Prof. dr Duško Vejnović, redovni profesor Univerziteta u Banjoj Luci, predsjednik Evropskog defendologija centra, Banja Luka, glavni i odgovorni urednik časopisa *Defendologija* i *Sociološki diskurs*

ZLOUPOTREBA INFORMATIČKE TEHNOLOGIJE U TERORISTIČKE SVRHE

Informatička (računarska) tehnologija postala je neminovnost i potreba svih članova savremene društvene zajednice. Svi smo svjesni ogromnog značaja upotrebe računara u savremenim društvima i činjenice da nema oblasti ljudske djelatnosti u kojoj računari nisu našli svoju primjenu. Zahvaljujući njihovoj ogromnoj moći u memorisanju i brzoj obradi velikog broja podataka, automatizovani informacioni sistemi postaju sve brojniji i gotovo nezamjenjivi dio cjelokupnog društvenog života svih subjekata (fizičkih, ali i pravnih lica) na svim nivoima. Tako računar postaje svakodnevni i nezaobilazni dio, segment svih sfera društvenog života od proizvodnje, prometa, vršenja usluga pa do nacionalne odbrane i bezbjednosti u najširem smislu. Upravo ova činjenica, da se računar koristi gotovo u svim segmentima našeg života, ukazuje na mogućnost njegove raznovrsne zloupotrebe. U početku primjene računarske tehnologije, kompjuteri nisu bili podobni za veće zloupotrebe, jer njihova primjena nije bila masovna, tako da se njima bavio samo uzak krug korisnika, informatičkih stručnjaka. Ono što je otvorilo vrata širenju mogućnosti da se kompjuterska tehnologija zloupotrebi u različite svrhe jeste njen brz razvoj, pojednostavljenje upotrebe, ali i dostupnost iste širokom krugu korisnika.Veoma je interesantna oblast **zloupotrebe informatičke tehnologije u**

terorističke svrhe, odnosno posljednjih godina postaje veoma zanimljiva materija kompjuterskog terorizma, kao svojevrsne forme kompjuterskog kriminaliteta. Računarski (informatički) kriminalitet je nemoguće definisati jedinstvenim i preciznim pojmovnim određenjem. To je „opšta forma kroz koju se ispoljavaju različiti oblici kriminalne aktivnosti, forma koja će u budućnosti postati dominantna.“[1] Naime, teškoće u definisanju **računarskog kriminaliteta** proizilaze zbog toga što se radi o relativno novom obliku kriminalnog ponašanja, ali i zbog toga što postoji velika fenomenološka raznovrsnost ove pojave, koja se teško može obuhvatiti jednom definicijom. Zbog toga, ističemo da je neophodno imati veoma širok pristup prilikom definisanja ove vrste kriminalnog ponašanja. Prva definicija kompjuterskog kriminaliteta potiče iz 1979. godine, i data je u Priručniku Krivičnog pravosuđa vezanog za računarski kriminalitet *Criminal Justice Resource Manual on Computer Crime,* a glasi **„računarski kriminalitet predstavlja svaki nelegalni akt za čije je uspješno krivično gonjenje neophodno dobro poznavanje kompjuterske tehnologije.“[2]** Ovakvo gledište je prilično široko postavljeno, ali je odmah prihvaćeno, pa čak je nekoliko godina kasnije unijeto u Studiju o međunarodnim pravnim aspektima kompjuterskog kriminala u 1983. godini. Ako detaljnije analiziramo karakteristična obilježja, uočavamo da je osnovna osobina računarskog kriminaliteta prvenstveno velika fenomenološka raznovrsnost, ali i specifičnost učinilaca ovih krivičnih dijela. Naime, „....postoje različite kategorije učinilaca računarskog kriminaliteta, obzirom da postoji mnoštvo različitih djela koje čine, ali i imajući u vidu motive koji ih pokreću u vršenju ovih aktivnosti.“[3] Brojni su pojavni oblici zloupotreba informatičke tehnologije, a obzirom da je ova vrsta

[1] Parker D., *Fighting computer crime*, Press, New York, 1983., pp.70

[2] The Criminal Justice Resource Manual on Computer Crime je pripremljen od strane SRI International, Menlo Park, California, USA, za Ministarstvo pravde SAD u 1979. godini

[3] Matijasevic J. and Spalevic Z., „*Specific characteristics of computer criminal offenses with regard to the law regulations“*, XLV International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2010 CONFERENCE, 23.-26. June 2010., Faculty of Technical Sciences, University „St. Clement Ohridski“, Bitola, Ohrid, Macedonia, pp.234

kriminaliteta u konstantnom razvoju i širenju, svakodnevno smo svjedoci nastanka novih, sve složenijih i opasnijih formi kompjuterskog kriminaliteta. Zatim je bitno pomenuti i specifičnost prostorne dimenzije kriminalnog djelovanja, uključujući i transnacionalni karakter kriminalnih radnji, vremensku dimenziju kriminalnog djelovanja, tj. brzinu činjenja krivičnih djela, zatim, konstantno širenje na nove oblasti društvenog života, težinu posljedica i visinu šteta nastalih činjenjem krivičnih djela iz ove oblasti, veliku tamnu brojku, uslijed čega dolazi do otežanog otkrivanja i dokazivanja učinjenih delikata, način vršenja i otkrivanja kriminalnih radnji, specifičan profil učinioca, velike mogućnosti prikrivanja izvršenih krivičnih dijela, kao specifičnost proistekla iz uslova stvorenih dejstvom većine karakterističnih obilježja kompjuterskog kriminaliteta, višestruku uloga računarske tehnologije i dr. Potrebno je naglasiti da pored krivičnih djela koja su usmjerena protiv bezbjednosti računarske tehnologije i elemenata informacionog sistema, postoji veliki broj tradicionalnih krivičnih djela koja se uz pomoć korišćenja računara i računarskih komponenti vrše brže, lakše, učiniocima se teže ulazi u trag, a posljedice su daleko ozbiljnije i veće[4]. **Razvijena informatička tehnologija postala je posljednjih godina vrlo efikasno sredstvo u rukama terorističkih organizacija za ostvarivanje njihovih destruktivnih ciljeva.** Naime, nove sofisticirane tehnike pružile su ne samo dobre mogućnosti za realizacije novih napada, već i za zaštitu sopstvenih kanala komunikacije, kao i promovisanje fundamentalističkih ideja. Teroristi više nisu geografski ograničeni u okviru određene teritorije, niti politički ili finansijski zavisni od pojedinih država. Oni se danas oslanjaju na savremene komunikacione kapacitete u okviru kojih internet ima veoma značajnu ulogu. Imajući u vidu da je veliki broj visokostručnih kadrova iz informatičke oblasti

[4] Matijašević J. i Petković M.: Krivična dela protiv bezbednosti računarskih podataka – analiza pozitivnopravnih rešenja i značaj u kontekstu suzbijanja visokotehnološkog kriminala, Zbornik radova sa međunarodne naučnostručne konferencije „Kriminalističko-forenzička istraživanja“, održane od 14.-15. oktobra 2011. godine, Internacionalna asocijacija kriminalista - IAK, Banja Luka, broj strana: 598-609, Vol. 4, Broj 1, str. 599

dostupan terorističkim organizacijama, svjesni smo opasnosti od zloupotrebe kapaciteta visoke tehnologije od strane terorista u narednim periodima. Akt računarskog sajber terorizma bi se mogao definisati kao korišćenje informacionih resursa u vidu prijetnje ili ucjene da bi se ostvario određeni teroristički cilj. Ono što ovako definisanom aktu nedostaje jeste jedan element terorizma, odnosno korišćenje ili prijetnja korišćenja fizičkog nasilja, tako da je pomenuta definicija bazirana na pretpostavci da u informacionom ambijentu dovođenje javnosti u stanje straha nije više neophodno, niti je neophodno uništavanje dobara i primjena nasilja nad ljudima da bi se ostvarili određeni teroristički ciljevi. Prema tome, glavni cilj je remećenje umijesto destrukcije, mada ni ona nije isključena, jer u društvima visoko zavisnim od informacione tehnologije remećenje informacionih sistema može izazvati kratkoročne probleme različitog obima i intenziteta, ali i mnogo značajnije, dugoročno gubljenje povjerenja u sposobnosti, u pouzdanost ovih sistema. Najvažnija područja primjene interneta od strane terorista su: planiranje i koordinacija, upravljanje operacijama (praktično više nije potreban fizički kontakt između onih koji upravljaju operacijama i onih koji neposredno izvode akcije), propaganda, prikupljanje sredstava, publicitet, psihološki rat, prikupljanje podataka, regrutovanje i mobilizacija, umrežavanje, dijeljenje informacija, pranje novca, kibernetički rat cyberwar, lažne kupovine sofisticirane opreme, bioterorizam (npr. oglašavanje falsifikovanih i lažnih lijekova), itd. Korišćenje interneta od strane terorista može biti trojako: kao oružje *cyber terrorism*, kao način komunikacije među aktivistima i kao medij za obraćanje javnosti. Cyber - terorizam, kao prvi način korišćenja interneta od strane terorista, se odnosi na smišljene, politički motivisane napade na računarske sisteme, programe i podatke koji kao ishod imaju nasilje i strah protiv civilnih meta.[5] Prvi teroristički napad na kompjutere zabilježen je još

[5] Zirojević M., „Upotreba novih informatičkih i komunikacionih medija u svrhe terorizma“, *Revija za bezbednost – stručni časopis o koripciji i organizovanom kriminalu,* Centar za bezbednosne studije, godina II, Br. 11/2008, Beograd, str. 5

1969. godine u Američkoj državi Mičigen, gdje su pripadnici jedne antiratne organizacije pod imenom *Beaver 55* napali centar za elektronsku obradu podataka poznatog hemijskog koncerna *Dow Chemical*, za koji se tvrdilo da proizvodi bojne otrove, napalm i drugo hemijsko oružje. Drugi način korišćenja interneta jeste kao sredstvo komunikacije među aktivistima. Poznato je da je Osama Bin Laden komunicirao sa pripadnicima Al Kaide putem pokretnih kompjutera i bežične mreže putem enkriptovanih poruka *encrypted messages*. Treći način korišćenja interneta od strane terorista odnosi se na obraćanje javnosti putem globalne računarske mreže. Brojne organizacije su ušle u internet prostor i stvorile svoje internet *web* stranice. „...Teroristički napadi se često vrlo pažljivo organizuju kako bi privukli pažnju elektronskih medija i međunarodne štampe. Uzimanje i zadržavanje talaca samo pojačava dramu. Sami taoci ne znače ništa teroristima. Njihova ciljna grupa su gledaoci, a ne stvarne žrtve.“ [6]

Redovan sadržaj *web* stranica terorističkih organizacija čine informacije vezane za istorijat nastanka organizacije i bitnih događaja tokom razvoja, političko i društveno određenje, biografski podaci lidera i istaknutih članova organizacije, njihovi govori i tekstovi, selektivni opisi značajnih aktivnosti u prošlosti, informacije o političkim i ideološkim ciljevima, kao i vijesti koje sadrže obavještenja o aktuelnim dešavanjima, takođe selektivno prikazanim, izbjegavajući nasilnički aspekt svojih aktivnosti. Zbog brojnih prednosti, internet je pogodan medij za predstavljanje jedne terorističke organizacije u svjetlu kakvom ona to želi i sa ciljevima koji se ovim putem vrlo efikasno mogu prikazati i ostvariti. Jedan od ciljeva predstavlja obezbjeđenje podrške što većeg broja pristalica, kao i korišćenje vješto urađenih i prilično sadržajnih prezentacija i tekstova u cilju opravdavanja svojih aktivnosti, dok je često prisutno i demantovanje bilo kakve upotrebe nasilja prilikom vršenja

[6] Jenkins B. V., *International Terrorism*, Crescent Publications, Los Angeles, 1975., pp. 65.

aktivnosti organizacije. Danas sve aktivne terorističke grupe imaju bar jedan oblik prisustva na internetu. Rezultati praćenja u periodu od 1998. do 2007. godine ukazuju na preko 5000 terorističkih *web* sajtova, *online* foruma i tzv. soba za *chat*. Neke grupe imaju više od jednog Internet sajta – jedan glavni tzv. *Home page* i veći broj nezvaničnih. Sa druge strane, „…računari su ponekad postajali i meta terorističkih organizacija. svojevrjemeno su IRA (Irska republikanska armija) i RAF (Frakcija crvene armije) izvršili više napada na kompjuterske centre u Engleskoj, Irskoj i Njemačkoj, u kojima su bili bazirani podaci o djelovanju terorista.“ [7] Sve više postajemo svjesni činjenice da informaciona tehnologija jeste dragocjeno oruđe u rukama jedne terorističke organizacije, ali ne smijemo izgubiti iz vida činjenicu da su rezultati tehnološkog napretka dostupni svim ljudima i državnim strukturama, i da u tom smislu, koristeći iste prednosti informacionih tehnologija možemo ispratiti svaku negativnu pojavu, pa tako i djelatnosti terorističkih organizacija. Kao što možemo vidjeti iz svega prethodno navedenog, možemo slobodno reći da **terorizam je sve ozbiljnija prijetnja čovjeku, životnoj sredini, pravnoj državi, demokratiji, vladavini prava, međunarodnom miru i stabilnosti.** Nekadašnji problem nacionalne bezbjednosti postao je predmet svjetske bezbjednosti, a time i visoke svjetske politike, pa i (opravdanog i neopravdanog) međunarodnog intervencionizma. Negativni efekti terorizma manifestuju se kroz najmanje tri dimenzije državnog i društvenog života: ljudsku, ekonomsku i bezbjednosnu (u užem smislu). Ljudska dimenzija odnosi se na kršenje ljudskih prava mnogih direktnih i indirektnih žrtava terorizma. Problem je tim veći što mnoge države još uvijek nisu koncipirale posebne strategije za prevenciju i suzbijanje terorizma, odnosno za zaštitu ljudskih prava potencijalnih i aktuelnih žrtava, što najčešće uslovljava njihovu viktimizaciju; ekonomska dimenzija odnosi se na efekte

[7] Aleksić Ž. i Škulić M., K*riminalistika*, Pravni fakultet Univerziteta u Beogradu i Javno preduzeće „Službeni glasnik“, Beograd, 2007., str. 391.

terorizma koji dodatno produbljuju nepovoljne činioce ekonomske tranzicije koji su, između ostalog, jedan od uzroka i uslova njegovog nastanka i bezbjednosna dimenzija, koja se tiče ugrožavanja nacionalne bezbjednosti usporavanjem procesa demokratizacije tzv. „tranzicijskih društava“, podrivanjem demokratskih institucija i vladavine prava, i stvaranjem brojnih socio-ekonomskih problema. Slabe i korumpirane državne institucije i neadekvatna legislativa onemogućuju uspješno suprotstavljanje ovom problemu, što iznutra i spolja ugrožava nacionalnu bezbjednost.Na spoljnopolitičkom planu, terorizam može indirektno da podstakne dezintegraciju, onemogućavanje ili otežavanje integracije države u određene međunarodne institucije i organizacije, uvođenje određenih oblika sankcija, intervencije međunarodne zajednice ili velikih sila kojima se ugrožava integritet zemlje kao i osudu međunarodne zajednice zbog toga što je vlada nesposobna da mu se suprotstavi, ne želi to da učini ili ga podržava. Posljedice po nacionalnu bezbjednost identične su posljedicama političkih i ekonomskih pritisaka. Na unutrašnjem planu države, efekti terorizma su izuzetno složeni, latentni i nerijetko predstavljaju strategijski rizik po bezbjednost države i građana usled aktivnosti kao što su: „…….ugrožavanja života ljudi, odnosno njihovog povrjeđivanja i smrti kao posljedica terorističkih napada; ugrožavanja zdravstvene bezbjednosti ljudi. Naime, osjećaj nesigurnosti građana i strah po egzistenciju, tj. po ličnu (porodičnu) i imovinsku bezbjednost je psihička reakcija čovjeka na terorizam. Stres, najčešće kontinuirani (tzv. serijski), u mnogome se odražava na fizičko i mentalno zdravlje i doprinosi efektu tzv. paranoičnog stanovništva; ugrožavanja životne sredine, biljnog i životinjskog svijeta, jer su degradacija životne sredine, epidemije i epizootije potencijalne posljedice tzv. ekološkog i bio terorizma, što se odražava i na bezbjednost ljudi, podstiče emigraciju i ugrožava poljoprivredu i prehrambenu industriju, a time i prehrambenu bezbjednost ljudi; destabilizacije ekonomije i ekonomskog investiranja, jer su nestabilna i krizna područja nesigurna za strane

investicije, što uslovljava pad proizvodnje, rast nezaposlenosti i siromaštva i razvoj „sive ekonomije“.[8] Osim toga, terorizam je nerijetko usmjeren prema nacionalnoj ekonomiji tzv. **ekonomski terorizam,** i to protiv proizvodnih kao i industrijskih kapaciteta, turističkih destinacija i objekata, (međunarodnog i unutrašnjeg drumskog, željezničkog, vodenog i vazdušnog) saobraćaja; ugrožavanja energetske bezbjednosti zemlje tzv. **Energetskim terorizmom** kojim se napadaju energetske instalacije i destimulišu investitori i izvoznici energije; ugrožavanja socijalne bezbjednosti, kao posljedice ugrožavanja života i zdravstvene bezbjednosti stanovništva i destabilizacije ekonomije; ugrožavanja finansijske stabilnosti države, jer složene akcije na preventivnom, represivnom planu i planu zaštite i pomoći žrtvama od strane vladinog i nevladinog sektora zahtijevaju velika budžetska izdvajanja; demografske destabilizacije države, ubijanjem stanovništva, padom prirodnog priraštaja, emigracijom u druge zemlje zbog straha od terorizma, degradacijom životne sredine i narušavanjem ekonomske i socijalne bezbjednosti; povećanja nacionalnog i vjerskog nacionalizma i tenzija, polarizacijom i fragmentacijom društva po etničkim, vjerskim, rasnim, socijalnim i političkim kriterijumima i produbljivanjem starih i rađanjem novih netrpeljivosti i mržnji između pripadnika ovih grupa; ekspanzije tzv. medijskog kriminala, odnosno terorističkih akata uslovljenih podsticajima masovnih medija i destruktivnom psihološkom propagandnom djelatnošću, kojima se političko nasilje prikazuje kao legitimno sredstvo za ostvarivanje političkih ciljeva, pred kojima popuštaju mehanizmi kontrole i samokontrole ekstremista; umrežavanja terorizma i drugih vidova kriminala, od kojih je svakako najopasnija sprega sa organizovanim kriminalom i sa kriminalnim (subverzivnim) aktivnostima obaveštajnih službi neprijateljski nastrojenih država. Ukoliko ih nisu „oteli“, teroristi nerijetko

[8] Aleksić Ž. i Škulić M., *isto,* str. 424

sredstvima organizovanog kriminala za simbolična sredstva i kroz kriminalne postupke otkupljuju kuće, imanja, preduzeća i imovinu stanovništva protiv kojeg su usmerili terorističke akte; povećanja korupcije u javnom sektoru, koje je izraženije u tzv. neuspješnim i nestabilnim državama; ugrožavanja funkcionalnosti pojedinih državnih resora, jer terorizam ometa nesmetano realizovanje državnih funkcija, prije svega ekonomsku, socijalnu, zdravstvenu, obrazovnu itd.; stvaranja nepovjerenja građana u državu i državne organe, koji su često nemoćni i nedovoljno efikasni na polju antiterorizma; stvaranja nepovjerenja građana i države u međunarodne organe i institucije koje mogu da budu neefikasne u pružanju međunarodne pomoći, koje mogu da tolerišu terorističke aktivnosti pojedinih grupa i država koje ih sponzorišu i koje mogu da sankcionišu državu koja je neefikasna na polju antiterorizma; urušavanja međunarodnih odnosa i imidža (ugleda) zemlje na međunarodnoj sceni, naročito u slučajevima međunarodnog terorizma, zbog stavljanja drugih zemalja ili međunarodnih organizacija na stranu terorista ili zbog ne pružanja pomoći i podrške ugroženoj državi, uslijed osude države zbog neefikasnosti njenog sistema zaštite, odbrane, bezbjednosti i drugo. Svakako da, u najširem smislu, terorizam ima negativne efekte po sve sfere društvenog i međunarodnog života. Navedenom klasifikacijom posljedica terorizma nisu isključene druge tipologizacije. U zavisnosti od terorističkih strategija i posljedica terorizma, i država će zauzeti stav o „tvrđem“ ili „mekšem“ antiterorističkom djelovanju, te primijeniti pomirljivu strategiju (činjenje izvesnih ustupaka teroristima u zamjenu za odustajanje ili prekid terorističkih aktivnosti), pregovaračku strategiju koja prvenstveno prihvata neposredno ili posredovano pregovaranje sa teroristima, ali koja uvijek ne mora da rezultira ustupcima ili nepopustljivu strategiju koja podrazumijeva rješavanje problemske situacije odbijanjem zahtijeva terorista ili bez ikakvog pregovaranja.Takođe, samo po sebi se postavlja pitanje kakav se terorizam može očekivati u budućnosti? Realno je očekivati da će terorističke napade pretežno

izvoditi pojedinci ili male grupe naoružane prostim automatskim oružjem. Osim toga, realno je očekivati upotrebu malih bombi, konvencionalnih (vojnih) i iz „kućne radinosti“ (tzv. improvizovanih). Sljedeći, viši, nivo terorističkih opasnosti dolazi od profesionalno obučenih grupa opremljenih konvencionalnim naoružanjem srednje klase koje koriste „auto-bombe“ (putnički automobil ili kamion napunjen konvencionalnim eksplozivom), projektile zemlja-vazduh (tipa Stinger) i toplotno i infra - crveno navođene projektile za napad na civilne i vojne vazduhoplove, ručne bacače raketa i slično oružje. Najzad, treći nivo opasnosti dolazi od visoko obučenih grupa opremljenih oružjem za masovno uništavanje koje bi koristile nuklearno, hemijsko ili biološko oružje, prije „prljave bombe“ nego vojnoformacijsko oružje.[9] Razumne politike i dogovori na međunarodnoj sceni najbolja su preventiva za sve izazove, rizike i prijetnje po mir i bezbjednost u svijetu, pa tako i od opasnosti od terorizma...

[9] Harmon C. C., „Terrorism Today“, *Current Trend and Future Threats. Terrorism Today*, Frank Cass, London, 2000., pp. 137–185