nakon istražnog postupka koji je trajao više od četiri godine, osuđen je, u kolovozu 1999. godine, na dodatnih 46 mjeseci zatvora, te novčanu kaznu. Čak i kad odsluži kaznu, zabranjeno mu je korištenje računala bez posebne dozvole njegova socijalnog radnika.

FBI je danas u oštrom ratu sa svim tipovima *hackera.* Za njima su raspisane tjeralice koje se najčešće oslanjaju tek na *cyber* nadimke, umjesto stvarnih imena. Početkom lipnja 1998. godine, grupe *hackera* iz različitih organizacija napale su organizirano stranice FBI-ja i toliko ih promijenile da su stranice bile privremeno i uklonjene s Interneta. Razlog tog napada bilo je uhićenje grupe *hackera* koji su upali na stranice američke vlade. Poruka "Sad je naš red da udarimo gdje boli!" ostavljena je na svim stranicama kao *hackersko* upozorenje i osveta djelatnicima FBI-ja zbog proganjanja i zlostavljanja *hackera*.

Sedma konvencija *hackera,* koja je održana u srpnju 1999. godine u Las Vegasu, nosila je ime DefCon[7], kraticu od "Defence Convention", što je objašnjeno brojnošću agenata u civilu koji su prisustvovali tom okupljanju. Naime, mjere praćenja i ubaciva-

[5] Mihovilović, Maroje: "Hakeri galaktičkog značenja", *Večernji list*, Zagreb, 26. veljače 1997.

[6] Mitnick je počeo s provalama u dobi od 17 godina. Do 33. godine bio je već šest puta uhićen i osuđivan. Jednom se branio tvrdnjom da je "ovisnik o računalu", pa je poslat na liječenje u psihijatrijsku ustanovu. Nakon što su mu oduzeli računalo i modem, vrlo je brzo pobjegao. Bio je u bijegu dvije godine do zadnjeg, konačnog uhićenja. O njemu je napisano nekoliko knjiga, a sprema se i film.

[7] Škevin, Igor: "Prerušeni agenti, zabava za hakere", *Jutarnji list*, Zagreb,17. srpnja 1999., str. 44.

nja agenata, koje pripadaju u standardne policijske metode, primijenjene su i na *cyber* kriminalce. Jedan od najvećih problema jest otkrivanje stvarnog identiteta tih osoba koje se, u svojim nezakonitim radnjama, najčešće služe nadimkom. Međutim, na takvim se okupljanjima traže i oni *hackeri* koji bi bili voljni pomoći u razotkrivanju prijestupnika.

Imala je i Hrvatska svojih nekoliko minuta "*hackerske* slave" kad su, u veljači 1997. godine, dvojica maloljetnih Zadrana upala na Pentagonovu stranicu. Usprkos pozornosti koju je događaj izazvao u Hrvatskoj, Pentagon je ubrzo izjavio da se radi o nekoj "nevažnoj" stranici i time je priča završena[8].

Upadi na stranice, bez obzira na to o kojem se dijelu svijeta radilo, nisu više toliko spektakularni niti neobični, a događaju se gotovo svakodnevno. "Preuređivanje" stranica velikih kompanija također je postalo gotovo svakodnevna situacija. *Hacking*, međutim, sve više postaje i sredstvo političke borbe i propagande, dobivajući dimenziju "borbe za ideologiju". Međutim, još uvijek ima i slučajeva koji se događaju iz čiste znatiželje, čistog "sportskog *hackinga*", bez namjere da se izvuče neka materijalna korist ili nanese ozbiljna šteta. Takav je slučaj *hackera*[9] iz Jeruzalema koji je provalio u računalo Pentagona u vrijeme Zaljevskog rata, a potom i izraelskog ministarstva obrane. Osobito su ga zanimale rakete "Patriot" pa je stigao i do tajnih podataka. Nakon panike koja je uslijedila, obje su vlade odahnule kad je 18-godišnjak uhićen i stavljen u kućni pritvor bez računala pri ruci.

Prema istraživanjima[10] psihologa Marca Rogersa, prosječni je *hacker* najčešće bijelac iz srednje klase, starosti od 12 do 28 godina, s očitim nedostatkom socijalnih vještina. Gotovo u pravilu dolazi iz nesložne ili razorene obitelji, osamljenik je koji više uživa u komunikaciji Internetom nego izravno. Gotovo djetinjasta razigranost bila je evidentna i na sedmoj konvenciji *hackera* koja je održana u srpnju 1999. godine u Las Vegasu, kad su sudionici "hakirali" računalo dvorane u kojoj se održavao skup ("igranje" s klima uređajem, rasvjetom, ozvučenjem i sl.)[11].

Hackerske su organizacije na Netu[12] vrlo brojne. Moguće je pronaći brojne podatke o povijesti *hackinga*[13], potom raznovrsne upute za *hacking*, tematske elektroničke časopise, datume okupljanja, rječnike[14] i sl. Ujedno, na tim je stranicama i popis najpopularnijih *hackera*, s njihovim kratkim životopisima i posebno istaknutim adresama

[8] Cf. Kovačević, Srđan: "Zadarski incident", *Glas Slavonije*, Osijek, 26. veljače 1997.

[9] Op. cit. Mihovilović, M.: "Hakeri...". Riječ je o Deriu Schribmenu, *hackeru* koji je svojim znanjem oduševio lokalnu policiju koja ga je došla uhititi. Istražitelji su odahnuli jer se ispostavilo da je sve to radio iz puke znatiželje i zadovoljstva, a ne iz razloga špijuniranja ili zarade.

[10] (...): "Hakeri su asocijalni tipovi", *Jutarnji list*, Zagreb, 21. travnja 1999.

[11] Op. cit. Škevin, I. : "Prerušeni agenti, zabava za hakere".

[12] Pretraživač AltaVista na upit "hackers" nudi oko 200 tisuća dokumenata (lipanj 1999.).

[13] <http://sptimes.com/Hackers/history.hacking.html>(lipanj, 1999.)
<http://www.discovery.com/area/technology/hackers/hackers.html>(lipanj, 1999.)

[14] <http://www.discovery.com/area/technology/hackers/glossary.html>(lipanj, 1999.)

koje *hackerima* daju statuse elektroničkih zvijezda. Međutim, treba napomenuti da su i brojni *hackeri* uhićeni te da odslužuju zatvorske kazne.

Međutim, *hackerstvo* je vodilo i razvitku sve jače zaštite informacija na Netu, osobito s obzirom na razvitak elektroničke trgovine (*e-commerce*). Prema Franjiću[15], elektroničko trgovanje nije samo prodaja robe i usluga već ima šire značenje i približava se pojmu poslovanja. Glavni problem širenja *e-businessa* bila je (ne)sigurnost dokumenata i novčanih transakcija. Podizanje razine sigurnosti komunikacije na Netu te uvođenje krivične odgovornosti za nedopuštene radnje, rezultiralo je 1998. godine procvatom elektroničke trgovine. Nakon SAD, elektroničke trgovačke velesile su Njemačka, Velika Britanija, Japan i Kanada[16].

Hackerstvo se, u međuvremenu, počelo usmjeravati prema "želji za istinom", demonstrirajući svoja uvjerenja preuređivanjem "neprijateljskih" stranica. Osobiti izazov predstavljaju službene stranice državnih institucija, među kojima po broju napada iz svijeta prednjače stranice organizacija CIA i FBI. Tijekom listopada 1998. godine, *hackeri* su se obrušili na stranice kineske vlade. Razlog su bila izvješća o stanju ljudskih prava u Kini. Prema rezultatima jednog novinarskog istraživanja[17], gotovo 50 posto svih napadnutih stranica čine stranice koje sadrže neke političke sadržaje ili smjernice određene državne politike.

Demonstracije virtualne moći, a bez nanošenja osobitih šteta, nisu više kažnjive na području Norveške. Naime, po odluci tamošnjeg Vrhovnog suda iz siječnja 1999. godine, svi *hackeri* koji samo upadnu, ali ne nanesu nikakvu štetu, neće krivično odgovarati. Odluka je donesena nakon spora koji se vodio zbog upada djelatnika norveške računalne tvrtke "*Norman Data Defense System*" na računala Sveučilišta u Oslu. Upad je napravljen zbog televizijskog snimanja emisije u kojoj se upozoravalo na nesigurnost norveških računalnih sustava.

3. Crna ruka[18] i Croatian Mind Hackers

Novi Kazneni zakon Republike Hrvatske, koji je stupio na snagu 1. siječnja 1998. godine, prvi put sadrži i odredbu o računalnom kriminalu:

[15] Franjić, Marko: *Digitalna ekonomij@*, Digimark d.o.o., Zagreb, 1999., str. 199.

[16] Ibidem. str. 206-211.

[17] <http:\\www.cnn.com\area\journal\rsrch&\stat\html> (svibanj 1999.)

[18] Organizaciju "Crna ruka" osnovali su srbijanski časnici, potkraj 19. stoljeća. Budući da ih ondašnji kralj Obrenović nije podržavao, ubili su ga 29. svibnja 1903. godine. Ključno načelo organizacije bilo je "ujedinjenje ili smrt". "Crna ruka" je, prema potvrđenim povijesnim kazivanjima, sudjelovala u ubojstvu prestolonasljednika Ferdinanda te kralja Aleksandra u Marseillesu.

Oštećenje i uporaba tuđih podataka

Članak 223.

(1) Tko ošteti, izmijeni, izbriše, uništi ili učini neuporabljivim tuđe automatski obrađene podatke ili računalne programe, kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.

(2) Tko unatoč zaštitnim mjerama neovlašteno pristupi automatski obrađenim podacima ili računalnom programu, kaznit će se novčanom kaznom do stopedeset dnevnih dohodaka ili kaznom zatvora do šest mjeseci.

(3) Kazneni postupak za kazneno djelo iz stavka 1. ovoga članka, ako se ne radi o obrađenim podacima ili računalnim programima državnog tijela, pokreće se povodom prijedloga.

(4) Posebne naprave i sredstva kojima je počinjeno kazneno djelo iz stavka 1. i 2. ovoga članka oduzet će se.

Kompjutorski kriminal u Hrvatskoj dijeli se na tri oblika[19]. Prvi predstavljaju slučajevi u kojima je računalo objekt napada i radi se o neovlaštenom pristupu podacima, njihovom kopiranju, mijenjanju ili uništavanju, te korištenju virusa, logičkih bombi i sl. Drugi oblik su sve kriminalne radnje u kojima računalo služi kao alat za izvođenje, primjerice, generiranje brojeva kreditnih kartica, krivotvorenje dokumenata, ucjene anonimnim *e-mailovima* i sl. Treći je oblik kada računalo služi za sigurnu komunikaciju među kriminalcima i predstavlja svojevrsnu arhivu podataka o kaznenim djelima, što je policiji od osobite važnosti.

Zasad, u Hrvatskoj su zabilježene tek provale na tuđe stranice, bez osobitih materijalnih šteta. Potkraj listopada 1998. godine, svega desetak dana nakon što je "Vjesnik" otvorio svoju Web stranicu, na njoj je osvanula poruka:

"*This site is hacked by Serbia Hackers Team Crna Ruka. Long live Great Serbia*!!".

Pošiljaoci su naznačili i svoju adresu i link. Link je vodio do teksta:

"*Mi nismo za rat!!! Mi ne želimo nikomu zlo!!! Nismo pripadnici nijedne političke stranke, ponajmanje vladajuće. Najmanje što želimo je da ikom pretimo, ali svaki pokušaj da se istina preokrene pokušaćemo da sprečimo na sve moguće načine.*"

[19] Vučetić, Nenad: "Što kaže policija?", *VIDI,* Zagreb, br. 34., 1999.

Hrvatski su *hackeri* odgovorili još istog dana upadom na Web stranicu Narodne biblioteke Srbije. Ostavili su poruku:

> "Čitajte Vjesnik, a ne srpske knjige!!!.
> *Our message to all of you:*
> *We're CROATIAN MIND HACKERS*
> *We fight for liberty of information.*
> *If liberty is anarchy let there be anarchy.*
> *Message to Serbian Hackers: F... YOU!*

Odgovor nije trebalo dugo čekati i bio je znatno ozbiljniji. Provaljeno je u računalo zagrebačkog instituta "Ruđer Bošković", točnije u datoteku korisničkih lozinki. Nije učinjena neka veća šteta, ali je ostavljena poruka da će idućeg puta sve podatke izbrisati. Upad je bio jednostavna demonstracija virtualne moći srbijanskih *hackera*. Nakon toga je iz Hrvatske uslijedilo rušenje stranica Medicinskog fakulteta u Nišu i poruka upozorenja o zabrani diranja u hrvatski *cyber* prostor. Mogli bismo reći "i tako dalje", iako nakon toga hrvatski mediji više nisu zabilježili nikakav spektakularni upad, što ne znači da ih zaista i nije bilo. Novinar[20] zaključuje da je slučaj zabrinuo informatičke stručnjake obje strane i da će se njima vjerojatno "pozabaviti" policija, kako se ne bi pretvorio u sukob koji više neće biti moguće kontrolirati.

"*Croatian Mind Hackers*" dvojica su srednjoškolaca poznata na Internetu po nadimcima *Pozitive Zero* i *Negative Zero*[21].

"...uspjeli smo *haknuti site* u najavljenom vremenu, znači točno u 23 sata. Za mijenjanje glavne stranice trebalo nam je oko 20 minuta, pa se već i po tome može zaključiti da osiguranje NBS-a nije preveliko... na ponovni upad u *cyberprostor* Hrvatske, uzvratit ćemo teškom paljbom", izjavljuju *hackeri*. Odbijaju svaku vezu s politikom, jer je to bila "obrana ponosa Hrvatske i hrvatskih *hackera*".

4. Srbijanski hackeri *protiv svih*

Višegodišnja strahovlada, uvijek na granici ozbiljnog sukoba, koju je srbijanski, a poslije jugoslavenski režim provodio nad stanovništvom Kosova, dobila je svoj epilog sredinom ožujka 1999. godine. Usprkos brojnim upozorenjima međunarodne zajednice, jugoslavenski je režim nastavio sa sustavnim terorom nad kosovskim civilima. Reakcija je uslijedila 24. ožujka 1999. godine, kad je počela borbena akcija NATO zrakoplovstva na području SR Jugoslavije. Akcija je nazvana "Allied Force" ili Zajednička snaga i trajala je do 6. lipnja iste godine, kad je jugoslavenski režim ipak prihvatio uvjete iz mirovnog ugovora.

[20] Slovaček, Velimir: "Proširena bojišnica u *cyber* prostoru", *Glas Slavonije*, Osijek, 9. studenoga 1998.

[21] (...): "Ako srpski hakeri opet napadnu, uzvratit ćemo teškom paljbom!", *Večernji list*, Zagreb, 8. studenog 1998.

Akcija je privukla svjetsku medijsku pozornost. Svakodnevno su brojne svjetske agencije i televizije izvještavale o tom sukobu. Usprkos nazočnosti brojnih novinara, SRJ nije objavila niti jedan dokument u kojem bi jasno odredila pravila ratnog izvješćivanja. Svojevrsna ratna cenzura ipak je djelovala, neki su novinari[22] zamoljeni da napuste SRJ u roku od 24 sata, dok se nekima prijetilo fizičkim obračunom, pa i smrću[23].

Akreditacije za ratne izvjestitelje izdavao je Vojni *press* centar koji je počeo djelovati u Beogradu nekoliko dana nakon početka NATO intervencije. Akreditacije su bile temeljni uvjet novinarskog boravka na području SRJ. Cjelokupne cenzorske ovlasti preuzela je na sebe Informativna služba Štaba Vrhovne komande Vojske Jugoslavije, a sankcije su se temeljile na vrlo nedemokratskim odredbama Zakona o javnom informiranju[24]. Slobodni je novinarski rad bio nemoguć, izvješća su obvezno "pregledavana" u Vojnom *press* centru i svaka je novinarska inicijativa mogla vrlo lako završiti uhićenjem pod optužbom objavljivanja vojne tajne[25].

Većina srbijanskih medija još je odavno stavljena pod kontrolu i nadzor režima. Jedina nezavisna radijska postaja, B-92, zatvorena je krajem ožujka 1999., grubom policijskom intervencijom. Odlukom srbijanske vlade, glavni urednik je smijenjen, pa i uhićen. Radio je ponovo počeo s radom 14. travnja, ali pod potpuno novom upravom i s novim djelatnicima. "Stara" ekipa B-92 svoj je radijski program počela emitirati preko Interneta[26].

Jugoslavenski su *hackeri*, odmah nakon početka borbene akcije, objavili pravi "virtualni rat" brojnim "neprijateljskim" stranicama, osobito stranicama NATO-a, američkog Ministarstva obrane, Senata i vlade. Cilj su bili serveri velikih sustava.

U *cyber* prostoru može se ratovati sljedećim načinima:

- Tradicionalnim *hackingom* koji podrazumijeva upad na tuđe stranice, njihovo "preuređivanje" ili potpuno uništenje;
- *Spam bombing* ili *spam*-poruke znače sustavno i organizirano slanje tisuća *e-mail* poruka različitih sadržaja, koje nakon određenog broja, jednostavno zasite, uspore ili potpuno onesposobe server. Tomu je slična i tzv. ping-metoda koja se sastoji od neprestanog slanja praznih poruka istom serveru. Rezultat je potpuno jednak;

[22] Kolovrat, Igor: "Ekskluzivno iz Beograda", *Globus*, Zagreb, br. 434, 2. travnja 1999. Beograd je u roku od 24 sata morala napustiti i višegodišnja dopisnica "Vjesnika" Vesna Peruničić. Jugoslavenske vlasti nisu joj željele produžiti radnu dozvolu u SRJ.

[23] Ta se prijetnja izravno odnosila na Christiane Amanpour, novinarku CNN-a, koja je pod tajanstvenim okolnostima hitno morala napustiti Beograd. Ratni zločinac Željko Ražnjatović Arkan otvoreno joj je prijetio smrću.

[24] Zakon o javnom informisanju, *Službeni glasnik RS* 36/1998. <http://www.propisi.co.yu/48h/full/glasnik> (travanj, 1999.)

[25] Zbog navodnog odavanja vojne tajne 20. travnja uhićen je Antun Masle, novinar "Globusa". Proveo je u pritvoru gotovo dva mjeseca. Spasio se bijegom.

[26] <http://www.b92.org> (travanj, 1999.)

- Napadi virusima uobičajeni su dodatak *hackingu* i *e-mail* porukama. Virusi se (najčešće) šalju kao "*attachment*", ali i kao "obična" pošta s nekim privlačnim naslovom. Slanje virusa je i bez ratne situacije, vrlo raširena i nemila zabava neodgovornih osoba. Ratno stanje ili cilj koji *hackeri* žele ostvariti osobito su opasni zbog naglog povećanja količine moćnih virusa na Internetu.

Kako se to može raditi, pokazuje i primjer poziva na "bombardiranje *spamom*" (slika 2.) što ga je objavio nepoznati *hacker*[27] iz Beograda. Poruka je sadržavala i adresu primaoca, sveučilišnog profesora iz Belgije, čija je "krivnja" bila isključivo u tomu što se u jednoj prvatnoj e-mail poruci "ogriješio" o tešku ratnu situaciju u SRJ.

Slika 2: Stranica Interneta s originalnim pozivom *hackera* na *spam* akciju.

... saljem vam poruku u prilogu. Primalac je jedan nas naucnik. Trebalo je da on ovih dana ucestvuje na Euroscience konferenciji u Belgiji. Kada je poceo rat, on je ljubazno i jednostavno javio organizatoru da ne moze doci.
Ovo je dobio kao odgovor: Date: Mon, 29 Mar 1999 08:29:38 +0100
From: "Prof. Dr. F. Adams" <adams@uia.ua.ac.be>
To: <obrisano>
Well deserved what you have. get away from that madman and you will in time perhaps be able to go to conferences again.
----------Ovo su reci jednog belgijskog profesora. Covek ima i svoj web-sajt http://inch.uia.ac.be/u/adams a e-mail mu mozete poslati preko mailto:adams@uia.ua.ac.be
----------Molim vas da ovo objavite na vasim web-sajtovima kako bi svi moglida ovu protuvu izbombardujemo mail-ovima kako mu i dolikuje.
Ako neka ima Mellisu-virus, neka mu ga posalje sto pre :-)
Hakeri iz Crne Ruke – evo vam posla.

Izvor: http:\\www.yugoslavia.yu\forum\hakeri&\cruka.html (svibanj 1999.)

Nakon početka akcije "Zajednička snaga" na server NATO-a dnevno je stizalo stotine tisuća elektroničkih poruka uvredljivih i prostačkih sadržaja. Prema riječima glasnogovornika NATO snaga, dr. Jamie Shea, na jednoj od uobičajenih press konferencija tijekom travnja 1999., "goleme količine *spama* usporavale su rad servera, ali ga nisu uspjele onesposobiti."

Tijekom travnja na Webu[28] srbijanskog poduzeća "Telekom" (jugoslavenski Internet *service provider*) pojavilo se obavještenje korisnicima:

[27] <http://beograd.rockbridge.net/arhiva/31martporuke.htm (travanj, 1999.)

[28] <http://www.telekom.yu/obaveštenje.html> (travanj, 1999.)

Administrator Internet okosnice prima veliki broj žalbi inostranih provajdera i njihovih korisnika na nedozvoljenu upotrebu Internet-a iz naše zemlje, posebno u odnosu na SPAM poruke.

U skladu sa uputstvom Ministarstva za telekomunikacije, a da bi sačuvao svoje veze s inostranim provajderima, "Telekom Srbija" a.d. upozorava da će isključivati korisnike koji zloupotrebljavaju Internet.

Isključivanje će se vršiti nakon prve opomene od strane administratora Internet okosnice ukoliko korisnik, usprkos opomeni, nastavi sa nedozvoljenom upotrebom Internet-a.

Pod nedozvoljenom upotrebom Interneta-a podrazumeva se, izmedju ostalog:

- slanje SPAM poruka (slanje e-mail poruka koje primaoci ne žele da primaju),

- neovlašćeni upad u tudje računarske resurse,

- korišćenje Internet okosnice za vršenje nezakonitih radnji.

Stranica je sadržavala i link na veliki dokument[29] pod nazivom "Kako da vodimo medijski rat!" i koji je predstavljao pravu paradigmu u korištenju Interneta u svrhe "virtualnog rata".

U uvodu je stajalo upozorenje o potrebi za ozbiljnošću, jer se "*srpski narod nalazi u ratu s najjačom i tehnički najbolje opremljenom silom na svetu...Pored rata bombama i krstarećim projektilima, protiv nas se vodi jedan od najperfidnijih medijskih ratova zabeleženih u ovom veku. Rat se vodi u svim medijima, a najviše na televiziji – i na Internetu.*"

U nastavku teksta govori se o *spamu* na Internetu, *"...jer u nameri da pokažemo svoju srčanost, ponekad smo skloni da izgubimo meru. Jedan broj domaćih korisnika...šalje ogromnu količinu poruka revolta u mnoge diskusione forume (newsgroups)...i bez obzira što se u suštini slažemo sa sadržajem poruka, moramo upozoriti na jednu izuzetno opasnu situaciju koja pritom nastaje: JUGOSLAVIJI PRETI REALNA OPASNOST ISKLJUČENJA SA INTERNETA*!".

Donosimo samo izbor nekih "uputa" u originalnom izdanju:

- *"Ne pokušavajte da pošaljete viruse ili slične programe ljudima s druge strane, pogotovu na službene adrese američke vlade ili vojnih institucija. Postoji zaštita protiv takvih stvari i nikakve koristi od vašeg pokušaja neće biti. Takva će akcija....samo još više pridoneti mogućem isključenju naše zemlje s Interneta.*
- *Nemojte da preterujete sa spam bombardovanjem, može da bude kontraproduktivno.*
- *Pokažimo da smo uljudni: svoje apele protiv ubijanja i razaranja u našoj zemlji treba da izrazimo pristojnim rečnikom, a ne vulgarnošću, svadjom i pljuvačkim parolama.*
- *Nemojmo slati spamove, pogotovo ne osobama ili organizacijama koje su van političkih krugova.*

[29] <http://www.tippnet.co.yu/medijski rat/yu.htm>(travanj, 1999.)

- *Koristite engleski za korespodenciju. Većina ljudi će tako lakše i brže primiti informaciju.*
- *Ukazujte da katastrofa pogadja sve u Jugoslaviji, koncentrišite se na ljudska stradanja, žene i decu.*
- *Ukoliko adresirate više ljudi iz bilo kog razloga, koristite 'Bcc' (blind carbon copy), a ne 'Cc' (carbon copy). Na ovaj način se izbegava zloupotreba (namerna ili slučajna) e mail adresa koje korisnik može da dobije.*

Ako surfujete:
- *Tražite lokacije na kojima ima glasanja oko primene sile u Jugoslaviji.*
- *Pokušajte da nadjete informacije koje idu nama u prilog, pogotovu na lokacijama poznatih medijskih kuća poreklom iz Nato zemalja.*
- *Posećujte sve javne vladine i vojne sajtove Nato zemalja. Cilj je da se svaki 'hit' registruje i natera da administratori troše vreme na analizu logova.*
- *Nemojte da posećujete prezentacije Albanske iredente. Administratori ovih sajtova treba da znaju da ih malo ljudi posećuje.*

Zaključak:
Sigurno vam ne treba objašnjavati kolika je moć Interneta. Budite svesni da je agresor angažovao značajne resurse u nameri da postigne uticaj na korisnike Interneta u Jugoslaviji, budući da nas smatraju elitnom ciljnom grupom. Ne sumnjajte da će u skorijoj budućnosti doći do daljnjeg razvoja događaja i na Internetu. Ovo je dragocen resurs koji moramo iskoristiti u intenzivnoj kampanji apelovanja protiv agresije NATO pakta, ali pritom moramo PO SVAKU CENU sačuvati vezu sa svetom ovim putem. Ne dozvolimo da se naše ponašanje protumači kao povod za odsecanje Jugoslavije sa Interneta.".

Dokument završava brojnim upozorenjima na "unutarnje i vanjske neprijatelje", te korisnim savjetima o zaštiti od mogućeg špijuniranja sadržaja elektroničke pošte.

Primjer ovih "medijskih pravila" koja su trebala zaštiti "jedinu jugoslavensku vezu sa svijetom", za sada je jedinstven. Očito je i funkcionirao, jer SRJ nije bila isključena s Interneta.

Postupak isključivanja može se odvijati u dvije faze. Prva je faza djelomično isključenje ili postavljanje inkriminiranih domena na *black hole* ili "crnu listu". Druga faza nosi potpuno isključenje zbog stavljanja cijele domene na "crnu listu. Dakle, prije potpunog isključenja domene ostavlja se mogućnost da lokalni provider uvede kontrolu nad inkriminiranim domenama, čime bi izbjegao obstrukciju *cyber* prostora.

5. Zaključak

Jedinstveni "virtualni rat" u dosadašnjoj povijesti Interneta samo je potvrdio goleme mogućnosti ovog medija. Već spomenuta izjava[30] zapovjednika NATO snaga, generala Wesleya Clarka u studenom 1999. godine, to je i potvrdila.

Na sjednici Odbora za oružane snage američkog Senata, Clark je ustvrdio da je NATO, umjesto bombardiranja SRJ, trebao "žešće napadati računala u Beogradu i Miloševićeve bankovne račune, zagušiti i preusmjeriti srpske komunikacije i propagandu." Ujedno, ponajprije s obzirom na tehnološku nadmoć NATO-a, Clark se založio i za cjelovitu promjenu dosadašnje ratne strategije, zalažući se za češće i efikasnije korištenje elektroničkih mogućnosti. Clarkova podrška metodama *cyber*-rata jedno je od rijetkih priznanja stvarnih mogućnosti današnje, aktualne i masovne, elektroničke komunikacije.

Rezultate nekog *cyber* rata možemo još uvijek samo pretpostavljati. Zasad su mogućnosti Neta zloupotrijebljene "jednostavnijim" kriminalnim radnjama. Austrija od 1999. godine sankcionira čak i uznemiravanje korisnika slanjem *spam* poruka. Netove slabe točke još uvijek ostaju otvorenim i (zasad) neriješenim problemom. To je ponajprije zaštita privatnosti te pitanje zaštite autorskih prava.

"Računalni kriminal" u međuvremenu je dobio i svoje "računalne forenzičare", osobe koje mogu ući u trag već izbrisanim dokumentima, osobito sadržajima elektroničke pošte. Najpoznatiji slučaj "forenzične analize" *e-maila* zbio se u sudskoj parnici[31] oko monopolističkog položaja "Microsofta", gdje je sadržaj već izbrisane poruke postao ponovno vidljiv te poslužio kao dokaz protiv "Microsofta".

Literatura

Knjige

Franjić, Marko, Digitalna ekonomija, Digimark d.o.o., Zagreb, 1999.

Članci

Keserović, B.: "Bombardiranje SRJ moglo se izbjeći Cyber-ratom", *Večernji list*, Zagreb, 6. studenog 1999.

Kolovrat, Igor: "Ekskluzivno iz Beograda", *Globus*, Zagreb, br. 434, 2. travnja 1999.

Kovačević, Srđan: "Zadarski incident", *Glas Slavonije*, Osijek, 26. veljače 1997.

Merkaš, Nataša: "Piši, briši, ali se čuvaj", Banka, *MZB d.o.o.,* Zagreb, br. 7, srpanj 1999.

[30] Keserović, B.: "Bombardiranje SRJ moglo se izbjeći Cyber-ratom", *Večernji list*, 6. studenog 1999., str. 10.

[31] O tomu pobliže: Merkaš, Nataša: *Piši, briši, ali se čuvaj*, *Banka,* MZB d.o.o., Zagreb, br. 7, srpanj 1999., str. 86-87.

Mihovilović, Maroje: "Hakeri galaktičkog značenja", *Večernji list*, Zagreb, 26. veljače 1997.

Slovaček, Velimir: "Proširena bojišnica u cyber prostoru", *Glas Slavonije*, Osijek, 9. studenoga 1998.

Škevin, Igor: "Prerušeni agenti, zabava za hakere", *Jutarnji list*, Zagreb, 17. srpnja 1999.

Vučetić, Nenad: "Što kaže policija?", *VIDI*, Zagreb, br. 34, 1999.

(...): "Ako srpski hakeri opet napadnu, uzvratit ćemo teškom paljbom", *Večernji list*, Zagreb, 8. studenoga 1998.

(...): "Hakeri su asocijalni tipovi", *Jutarnji list*, Zagreb, 21. travnja 1999.

Internet

<http://sptimes.com/Hackers/history.hacking.html> (lipanj, 1999.)

<http://www.discovery.com/area/technology/hackers/hackers.html> (lipanj, 1999.)

<http://www. discovery.com/area/technology/hackers/glossary.html> (lipanj, 1999.)

<http://www.cnn.com/area/journal/rsrch&/stat/html> (svibanj, 1999.)

Zakon o javnom informisanju, Službeni glasnik RS 36/1998.

<http://www.propisi.co.yu/48h/full/glasnik> (travanj, 1999.)

<http://www.b92.org> (travanj, 1999.)

<http://beograd.rockbridge.net/arhiva/31mart/poruke.htm (travanj, 1999.)

<http://www.telekom.yu/obaveštenje.html> (travanj, 1999.)

<http://www.tippnet.co.yu/medijski rat/yu.htm> (travanj, 1999.)

Marina Mučalo, Nikša Sviličić

VIRTUAL WAR

Summary

Was Wesley Clark, NATO's commander-in-chief, right when he said that, instead of launching the operation 'Allied Force' against it, the allies should have electronically isolated SR Yugoslavia?

Yugoslav hackers and crackers used to good advantage the freedom of the cyberspace. During NATO's intervention, they declared a real 'virtual war' to all the countries supportive of this campaign, particularly to the USA. By swooping down by all available means on numerous official web pages of various American institutions and totally abusing the communicational freedoms on the Net, Yugoslav hackers in fact demonstrated a small part of the possibilities of the new e-force. However, the deleterious consequences of Yugoslav on-line users' activities were so harmful that they prodded the international community into issuing a blunt warning to the Serbian Telecom - we shall switch you off from the Internet!

The objective of this research is primarily to evidence a totally novel phenomenon on the Internet, the first organized virtual war taking place in the cyberspace, at the time when a real military campaign was waged against SRY. One of the outcomes of these activities was 'striking out' the documents from the Net that had been preserved only in this texts' authors' archive. There are no additional scientific resources, since the key sources for this article were the Internet and newspaper articles.

Although envisaged as a medium available to all, the Internet must soon be safeguarded and protected by legal means. Otherwise, it might simply cave in under the onslaught of all abuses and innumerable viruses circulating the global cyberspace. Due to the increase in the number of users and services, it may be expected that soon a completely new branch of criminal law is to emerge - computer crime.