Primljeno: studeni 2009.

KRUNOSLAV ANTOLIŠ*

Internetska forenzika i *cyber* terorizam

UVOD

Internet je sastavni dio života suvremenog čovjeka, koji ga rabi s punom sviješću o njegovoj koristi, ali nerijetko s nedovoljno informacija o ugrozama koje izravno ili u paketu s njim ugrožavaju njegovu privatnost u užem ali i sigurnost u širem smislu.

Zloporaba interneta činjenica je s kojom se danas dnevno susrećemo, a sigurno je najopasnija ona od strane terorista. Oni se internetom ponajprije služe u svrhu širenja terorističkih ideologija i poticanja na počinjenje terorističkog akta te kao platformom za novačenje i obučavanje terorista. Internetom se služe u pripremi te tijekom terorističkog napada kada im on služi kao komunikacijska infrastruktura.

Problemi koji se pojavljuju na planu borbe protiv zloporabe interneta u terorističke svrhe ponajprije su pravno formalne, a potom i informatičke naravi. Na tom je planu potrebno stvarati pravne i informatičke preduvjete za učinkovitu borbu protiv terorista i to svima onima koji su zaduženi da nas zaštite od terorista, ali i nama samima. Veliki doprinos toj borbi, stvaranje je nove i jačanje postojeće informacijske infrastrukture u kojoj će internetska forenzika, kao narastajuća disciplina, imati istaknutu ulogu.

Zakonsko osmišljavanje međunarodnih pravnih normi u području interneta danas je jedan od najvećih pravnih izazova. Doprinos borbi protiv terorizma koji je moguće dati s toga stajališta je nemjerljiv, jer nas međunarodno prihvaćeni pravni okvir stavlja u prepoznatljivu poziciju legalista, tj. daje legitimitet svemu onome što činimo u skladu s pravnom normom u borbi protiv najveće opasnosti suvremenog čovjeka, a to je definitivno terorizam. Zloporaba interneta od terorista danas je sveprisutna, dok je istodobno zakonska regulativa nedorečena ili u ovoj današnjoj formi i sadržaju međunarodno gledano neprihvatljiva. U prilog ovoj tezi ide primjerice i činjenica glede prihvaćanja europskih normi i to ponajprije *Konvencije o kibernetičkom kriminalu* (NN-MU 9/02., 4/04., 4/08., 7/08.) i *Konvencije Vijeća Europe o sprječavanju terorizma* (NN-MU 10/07., 1/08.). Spomenute konvencije

* dr. sc. Krunoslav Antoliš, profesor visoke škole na Visokoj policijskoj školi MUP-a RH, Zagreb.

jedino združene daju dovoljno prostora za učinkovitu borbu protiv terorističke zloporabe interneta. No, žalosna je činjenica kako su do ovoga trenutka spomenute konvencije zajedno prihvaćene od strane svega dvanaestak zemalja, a napominjemo činjenicu kako je otvoren prostor da se u prihvaćanje ovih konvencija uključe i zemlje koje nisu članice Europske unije kao što je primjerice Hrvatska. Ove brojke govore u prilog tezi kako sve do sada učinjeno nije niti približno dovoljno, kako bi se, primjerice, bar na razini Europske unije mogli učinkovito boriti protiv terorističke zloporabe interneta. Ni budućnost spomenutih konvencija ne prepoznaje se kao svijetla, jer najveće svjetske sile ne pokazuju interes za međunarodno pravno reguliranje interneta. Istodobno, nažalost, u situaciji smo da se s nacionalnog stajališta samostalno moramo nositi s problemom svekolikih ugroza koje nas vrebaju s interneta, a da u tom pogledu nismo u prilici računati na pomoć saveznika, jer je, primjerice, u tom smislu politika NATO saveza prilično eksplicitna i kaže kako je briga o informacijskoj sigurnosti nacionalno pitanje, a ne pitanje saveza i to po onoj narodnoj poslovici: "Pomozi si sam, pa će ti i Bog pomoći." Dakle, u ovom pogledu ni u kojoj situaciji, kada je riječ o *cyber* napadu, ne postoji mogućnost aktiviranja članaka ugovora NATO saveza, po načelu – ako je napadnuta neka od članica – da su ostale dužne pružiti pomoć, tj.u slučaju da je napadnut NATO savez u cjelini, kao što je to slučaj kod klasičnog napada konvencionalnim oružjem. Na tragu ovog koncepta NATO savez ne prepoznaje ni internet kao kritičnu infrastrukturu saveza o čijoj bi sigurnosti brinuo. Situacija u kojoj se nalazi svijet u ovom trenutku je u tom pogledu više nego zabrinjavajuća, jer ne postoje jasne pravne norme o internetu međunarodno prihvaćene, pa se tako u slučaju *cyber* napada bez obzira tko iza njih stajao (pojedinci, organizirane skupine, teroristi, države ili savezi) nalaze u prilično nezavidnoj situaciji, te su i reakcije na njih u biti upitne sa stajališta međunarodnog legitimiteta, tako da to više sliči na onu narodnu poslovicu: "Tko jači, taj kvači." Međunarodna pravna forma nužna je i poradi legalizacije metoda, tehnika i alata, primjerice, internetske forenzike, koje su nam jedine na raspolaganju kada smo napadnuti. I to prije svega da bismo se primjereno zaštitili, a potom i ustanovili tko stoji iza napada, i precizirali barem lokaciju s koje je napad ostvaren. Važnost interneta za nacionalna gospodarstva, ali i svjetsko gospodarstvo, iz dana u dan sve je veća, te je i potreba za stvaranje međunarodno prihvatljivog pravnog okvira neupitna, a posebice sa stajališta zakonitosti progona svih onih koji se tom globalnom platformom služe za realizaciju svojih *cyber* napada, te za njihovo dovođenje pred lice pravde, što je preduvjet demokratskog koncepta življenja u suvremenom društvu.

1. INTERNETSKA FORENZIKA

Pojam internetska forenzika eksplicitno nas povezuje s temeljnom zadaćom ove discipline, a to je istraga internetske infrastrukture u svrhu prikupljanja dokaza potrebitih pri istraživanju nezakonitih aktivnosti pojedinaca i skupina, te s osmišljavanjem sigurnosnih rješenja za nadzor i prevenciju ugroza s interneta. No, kao što je to slučaj i s računalnom forenzikom, razni autori daju nam različite definicije pojma internetske forenzike, u okviru kojih se jedni usredotočuju na metodologije kojima se koriste internet forenzičari, drugi na alate koje koriste internet forenzičari, a treći na svrhu i razloge primjene internetske forenzike.

Jedno od najtežih pitanja koje se može postaviti u svezi s internetskom forenzikom, definiranje je točnog datuma i mjesta njenog nastanka, a problem leži u njezinom izrastanju iz računalne i mrežne forenzike, koje se javljaju sredinom osamdesetih godina prošloga stoljeća. Počeci se izravno povezuju s određenim akcijama FBI-a u konkretnim procesima u SAD-u, te s pokretanjem sustava izobrazbe za osobe koje su zadužene za policijske istrage u kojima se prikupljaju i istražuju računalni dokazi. Godine 1989. u Federacijskoj policijskoj vježbovnoj središnjici (*Federal Law Enforcment Training Center*) i to njegovom Institutu za istraživanje financijskih prijevara (*Financial Fraud Institute*), počinje se sa stvaranjem programa i protokola za rad s nadolazećom disciplinom – računalnom forenzikom, koja je danas u svijetu poznata i priznata znanstvena disciplina.[1] Situacija s internetskom forenzikom u svjetskim okvirima nije ni približno tako dobro statusno određena, a njezino pojavljivanje u formi discipline otpočelo je s početkom novog milenija. Kao jedan od prvih jačih sustavnih iskoraka na tom planu objava je knjige Robera Jonesa pod nazivom Internetska forenzika (*Internet Forensic*) s podnaslovom Uporaba računalnih dokaza u rješavanju računalnog kriminala, a koja je tiskana 2005. godine.[2]

Za nove pojmove struke i znanosti nije nebitan pokazatelj o pojavnosti i prisutnosti pojma na globalnoj razini, tj. onaj kojega možemo dobiti istraživanjem pojavnosti pojma na internetu i njegove frekventnosti kroz određeno vremensko razdoblje, te usporedbe sa sličnim pojmovima kao što su to primjerice računalna i/ili mrežna forenzika. Može se uočiti da je 2003. godine frekvencija na Google tražilici za pojam "računalna forenzika" 60 600, "mrežna forenzika" 3 250, a "internetska forenzika" 146.[3] Današnje pretrage daju sljedeće rezultate: "računalna forenzika" 296 000, "mrežna forenzika" 20 000, a "internetska forenzika" 3 370. Evidentan je najveći porast od čak 23 puta pojavnosti pojma "internetska forenzika", što se moglo očekivati s naslova eksponencijalnog rasta interneta u posljednjem razdoblju, a samim tim i s rastom mogućnosti za razne oblike njegove zloporabe, izučavanjem kojim se težišno bavi internetska forenzika. Dakle, kao i mnogo puta do sada, Zapad je taj koji se u tom smislu može s pravom smatrati mjestom rođenja internetske forenzike. S novim tehnologijama pa tako i onima iz sfere IT, koje uz određenu vremensku zadršku stižu i u Hrvatsku, dolaze njene dobre ali i loše strane. Pred nama je u ovom trenutku izazov da učeći iz naučenih lekcija Zapada pokušamo umanjiti loše strane, a iskoristimo dobre.

Na tragu ovog izazova Visoka je policijska škola u svoje nastavne sadržaje ugradila i ovu problematiku, koja se ojačava i s konkretnim praktičnim radionicama, poput radionice na temu Digitalni dokazi i računalna forenzika. U okviru te radionice uporabom konkretnog forenzičkog alata *EnCase Forensic 11.6.2* bavili smo se konkretnim problemima računalne forenzike, od sudskog naloga koji je nalagao provedbu pretrage forenzički ispravne slike predmetnog računala, do zaključnog stvaranja sudski prihvatljivog izvješća[4].

Pored osposobljavanja vlastitih stručnjaka za prikupljanje i obradu računalnih dokaza, od velike su koristi i forenzički eksperti koji su sposobni i ovlašteni vještačiti

---

[1] *http://www.mile2.com/What_is_Computer_Forensics.html*
[2] *http://www.amazon.com/Internet-Forensics-Robert-Jones/dp/059610006X*
[3] *http://www.berghel.net/col-edit/digital_village/aug-03/dv_8-03.php*
[4] *http://www.bestnetworksecurity.com/images/uploads/guidance-for-education.pdf*

u konkretnim slučajevima, kada je znanje potrebito za uspješno vještačenje takvo da ga nije moguće pronaći u redovima policije. Sa stajališta internetske forenzike otvaraju se, dakle s pravom, i pitanja angažiranja vanjskih eksperata, ali i jasnih traženja sa stajališta njihovog poznavanja istražnih radnji i postupaka. Sličan je slučaj sa sudskim vještacima, kojima je pored područja u kojem su eksperti, potrebno i poznavanje zakonskih rješenja te sudske prakse, kako bi njihove ekspertize bile uporabljive u sudskom postupku. Praksa iz zapadnih zemalja, primjerice Velike Britanije, takva je da problematiku angažiranja vanjskih eksperata za računalnu forenziku razrađuje u formi standarda, *British Standard European Norm International Standardization Organization accreditation* – BS EN ISO (Britanski standard - Europske norme za međunarodnu standardizaciju akreditiranja organizacija).

Konkretno tu su BS EN ISO 9001:2000, koji govori o prilagođenosti sustava upravljanja standardima ili BS EN ISO 27001, koji određuje usklađenost sa standardima informacijske sigurnosti[5].

2. TERORIZAM I INTERNETSKA FORENZIKA – GLOBALNA, REGIONALNA I NACIONALNA RAZINA

U sagledavanju svekolikih ugroza koje nam dolaze iz sfere terorizma, a posebice u svezi s tim povezana pitanja informacijske sigurnosti, dobro je poći od mudrosti do kojih su došli oni koji su na temu sigurnosti ozbiljno i sustavno promišljali, a dijelom ih i zapisali u knjigama poput one Sun-cu-a, Umijeće ratovanja[6]. I tu prije svega mislim na sljedeće:

> *"Upoznaj neprijatelja da bi ga pobijedio.*
> *Najteže stvari na svijetu moraju biti načinjene dok su još lake, najveće stvari na svijetu moraju biti načinjene dok su još male.*
> *Duboko znanje je: biti svjestan smetnji prije smetnji, biti svjestan opasnosti prije opasnosti, biti svjestan razaranja prije razaranja, biti svjestan nesreće prije nesreće.*
> *Pobijediti bez borbe je najbolje."*

Ako se slažemo s tezom da je informacija moć, onda je sigurno potrebito osmisliti zaštitu sustava koji je po svojoj naravi stvaraju, pohranjuju, prenose i dostavljaju ovlaštenim osobama, a to su informacijski sustavi te također i infrastrukture koja ih globalno podržava, a to je internet. Strateški okvir za borbu protiv terorizma dan je putem *Nacionalne strategije za prevenciju i suzbijanje terorizma Republika Hrvatske* (NN 139/08.). Hrvatski zakonski okvir koji osigurava zaštitu od terorizma i inih ugroza informacijskih sustava, uključuje i *Konvenciju o kibernetičkom kriminalitetu*, te *Zakon o informacijskoj sigurnosti* (NN 79/07.). Kvaliteti pravnih normi na nacionalnoj razini pridonijele su i izmjene i dopune Kaznenog zakona (NN 152/08.) te Zakona o kaznenom postupku (152/08.), a koje su nastale i usklađene temeljem Konvencije Vijeća Europe o sprječavanju terorizma. One, primjerice, uvode u kazneno zakonodavstvo Republike Hrvatske novu

[5] *http://www.articlesnatch.com/Article/Is-More-Regulation-Needed-To-Ensure--Computer-Forensics-Experts--Are-Up-To-Standard-/568054*
[6] *http://hr.wikipedia.org/wiki/Sun_Cu*

definiciju kaznenog djela terorizma (čl. 169. KZ-a), te kaznenih djela koja se izravno vežu uz terorizam, a ona se odnose na novačenje i obuku za terorizam (čl. 169.b KZ-a) te javno poticanje na terorizam (čl. 169.a KZ-a).

Republika Hrvatska, pored domaćeg zakonodavstva u području borbe protiv terorizma, ima i obveze preuzete na međunarodnoj razini, koje svakako nisu malene, a posebice tu moramo voditi brigu o međunarodnoj bilateralnoj suradnji na planu borbe protiv terorizma koja je formalizirana ugovorima sa 29 zemalja svijeta, a u što su uključene prije svega i sve susjedne zemlje. Potom su tu i obveze iz multilateralne suradnje, te obveze preuzete od strane međunarodnih organizacija kojih je Hrvatska član, kao što su UN, NATO, i druge koje su formalizirane u rezolucijama, konvencijama i protokolima. Iz svega spomenutog razvidno je da se terorističko djelo može izravno povezati s pitanjem informacijske sigurnosti, tj. da informacijska sigurnost nacionalne razine može biti ugrožena terorističkim aktom – *cyber* napadom s interneta.

Upravo je prostor koji je težišno zahvaćen internetskom forenzikom zloporaba interneta te uspostava određenih sustava i sigurnosnih rješenja s naslova ugroza koje vrebaju s interneta. Internetska forenzika je kao forenzička disciplina u zapadnim zemljama nešto što polagano ali sigurno zauzima svoj značajni prostor u sferi borbe protiv računalnog kriminala. Ono što internetskoj forenzici još uvijek ne polazi za rukom na svjetskoj razini, za razliku od računalne forenzike, jest etabliranje u formi znanstvene discipline, no strukovno gledano – internetska bi forenzika zbog svoje posebnosti i trendova, mogla s vremenom poprimiti i tu dimenziju. Što se tiče situacije kod nas, internetska forenzika još je u povojima, samo je se dijelom prepoznaje, i to ponajviše u sklopu predavanja koja su težišno vezana uz računalnu i/ili mrežnu forenziku.

Važnost računalne forenzike razvidna je i s pozicije činjenice o kojoj nas izvješćuju svjetski forenzički sajtovi, i upozoravaju kako je 85% sveukupno počinjenih kaznenih djela ostavilo tragove u formi računalnih dokaza[7]. Razvitak forenzičkih alata ima i svoju protutežu u istodobnom razvoju softvera koji upravo imaju kontra zadaću, a ona je uništavanje dokaza, što je zasigurno novi strukovni izazov, ali i prijetnja informacijskoj sigurnosti.[8]

Ne samo kriminal na računalima, nego i sve ono što se može svesti na zajednički nazivnik – računalni kriminalitet, svakodnevno je prisutno i u Republici Hrvatskoj. Također ne treba biti policijski ekspert da bi se zaključilo da je računalni kriminalitet u porastu, jer se nažalost po tome nimalo ne razlikujemo od ostalih europskih zemalja. Ako želimo biti i egzaktni, tu su i statistike MUP-a RH koje govore u prilog ovoj tvrdnji.[9] No ono što ponajviše utječe na rast računalnog kriminaliteta jest porast uporabe informacijskih tehnologija, te zaživljavanje elektroničkih oblika poslovanja pri čemu ponajprije mislim na kartično poslovanje, elektroničku trgovinu i dr. Sve spomenuto moguće je prepoznati kao potencijalnu metu računalnih kriminalaca, koji nisu nužno samo hrvatski građani, o čemu govori i niz primjera iz policijske prakse. Tako, primjerice, zbog kartičnih prijevara tijekom 2007. godine u ožujku je u Zagrebu uhićeno šest osoba državljana Velike Britanije, u lipnju je u Rijeci uhićeno šest osoba rumunjskih državljana, dok je u kolovozu u Zagrebu

[7] *http://www.mile2.com/What_is_Computer_Forensics.html*
[8] *http://www.evidence-eliminator.com/*
[9] *http://www.mup.hr/UserDocsImages/statistika/2009/pregled_08.pdf*

uhićen jedan državljanin Malezije[10], a u PU splitsko-dalmatinskoj i zadarsko-kninskoj organiziranom su akcijom uhitili tzv. bugarsku grupu[11].

Hrvatska policija sustavno prati sve pojavne oblike računalnog kriminaliteta, a zbog njegove međunarodne dimenzije tu je neizostavna i intenzivna suradnju s Interpolom i Europolom.

3. RAČUNALNI KRIMINAL I NACIONALNO ZAKONODAVSTVO

Postavlja se pitanje hoće li računalni kriminalitet u budućnosti rasti? Odgovor na ovo pitanje je nažalost potvrdan. Osobno očekujem porast računalnog kriminaliteta i to proporcionalno implementaciji novih tehnologija, a posebice informacijskih koje u svojoj osnovi počivaju na računalnoj infrastrukturi. Može se očekivati porast računalnog kriminaliteta u području elektroničkog poslovanja, a što je vidljivo iz iskustava zapadnih zemalja. Činjenica je da nove tehnologije, a posebice one informacijske, daleko brže dolaze do nas i na krilima globalizacije ulaze u sve sfere suvremenoga života. Kriminalci su ti koji, čini se, nažalost imaju svojstvo brze prilagodbe novim tehnologijama i u njihovoj zloporabi vide prostor za nezakonito, brzo bogaćenje. Po tome su velikim dijelom gotovo uvijek u prednosti u odnosu na one koji su tu da ih na zakonit način u tome spriječe, tj. u odnosu na policijske snage koje uporište za svoje djelovanje crpe iz zakonske regulative. Zakonska regulativa je ona koja se nažalost prilično sporo mijenja i prilagođava novonastalim situacijama, jer je pokretanje izmjena i dopuna zakona još uvijek postupak ponajprije determiniran onime što se već dogodilo – dakle kurativan, a tek manjim dijelom onime što bi se tek moglo dogoditi tj. preventivan. Takav je slučaj i s izmjenama i prilagođavanjem nacionalnog zakonodavstva borbi protiv računalnog kriminaliteta, a posebice propisivanjem zakonitog postupanja na području prikupljanja, obradom i predočavanjem sudu računalnih dokaza.

U hrvatskom zakonodavstvu postoje ponajprije dvije razine propisivanja kaznenih djela. Jedna je razina zakonskih obveza preuzetih iz međunarodnog zakonodavstva, tipa konvencija, protokola i sl. Primjer konvencije je *Konvencija o kibernetičkom kriminalu*, a primjer protokola je *Dodatni protokol uz Konvenciju o kibernetičkom kriminalu o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava*.

Sljedeću razinu čine Kazneni zakon[12] i Zakon o kaznenom postupku[13] koji propisuju kaznena djela i iz područja računalnog kriminaliteta, te način zakonitog postupka pribavljanja dokaza. Tu je posebice značajno za ovu problematiku istaknuti Zakon o izmjenama i dopunama Kaznenog zakona (NN 105/04.) koji u hrvatsko zakonodavstvo donosi, tj. propisuje sljedeća kaznena djela: dječja pornografija na računalnom sustavu ili mreži (čl. 197.a), povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava (čl. 223.), računalno krivotvorenje (čl. 223.a), računalna prijevara (čl. 224.a).

---

[10] *http://www.mup.hr/6780/1.aspx*

[11] *http://www.vjesnik.hr/html/2009/03/30/Clanak.asp?r=tem&c=1*

[12] Kazneni zakon. (NN 110/97., 27/98., 50/00., 129/00., 51/01., 111/03., 190/03., 105/04., 84/05., 71/06., 110/07., 152/08.)

[13] Zakon o kaznenom postupku. (NN 110/97., 27/98., 58/99., 112/99., 58/02., 143/02., 115/06. 152/00., 76/09.)

4. INTERNETSKA FORENZIKA I *CYBER* TERORIZAM

Internet kao komunikacijska platforma suvremenog čovjeka, nerijetko je poslužio za krađu identiteta i slične oblike zloporaba. No ono što nas danas posebice brine jest zloporaba interneta od strane terorista. Poseban problem predstavlja *cyber* terorizam, koji je ilustrirao svoju snagu i moć primjerice u slučajevima Estonije, Gruzije, Kirgistana, a u najnovije vrijeme to su napadi na informacijske sustave državne uprave u SAD-u, Južnoj Koreji[14]. Unatoč mnogobrojnim zakonskim rješenjima koja danas uvelike pružaju mogućnosti uspostave visokog stupnja informacijske sigurnosti, internet je kao dio informacijske infrastrukture još uvijek, u pravno formalnom smislu uvelike ostao u zrakopraznom prostoru. Sve ono što danas vidimo da se događa putem interneta u smislu, ponajprije njegove zloporabe od strane terorista, nije moguće spriječiti upravo zbog njegovog globalnog karaktera, tj. zbog nepostojanja globalnih i općeprihvaćenih jedinstvenih pravnih normi. Te norme morale bi imati međunarodni karakter, a zadaća bi im se svodila na cjelovito normativno obuhvaćanje svega onoga što je internetom fizički dostupno. Usmjerenost normi trebala bi biti orijentirana ka zemljama domaćinima davateljima internetskih usluga. Tu je bitno propisati ovlasti i odgovornosti za nadzor sadržaja i usluga. Sljedeća razina normi su one u svezi s ovlastima za reagiranje i sankcioniranje nezakonitog ponašanja.

Sve ovo bilo je razlogom da u sklopu predavanja na temu Internet i globalni teroristički pokret, koje sam u srpnju, 2009. godine održao na međunarodnoj konferenciji o terorizmu u Münchenu, potaknem izradu međunarodnog zakona o pravu interneta, po uzoru na sličan međunarodni pravni akt o pravu mora.[15] Kao što je more globalno prisutno, smatram da s pravom možemo uočiti i sveprisutnu dimenziju interneta na globalnoj razini, uz važnu napomenu, a to je da za razliku od mora ne postoji zemlja koju internet ne oplahuje.

5. ZAKLJUČAK

U borbi protiv zloporabe interneta prije svega moramo se usredotočiti na stvaranje pravnih ali i tehničkih preduvjeta, kao što je primjerice daljnji razvitak internetske forenzike. Pravne norme moraju se usmjeriti na ovlasti i odgovornosti zemalja domaćina – davatelja internetskih usluga, za nadzor sadržaja i usluga, a potom i ovlasti za reagiranje i sankcioniranje. Ovaj napor najveći je pravni izazov međunarodne zajednice, a istodobno i najveći doprinos u borbi protiv terorizma na globalnoj razini – posebice uzimajući u obzir terorističke zloporabe interneta koje su danas globalnih razmjera, s jasnim ciljem uspostave globalnog terorističkog pokreta. Ono što je izrazito naglašeno briga je o normativnom uravnoteživanju demokratskih sloboda i njihovom ograničavanju na internetu. S pravom se može očekivati kako će nacionalna razina informacijske sigurnosti sve više biti ugrožena i terorističkim djelovanjem s interneta. Kao mudar odgovor na ovakve trendove potrebito je pristupiti izgradnji preventivnih mehanizama zaštite IDS tipa – *Intrusion detection system* (Sustav za otkrivanje neovlaštenog upada u računalne sustave), temeljenih na

---

[14] *http://online.wsj.com/article/SB124701806176209691.html*

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

zakonitostima internetske forenzike, kako bi se pravodobno pripremili za napad na našu informacijsku infrastrukturu, koju bi se s pravom moglo proglasiti kritičnom nacionalnom infrastrukturom. Velika važnost internetske forenzike ogleda se i u situacijama kada se dogodi *cyber* napad, koji nismo uspjeli spriječiti mjerama informacijske sigurnosti i IDS-ovima. Tada nam je internetska forenzika ponovno od velike koristi jer nam pomaže u raščlambi onoga što nam se dogodilo, te identificiranju i prikupljanju računalnih dokaza o počiniteljima.