Zbornik Instituta za kriminološka
i sociološka istraživanja
2016 / Vol. XXXV / 2 / 93-108
Pregledni naučni rad
UDK: 343.533::004

TERORIZAM U SAJBERPROSTORU

Marko Krstić*
Ministarstvo unutrašnjih poslova Republike Srbije,
Policijska uprava u Šapcu

Cilj rada je istraživanje sve većih opasnosti sajber-terorizma gde će se razmotrati njegov koncept i pokušati dati odgovor zašto teroristi sprovode ovaj vid aktivnosti. U radu će se prezentovati okruženja koja predstavljaju najveći rizik, profilne informacije o tome ko može predstavljati pretnju i opšte klasifikacije napada i opasnosti koje isti nose sa sobom. Čini se da se među glavnim motivacijama terorista razmatra njihova upotreba interneta za različite aspekte terorističke kampanje kao što su propaganda i zapošljavanje. To će razmotriti različite taktike koje koriste i prezentovati način na koji je internet pružio novu priliku za teroriste u njihovom provođenju kampanja i kako je adaptiran za njihove potrebe. Sajber-terorizam je nova teroristička taktika u ekspanziji i koja koristi informacione sisteme ili digitalne tehnologije, posebno internet, ili kao instrument delovanja ili kao mete, gde predstavljaju bojno polje za teroriste gde oni nastoje da ga iskoriste kao sredstvo za unapređenje njihove kampanje i napada. Kako se razvijena društva sve više oslanjaju na elektronske komunikacije, sistemi za kontrolu i trgovinu stvaraju potencijal za teroriste da pogode metu postaje sve realnija mogućnost. Internet danas postaje više način života i olakšava svojim korisnicima da postanu mete sajberterorista.

KLJUČNE REČI: terorizam / sajber-prostor / sajber-terorizam / sajber-teroristi / internet

* E-mail: marko.krstic.1982@gmail.com

UVOD

Ekspanzija tehnologije uslovljava sve veću upotrebu interneta od strane terorističkih organizacija i njihovih pristalica za različite svrhe, uključujući regrutovanje, finansiranje, propagandu, obuku, podsticanje na izvršenje terorističkih akata, kao i prikupljanje i širenje informacija za te svrhe. U virtuelnom svetu, sajber-teroristi koriste kompjuter kao alat za napad na drugi kompjuter gde ti napadi ne ostaju samo u virtuelnom svetu, već su usmereni i na živote ljudi i njihovu imovinu. Povećanje korisnika interneta i zavisnosti od istog, dramatično povećavaju bezbednosne rizike i iako su mnoge prednosti ovog globalnog medija evidentne, on se sa druge strane često koristi da se olakša komunikacija unutar terorističke organizacije. Zabrinutost zbog potencijalne opasnosti koju predstavlja sajber-terorizam je itekako osnovana, što ne znači međutim, da su svi strahovi koji se artikulišu u medijima, državnim institucijama i u drugim javnim forumima, racionalni i razumni.

Internet je inače izrazito globalni medij i ima potencijal da doprinese da sva društva zajedno osiguraju jednak pristup informacijama, ali u isto vreme predstavlja platformu akterima da unaprede svoje kriminalne ciljeve, kao i da se angažuju i organizuju terorističke akte. Danas je internet sve dostupniji i zastupljeniji i ima sve veći značaj u našim društvima, a teroristi logično prate ovaj trend i sve to maksimalno koriste. Kombinacija ovog novog medija i rastuće pretnje globalnog terorizma poziva na tradicionalne pravne odgovore države. Sajber-prostor, internet, intranet i ekstranet, postali su najvredniji i istovremeno najkritičniji resursi, a teroristi i sajber-kriminalci će maksimalno iskoristiti tehničke, pravne, političke i kulturne slabosti i širok spektar ranjivosti sistema. Pretnja sajberterorizma izaziva je okupirala naslove i pažnju političara, stručnjaka za bezbednost i javnosti, jer je terorizam fleksibilna pretnja i stalno će tražiti slabe tačke u državama ili organizacijama koje su mete napada. Veliki deo literature o sajber-terorizmu pretpostavlja da su ranjivost računarskih mreža i ranjivost kritične infrastrukture identični i da te slabosti izlažu nacionalnu bezbednost značajnom riziku.

Tokom proteklih nekoliko decenija, digitalna revolucija je podigla globalnu povezanost na potpuno novi nivo i samim tim su veliki izgledi da će sajber-prostor u budućnosti postati "poligon" za terorističke aktivnosti. Postaje jasno da se ciljevi terorista moraju prebaciti sa "bruto" nanošenja panike, smrti i razaranja, na ometanje vitalnih informacionih sistema preko sajber-napada koji će svakako imati prednost nad fizičkim napadima, inače karakterističnim za teroriste. Ideja sajber-terorizma postoji već duže vreme, ali postavlja se pitanje, u kojoj meri su terorističke grupe svesne štete koju mogu da nanesu koristeći informacije i komunikacione tehnologije? Da li sajber-terorizam predstavlja ozbiljan i realan rizik ili pak fantomsku i virtuelnu pretnju? Širina oblasti u kojima sajber-teroristi mogu izvršiti napad je u najmanju ruku zastrašujuća. Ovaj oblik terorizma je realna opasnost u eri brzog tehnološkog razvoja i više je nego očigledno da njegov model delovanja sa

vremenom postaje sve sofisticiraniji i nepredvidiviji. Potencijalne mete su sistemi koji kontrolišu odbranu države i kritične infrastrukture i "teroristi budućnosti" će voditi ratove bez direktnog kontakta i eksplozija bombi. Da bi se razumeo sajber-terorizam, važno je obratiti pažnju na njegovu pozadinu, kako bi se videlo kako terorističke organizacije ili pojedinci koriste prednosti i pogodnosti novih tehnologija i kakve mere vlada i međunarodnih organizacija preduzimaju da pomognu u borbi protiv njega. Sajber-terorizam je danas postao novo oružje za uništavanje ekonomske, političke i sociološke strukture i stoga je neophodno razmotriti različite namere, događaje, akte i domete kompjuterske tehnologije na kojima se temelji terorizam.

Kako su računari i mreže postale "žila kucavica" za svaku funkciju u državi i inostranstvu, u njima leži novi put za eksploataciju i zloupotrebu od strane sajber-terorista. Njihovi napadi na sigurnosne mreže i informacije predstavljaju kompleksne probleme koji su aktuelni u novim oblastima nacionalne bezbednosti i javne politike.

DEFINISANJE I SPECIFIČNOSTI SAJBERTERORIZMA

Sajber-terorizam predstavlja novu verziju terorističke aktivnosti i predstavlja krivično delo upotrebe savremenih tehnologija kroz nekonvencionalne napade na daljinu, izvan fizičkih i državnih granica, uz pomoć tzv. "sajberspace" (sajber-prostor). Korisnik interneta, pa samim tim i terorista, može lako sakriti svoj identitet i postati anoniman u ovom "prostoru" (Moslemzadeh, Manap, 2013) a za sajber-terorizam je još karakteristično da se ne zna tačno mesto gde se odvija napad koji ima naglašenu tendenciju da prelazi nacionalne granice nakon čega "iščezava" (Brenner, 2004).[1] Ovaj vid napada možda ne predstavlja direktnu pretnju po živote ljudi kao u slučaju tradicionalnog terorističkog napada[2], ali bi svakako mogao da uništi ili ozbiljno ošteti kompletan ekonomski i društveni sistem jedne zemlje. Upravo iz tog razloga se slobodno može reći da je sajber-terorizam definitivno realna opasnost koja će, nažalost, sve više uzimati maha u budućnosti (Cottim, 2010). Sajber-oružja postaju sve moćnija i jednostavnija za korišćenje sa grafičkim korisničkim interfejsima koji zahtevaju malo veština od strane korisnika (Denning, 2000). Zbog svoje dostupnosti, sajber-terorizam koristi asimetrična sredstva, protiv kojih još uvek ne postoje dovoljno efikasni i delotvorni instrumenti borbe (Kurmnik, Ribnikar, 2003).

[1] Konvencija o sajber-kriminalu je jedan od najvažnijih međunarodnih ugovora ovoga tipa i iako je ova konvencija kategorisana kao regionalna borba protiv sajber-terorizma, mnoge države su je ratifikovale i tako postale članice-potpisnice, jer su shvatile njen značaj. Međutim, najznačajniji sporazum o sajber-kriminalu ne obuhvata ovaj vid terorizma i stoga bi najbolje bilo da se on dopuni posebnim protokolom o sajber-terorizmu.

[2] Može se reći da je sajber-terorizam isti kao i "fizički", "konvencionalni" terorizam, osim što za napade koristi kompjutere (Brett, 2007) gde umesto da izvrše akte nasilja protiv lica ili fizičke imovine, sajber-teroristi vrše razaranja i "prekide" digitalne imovine (Denning, 2007).

Beri Kolin *(Berry Collin),* viši istraživač na Institutu za bezbednost i obaveštajne poslove u Kaliforniji, je kreirao termin sajber-terorizam još 1980. godine. Koncept se sastoji od dva elementa: "sajber-space" i terorizma. Prvi može biti zamišljen kao "ono mesto u kome kompjuterski programi funkcionišu i pokreću podatke" i ovi napadi moraju imati "terorističku komponentu" kako bi se kvalifikovali kao čin sajber-terorizma; moraju da uliju strah i poseduju političku motivaciju. Teroristi "koriste" računar kao potporu njihovim aktivnostima, bez obzira da li za propagandu, komunikaciju, ili u druge svrhe[3] (Conway, 2005).

Ovaj oblik terorizma se dalje definiše kao: "sa predumišljajem, politički motivisani napadi na informacije, računarske sisteme, programe i podatke koji rezultiraju nasiljem nad nevojnim ciljevima od strane grupa nižih nivoa". Sajber-terorizam omogućava teroristima da se više fokusiraju na napade kroz virtuelni rat bilo gde u svetu, po niskoj ceni, sa visokim nivoom anonimnosti i bez vremenskog ograničenja ili prostora (Siraj, 2009). Prema Filipu Brunstu *(Philiph Brunst),* postoje razmimoilaženja u formulisanju sajber-terorizma usled nedostatka tačne terminologije o ovom pojmu. Mark Polit *(Mark Pollit)* ga definiše kao "planske, politički motivisane napade na informacije, računarske sisteme, računarske programe i podatke koji imaju za rezultat nasilje nad civilima"(Cassim, 2012). Sajber-napad podrazumeva neovlašćene mrežne povrede i krađu intelektualne svojine i drugih podataka i često je finansijski motivisan (Theohary, Rollins, 2015). Džejms Luis *(James Luis)* iz Centra za strateške i međunarodne studije nudi jasnu definiciju ovog fenomena, uz napomenu da je sajber-terorizam "upotreba računarskih mrežnih alata prema kritičnim tačkama nacionalne infrastrukture u cilju prinude ili zastrašivanja vlasti i civilnog stanovništva" (Herzog, 2011).

Sajber-terorizam je još neprozirniji i zagonetniji termin od klasičnog terorizma, predstavljajući još jedan "sloj" u već ionako spornom konceptu. Sajber-događaji se, uopšte, često pogrešno prezentuju javnosti i pogrešno tumače u medijima. Ljudi imaju tendenciju da koriste termine *sajber*, *sajber-terorizam*, *sajber-kriminal*, i *hakerizam* naizmenično, iako postoje bitne, ponekad veoma osetljive razlike između ovih naizgled istih pojmova (Starr, 2012). Druga oblast sa etičkim dilemama uključuje nedržavne aktere čiji su sajber napadi politički ili društveno motivisani. Ovaj domen sukoba se često naziva "haktivizam", jer predstavlja sublimaciju hakovanja i aktivizma. Ako su napadi dizajnirani da budu dovoljno destruktivni i ako ozbiljno škode i terorišu društvo, mogu se kvalifikovati kao "sajberterorizam" ili "integracija sajber-napada sa terorizmom" (Denning, 2008). Radna definicija ovog fenomena se promenila tokom vremena i ovaj izazov nije isti za opšte studije terorizma, u kojima je već godinama, najčešća i najkarakterističnija taktika

[3] Podrška i izvor finansiranja terorista nije uvek samo u vidu novca, jer terorističke organizacije mogu da koriste internet kako bi u svoje aktivnosti uključile druga zamenljiva dobra (zlato ili dragulje, na primer) akumuliraju zalihe, ili regrutuju svoje vojnike (Hinnen, 2004).

bombardovanje. Drugo, ono što će biti uključeno u definicijama, ili čak u tipologiji, obično se bazira na osnovu ličnih perspektiva istraživača[4] (Keith, 2005).

Terorizam predstavlja presek nasilnog kriminala i političke aktivnosti, a njegova politička priroda je zapravo ono što ga diferencira od ostalih kriminalnih aktivnosti motivisanih finansijskom dobiti ili ličnim animozitetom. U principu, špijunaža i kriminalna aktivnost ne predstavljaju terorizam, ali ih ne treba ih smatrati ni delom sajber-terorizma (Nelson, *et.al*, 1999). Neophodno je definisati konkretno mesto gde se sajber-prostor i terorizam spajaju i iako se ovi napadi javljaju u sajber-prostoru, oni i dalje pokazuju neke zajedničke elemente sa svim aktima konvencionalnog terorizma: 1 sa predumišljajem preduzeto nasilje, 2. politički karakter, 3. usmerenost na civilne ciljeve, 4. nasilje sprovedeno od strane *ad-hoc* grupa (Hunt, 2004). Treba naglasiti da se termin sajber-terorizam odnosi samo na terorističke akcije preduzete od strane pojedinaca, grupa pojedinaca ili organizacija, jer u slučajevima u kojima država deluje na isti način, to bi se smatralo činom agresije ili uporebe sile prema međunarodnom pravu, što se najčešće kvalifikuje kao informatički rat (Gable, 2010).

Koreni ovog pojma mogu se pratiti unazad do ranih 1990-ih, kada je brz rast u upotrebi interneta i raspravama o nastajanju "informatičkog društva" pokrenuo nekoliko studija o potencijalnim rizicima sa kojima se suočavaju visoko umrežene, visoko tehnološki zavisne države. Već 1990. godine, *Nacionalna akademija nauka* u SAD počela je izveštaj o Kompjuterskoj bezbednosti sa rečima: "U opasnosti smo, jer cela Amerika zavisi od kompjutera; sutrašnji terorista može biti u stanju da učini više štete sa tastaturom nego sa bombom".[5] Prvo, iz psihološke perspektive, dva najveća straha savremenog doba se sublimiraju u izraz "sajber-terorizam": strah od slučajne, nasilne viktimizacije sa nepoverenjem i otvorenim strahom od kompjuterske tehnologije. Nepoznata pretnja se smatra više pretećom i opasnom od poznate pretnje i iako sajber-terorizam ne podrazumeva direktnu opasnost od nasilja, njegov psihološki uticaj na zabrinuta društva može biti moćan isto kao i posledica "terorističkih bombi". Neznanje je treći faktor, jer sajber-terorizam sintetizuje dve sfere: terorizam i tehnologije, tako da mnogi ljudi ne razumeju ovo u potpunosti i stoga imaju tendenciju da ga se plaše (Studies in Conflict & Terrorism, 2005).

[4] Sajber-terorizam ne predstavlja jedini način infrastrukturnog prekida. Nakon Prvog svetskog rata, evropski stratezi su identifikovali važne potencijalne napade na infrastrukturu, sposobne da "osakate" operativne sposobnosti neprijatelja. Te teorije su implementirane u praksu tokom Drugog svetskog rata od strane Kraljevskog ratnog vazduhoplovstva i vojske SAD tokom operacije usmerene na uništenje ratnih objekata, onemogućavanja transportnog sistema i prekida struje i imaju slične efekte kao sajber-terorizam (NATO).

[5] Iza izolovanih i upornih napada na zvanične veb lokacije, potencijalne mete za hipotetički sajberteroristički akt u SAD uključuju većinu kritične infrastrukture nacije: komunalne usluge, kao što su struja, voda i gas, objekti i njihovi sistemi za snabdevanje, finansijske usluge, kao što su banke, bankomati i trgovačke kuće; i informacioni i komunikacioni sistemi. Ova situacija oblikuje neku vrstu bojnog polja i može da deluje kao multiplikatorna sila za tradicionalne terorističke akte (Estevez-Tapiador, 2004).

Nakon 9/11, bezbednost i diskurs terorizma prezentuju vidljivu ekspanziju ovog oblika sajber-terorizma, s obzirom na štetu koju može da nanese.[6] Postoji nova politička dimenzija sa novim fokusom na ovaj vid terorizma a rasprave o nacionalnoj bezbednosti, uključujući i bezbednost sajber-prostora, uvek privlače političke aktere sa programima koji prevazilaze konkretne debate o sajber-terorizmu"[7] (US insstitute of peace contens). Pretpostavka ili cilj sajber-terorizma je da nacije i kritična infrastruktura postanu zavisni od računarskih mreža i njihovog rada, čime bi nova vrsta ranjivosti bila stvorena - "ogromna elektronska Ahilova peta". Samim tim, neprijateljski narod ili grupa bi mogli da iskoriste te slabosti da prodru u slabo sigurnu računarsku mrežu i ometaju ili čak onesposobe njene vitalne funkcije (Lewis, 2002).

OBRASCI DELOVANJA

Računarski napad se može definisati kao akcija usmerena protiv kompjuterskih sistema kako bi se prekinuo rad opreme, kontrole prerade, promene ili korumpiranje sačuvanih podataka. Sajber-terorizam može da se realizuje na više različitih nivoa[8] gde je najjednostavniji napad jedne osobe na drugu preko računara (Pope, 2014). Ali različite metode napada ciljaju različite ranjivosti i uključuju različite vrste oružja, od kojih neke mogu biti u okviru postojećih mogućnosti nekih terorističkih grupa[9] (Wilson, 2005). Sajber-terorizam predstavlja približavanje sajber-spejsa i terorizma i odnosi se na nezakonite napade i pretnje napada na računare, mreže, a podaci koji se nalaze u njemu, težeći da zastraše ili prisile vladu ili

[6] Dokazano je da su teroristi koristili internet u planiranju svojih operacija 9/11. Računari oduzeti u Avganistanu navodno su otkrili da je Al Kaida prikupljala obaveštajne podatke o ciljevima i slanju šifrovanih poruka preko interneta. Kao što je nedavno otkriveno, 16. septembra 2002. godine, Al Kaidine ćelije koje deluju u Americi navodno su koristili usluge telefonske veze zasnovane na Internetu da komuniciraju sa ćelijama u inostranstvu. Ovi incidenti ukazuju na to da se internet koristi kao *"ciberplaning"* sredstvo za teroriste, gde on pruža teroristima anonimnost, komandne i kontrolne resurse, kao i niz drugih mera da koordiniraju i integrišu opcije napada (Thomas, 2003).

[7] Postoji čitav "arsenal" reči kompjuterskog kriminala: *infowar, netwar, sajberterorizam, ciberharasment, virtuelni rat, digitalni terorizam, cybertatcits, kompjutersko ratovanje, napad "preko" i sajber-provala.* Oni se koriste da pokažu šta neki vojni i politički stratezi opisuju kao "novi terorizam" našeg vremena.

[8] Sajber prestupnici mogu koristiti automatizaciju da pojačaju svoje aktivnosti a jedan od primera ovakvog pristupa je *"Spam"*, gde prestupnici mogu poslati milijarde neželjenih masovnih "spamova" preko poruka u kratkom vremenskom periodu. Hakerski napadi su još jedan primer upotrebe automatizacije, gde je 80 miliona hakerskih napada svaki dan rezultat dostupnosti softverskih alata koji mogu da napadnu hiljade kompjuterskih sistema u razmaku od samo nekoliko sati (Gerke, 2010).

[9] Napad na računarsku mrežu *(CNA),* ili "napad preko" remeti integritet ili autentičnost podataka, obično kroz zlonamerni kod koji menja programsku logiku koja kontroliše podatke, što dovodi do grešaka u izlazima. Hakeri oportunistički pretražuju internet u potrazi za kompjuterskim sistemima koji su pogrešno podešeni ili gde nedostaju neophodni sigurnosni softveri. Jednom zaražen zlonamernim kodom, računar se može kontrolisati na daljinu od strane hakera koji mogu, putem interneta, slati poruku komandi da špijunira sadržaje tog računara ili napadima ometaju druge računare. Sajber-napad obično zahteva da ciljani računar ima neku unapred postojeću manu sistema, kao što su greške u softveru, nedostatak zaštite antivirusa ili pogrešnne konfiguracije sistema, koju zlonamerni kod zna da iskoristi.

svoje ljude u cilju političkih ili društvenih promena.[10] Dalje, da bi se napad kvalifikovao kao sajber-terorizam, trebalo bi da dovede do nasilja protiv lica ili imovine, ili bar da izazove dovoljno štete ili straha. Teroristi su se preselili u sajber-prostor da olakšaju tradicionalne oblike terorizma kao što je napr. bombardovanje. Oni oni koriste internet za komunikaciju, koordinaciju događaja i unapređenje njihovog programa i iako takva aktivnost ne predstavlja sajber-terorizam u užem smislu, pokazuje da teroristi imaju izvesnu nadležnost i primat koristeći nove informacione tehnologije (Denning, 2000).

Dening *(Denning)* tvrdi da ako su teroristi u stanju da se adekvatno obuče i steknu odgovarajuće tehnološke veštine, što bi bilo opasno za ceo svet. On dalje navodi: "Da bi se razumela potencijalna opasnost od sajber-terorizma, moraju se uzeti u obzir dva faktora: prvo, da li postoje ciljevi koji su ranjivi na napade koji mogu dovesti do nasilja ili teških povreda i drugo, da li postoje "glumci" i akteri sa sposobnošću i motivacijom da ih sprovedu[11] (Imran, 2014).

Propustljivost sajaber-prostora znatno olakšava terorizam u njemu i ovaj prostor se razlikuje u tom pogledu od fizičkih granica gde npr. imigracioni službenici kontrolišu ulazak stranaca i njihov ulazak u zemlju, dok carinici kontrolišu uvezenu robu kako bi se utvrdilo da nije krijumčarena. Sajber-prostor može da se koristi da pobedi ovaj sistem i izbegne kontrole i inspekcije i teroristi u različitim zemljama mogu da razmenjuju elektronsku poštu sa malo straha da će biti praćeni i uhvaćeni[12] (Brenner, Goodman, 2002). Iako mnogi tvrde da je sajber-terorizam samo još jedno "vozilo" za propagandu i smicalice vlade za kreiranje straha u javnosti, bilo je nekoliko slučajeva koji jasno pokazuju da je pretnja je veoma realna i sposobnost da se sprovede akt je zaista ostvariva[13]. Sajber-terorizam ima nekoliko različitih karakteristika i one pomažu da se bolje razumeju razlike na tankoj liniji između sajber-terorističkog napada u odnosu na sajber-napad ili aktivnosti hakera (Puran, 2003). Najmanje polovina svih računarskih incidenata nisu uzrokovani namerno, što podrazumeva ne samo nesreće već i nenamerne posledice ranjivosti. Ta ranjivost proizilazi iz zloupotrebljene konfiguracije mreža, softverskih grešaka, nepravilno ili loše tehničke ili administrativne primene informacione bezbednosne politike,

[10] Fizički napadi imaju za cilj fizičke strane Interneta, čvorova i komunikacionih medija, kroz fizička ofanzivna sredstva. Fizička oštećenja namerno, ili nenamerno, mogu imati isti efekat (Kostopoulos, 2008).

[11] Dejvid Kopeland *(David Copeland)* na primer, koristi internet materijal da napravi "nokat-bombu" sa namerom da dopre do različitih lokacija u Londonu. Iako je koristio sajber-tehnologije za pomoć u konstruisanju bombe, pitanje je da li bi on potpao pod definiciju teroriste u uobičajenom smislu te reči danas. Druga stvar je dakle, ako neko dobije instrukcije na internetu o tome kako napraviti bombu, i da li se on smatra sajber-teroristom? Uglavnom, argument je da računari treba da se direktno koriste za sajber-napad terorista.

[12] *Cyberspace* ima ne-teritorijalno utvrđene granice, jer su troškovi i brzina prenosa poruka na Internetu skoro potpuno nezavisni od fizičke lokacije: poruke se mogu preneti sa bilo koje fizičke lokacije na neku drugu, bez degradacije, propadanja, ili značajnim zakašnjenjem i bez ikakvih fizičkih znakova ili barijera koje bi inače držali određena geografska udaljena mesta i ljude odvojene jedni od drugih.

[13] Primer za sajber-terorizam su upadi u CIA ili FBI da se zastraši ili prisili američki narod. Drugi primer bi bio upad u bolničke baze podataka i promenu podataka o pacijentima na način koji bi izazvali da pacijenti umiru zbog lažnih doza lekova ili alergija na hranu. U 2003. godini, projektovani iznos je bio 6,5 milijardi $ poremećaja i štete u svetskim poslovima

neadekvatno obučeni računarski korisnici i ljudska greška (Bosch, Bailes, Fromvelt, 2004).

Dok su sajber-incidenti motivisani političkim i socijalnim razlozima, postavlja se pitanje da li su zaista dovoljno štetni ili zastrašujući da bi se okvalifikovali kao sajber-terorizam? Dok mnogi hakeri poseduju znanje, veštine i alate da napadnu kompjuterske sisteme, oni generalno nemaju motivaciju da dovedu do nasilja ili ozbiljne ekonomske ili socijalne štete[14] (Denning, 2000). Osim toga, uspešan sajber-teroristički događaj bi mogao da zahteva više preduslova nego znanja - sredstva koja su u suštini jednom stečena, dostupna su vlasniku i može ih koristiti iznova. Na taj način, bilo bi moguće da takav ambijent omogući stvaranje potpuno novih terorističkih grupa: nema novčanih sredstava neophodnih za realizovanje akcija, a članovi bi mogli da se organizuju dosta brzo i lako pobegnu u anonimnost sajberspejsa (Weimann, 2005).

Naravno, povećanje informacija, komunikacija i komunikacionih tehnologija ne utiču samo na terorističke grupe. Informacija predstavlja "novu krv" međunarodnog sistema i mnogo promena se desilo kao kao rezultat širenja informacione infrastrukture (Conway, 2005). Danas, zapadna društva zavise u skoro svakom aspektu života od računarske komunikacije; kompjuterski sistemi kontrolišu skoro sve što je potrebno za našu svakodnevnicu i naše planove za vanredne situacije. Sajber-terorizam[15] je sličan po svojim karakteristikama i sa drugim ranije pomenutim oblicima terorizma (Aviv-Cohen, 2010). Kao i "konvencionalni", nastojaće da promeni mišljenje ciljane publike, međutim, može da koristi različite načine delovanja u tu svrhu (Mliyanarachci, Wijesinghe, Jayarathine). Glavni motivi za teroristično nasilje uopšte su političke, ideološke ili verske prirode i ako sajber-terorizam zaista predstavlja približavanje terorizma i sajber-prostora, onda će se isti motivi primenjivati za njega, samo u drugom mediju. Mnogi od veb-lokacija postavljenih od strane terorističkih grupa se služe političkim ciljevima, ideologijom ili religijom i zaista, sajberp-rostor nudi određene prednosti nad fizičkom medijumu. Za početak omogućava sajber-teroristima pogodnosti za udaljene i anonimne operacije i takođe, izbegava potrebu za rukovanjem fizičkim oružjem i eksplozivom, kao i pratećim rizicima od spektakularne propasti propalog pokušaja kada bombe eksplodiraju prerano (Kheng, 2003).

Kao što je već objašnjeno, osim ofanzivnih operacija terorista, oni mogu efikasno da koriste sajber-prostor za bezbedne komunikacije. Al Kaidin *"Priručnik za obuku"* je samo jedan od mnogih dokaza o posvećenosti terorističkih organizacija za

[14] U novembru 2014. godine, izvršen je sajber napad na *Sony Pictures* od strane grupe hakera koji su identifikovani kao "*Our-mine"*. Prvobitno su objavljene poverljive informacije, kao što su imena zaposlenih , adrese i plate i izazvana je takođe fizičko oštećenje velikog broja računara. Ovo je usledilo mesec dana kasnije sa zahtevom da se poništi komedija pod nazivom "Intervju" i koje je *Sony* delimično ispunio (Wallace, 2016).

[15] Sajber-terorizam se može manifestovati i u ometanju podakata banaka, prodora u ZTP računare, blokiranje računara za komunikaciju na međunarodnom aerodromu i brisanju biračkih spiskova 24 sata pre izbora i još mnogo toga. Svi ovi sistemi su provajderi, što znači da su povezani na Internet na jedan ili drugi način, i stoga su pod rizikom od invazije.

bezbednom komunikacijom. Naime, među najvažnijim i najobimnijim lekcijama opisanim u ovom uputstvu su dve lekcije koje pružaju smernice o pravilnom korišćenju komunikacija i zaštiti podataka (Petreski, Bogdanoski, 2013).[16]

ŠIRENJE PROPAGANDE PUTEM INTERNETA

Sajber-prostor teroristima nudi mnogo potencijala i predstavlja alat za zapošljavanje, radikalizaciju, propagandu i prikupljanje sredstava, kao i pružanje brze i jednostavne komande i kontrole[17]. S obzirom na jednostavnost upotrebe i sve veće oslanjanje na razvijena društva na internetu, mogućnost za terorističku eksploataciju se svakodnevno širi (Brantly, 2014).[18] Čak i pre ekspanzije interneta, Aleks Šmit i De Graf *(Alex Schmid & Janni De Graaf, 1982)* su zapazili da je "komunikaciona revolucija 20. veka značajno promenila lice terorizma" (Terrorism & the Media, 2008). Posle događaja od 9/11 i antiterorističke kampanje koja je usledila, veliki broj terorističkih grupa se preselio u sajber-prostor[19], kreirajući hiljade sajtova preko kojih promovišu svoje poruke i aktivnosti. Socijalni mediji se razlikuju od tradicionalnih i konvencionalnih u mnogim aspektima, kao što su interaktivnost, dostizanje zadovoljavajuće frekvencije, upotrebljivost, neposrednost. Nove komunikacione tehnologije, kao što su relativno jeftine i dostupne mobilne i veb-mreže, stvaraju visoko interaktivne platforme kroz koje bi pojedinci planirali akcije, diskutovali i menjali njihov sadržaj (Weimann, 1983). Internet nudi moćan, jeftin i prodoran alat za komunikaciju i koordinaciju akcija, sa oko 300 miliona ljudi na mreži samo od 2000. godine. Grupe bilo koje veličine, mogu dostići jedni druge i koristiti internet da promovišu svoj program. Njihovi članovi i pratioci mogu doći iz bilo kog geografskog područja na Internetu, a mogu pokušati da utiču na spoljnu politiku bilo gde u svetu (Denning, 2007).

---

[16] Čak i pre 9/11, kompjuterska bezbednost je postala naročito ozbiljan problem za firme u SAD. *Computerworld* je objavio izveštaj sa detaljima iz oktobra 2000. godine i računarskih napad na *Microsoft corporation*, u kojima su se hakeri prerušili kao *offshore* radnici preduzeća kako bi dobili pristup internoj mreži *Microsoft-a*. Centar za strateške i međunarodne studije je kasnije zaključio da ako *Microsoft* može biti meta, nijedna kompanija nije sigurna. Računarski crv, na primer, je izazvao više od 11 milijardi $ gubitaka u 2000. godini (Raghavan, 2003).

[17] Islamski teroristi su naročito aktivni na Internetu. U oktobru 2003. godine, na internet *Haganah-u*, projektu posvećenom borbi protiv terorizma, navedeno je 65 aktivnih sajtova sa pripadnosti islamskim terorističkih organizacija. Među njima su Al-Aksa Martirs brigada (10 websites), Al-Kida (24), Hamas (19), Hezbolah (5), Hizb-ut-Tahrir (4), a palestinski Islamski džihad (2). Projekat je tvrdio da su teroristi dobili oko 300 dodatnih sajtova podrške (Denning, 2010).

[18] Iako su neki sajtovi povezani sa terorističkim organizacijama počeli da prikupljaju *Bitcoin* donacije, izgleda da je ova praksa relativno ograničena. Moguće je da se sa povećanjem tehničkih kapaciteta ovih organizacija, njihovo korišćenje digitalnih valuta takođe intenzivira. Ovo povećanje će verovatno biti malo, u odnosu na ukupno finansiranje terorizma preko drugih kanala kao što su, kidnapovanje, pretnja kompanijama, prodaja narkotika, nafte, i još mnogo toga.

[19] Zvanični sajtovi nekih stranih terorističkih organizacija mogu predstavljati terorističke lokacije, kao i lokacije njihovih pristalica i simpatizera. Ali kada sajtovi bez formalne terorističke pripadnosti sadrže naklonjena osećanja prema političkim ciljevima terorističke grupe, definicija postaje "zatamnjena". U poslednjih nekoliko godina veliki broj ljudi sa simpatijama gleda na talibanske sajtove koje su razvili na internetu, međutim, čestim prekidima istih, teško je pratiti njihov sadržaj i osećanja (Kaplan, 2009).

Jedan od glavnih ciljeva upotrebe interneta od strane terorista je širenje propagande koja obično ima oblik multimedijalne komunikacije i pruža ideološku ili praktičnu nastavu, objašnjenja, opravdanja ili promociju terorističkih aktivnosti. One mogu da sadrže virtuelne poruke, prezentacije, časopise, rasprave, audio i video fajlove i video igre razvijene od strane terorističkih organizacija ili njihovih simpatizera[20]. Dalje, širenje propagande generalno nije, samo po sebi, zabranjena aktivnost, ipak, ono što čini ovaj vid propagande, za razliku od legitimnog zastupanja sa tačke gledišta, često je subjektivna procena. Promocija nasilja je zajednička tema u propagandi terorizma i širok domet sadržaja distribuiran preko interneta eksponencijalno povećava publiku koja na koju može da se utiče.[21] (In collaboration with the United Nations Counter, 2012). Teroristi moraju imati u svojim rukama medij da bi objasnili svoju poruku i "opravdali" svoje postupke, jer pre pojave interneta, relativno je bilo teško privući masovnu publiku (Charvat, 2014).

Pored klasičnih pretnji terorizma, uticaj savremenih medija je pokrenulo tzv propagandni rat, kome terorističke organizacije pridaju veliki značaj. Ovaj rat može biti veoma moćno psihološko oružje i može značajno povećati efekat određenih radnji. Teroristi, s jedne strane, praktikuju medijsku propagandu kako bi pokazali "apsolutno prostranstvo svojih ciljeva"[22], ali u isto vreme oni su svesni koliko im šteti negativan publicitet u njihovoj realizaciji. Značenje terorističke propagande, tj četiri glavna cilja u korišćenju masovnih medija su: 1. da prenesu propagandna dela i da se usadi ekstremni strah ciljnoj grupi; 2. mobilisati širu podršku za "svoju stvar" u opštoj populaciji i međunarodno mišljenje sa akcentom na teme kao što su pravednost svog cilja i neminovnosti pobede; 3. osujetiti i poremetiti odgovor vlade i bezbednosnih snaga; 4. mobilisati, podstaći i povećati svoje birače, stvarne i potencijalne pristalice i na taj način da se povećati zapošljavanje, podizanje više novca i samim tim inspirisati nove napade (Wilkinson, 2002).

Pitanje koje se postavlja je, ko zapravo predstavlja pravu publiku i sledbenike terorista na internetu? Da li je to vlada koja će potrošiti svoj novac i energiju i goniti ih kada utvrdi potencijalne tragove ili je to onaj širok auditorijum koji će slediti teroriste i zastupa njihovu ideologiju (Commitee on homeland security, 2011). Terorizam je tesno povezan sa konceptom propagandne i pojedinci koji se njime se u javnoj sferi su žigosani kao teroristi: semantičari ističu da način na koji mi vidimo jednu osobu umnogome zavisi od naših potreba, projekcija i procena ali sud o njoj se

[20] Pojedine terorističke grupe koriste visoke frekvencije šifrovanog glasa, tj. održavanje veza sa državnim sponzorima terorizma. Teroristička organizacija Hamas navodno koristi šifrovane internet komunikacije za slanje mapa, slika i ostale detalje u vezi sa terorističkim napadima (Denning, 1999).

[21] Znanje i veštine o pravljenju bombi je dostupno na džihadističkim sajtovima u formi veoma detaljnih procedura u video uputstvima koja pokazuju kako se prave improvizovani eksplozivni uređaji. Postoje čvrsti dokazi da su takve *online* kontrukcije odigrale ključnu ulogu u bombaškim napadima na Madrid 2004. i Kairo 2005. godine, London i Zapadni Glazgov, kao i neuspeli pokušaj napada u Nemačkoj (Cohen-Almagor, 2012).

[22] Tajne metode uključuju donošenje šifrovanim porukama, ugrađivanje nevidljive grafičke kodove pomoću steganografija, koristeći internet za slanje pretnje smrću, i angažovanje hakere da prikuplja obaveštajne podatke kao što su imena i adrese službenika za sprovođenje zakona iz onlajn baza podataka (Cronin, 2003).

posle ne menja kada se promeni okvir posmatranja (Lipschultsh, 2007). Ukratko, propaganda je dizajnirana za manipulaciju "verovanja" i izaziva akciju u interesu propagatora "ubrizgavanjem" poruka u glave slušalaca. To uključuje korišćenje slika, slogana i simbola u igri predrasuda i emocija, a njen krajnji cilj je da se zavede primaoc poruke kako bi došao na "dobrovoljno" prihvatanje pozicije propagandista kao da je njihov lični. Često se pod propagandom smatraju lažne informacije koje treba da uvere one koji već veruju i u svojoj modernoj upotrebi (Brahms, 2008).

Usled procesa globalizacije, naročito u oblasti tehnologije, terorističke grupe teže da kontrolišu medijske tehnologije da rade u njihovom najboljem interesu. Povećanje Internet usluga i pristupa efikasnijim i jeftinijim računarima, softverima i bežičnim tehnologijama, teroristima se pruža mogućnost da reklamiraju i propagiraju svoje ciljeve putem interneta (Lumbaca & Gray, 2011). Danas smo svedoci sve veće i sve sofisticiranijeg terorističkog prisustva na internetu i to predstavlja veoma dinamičan fenomen: iznenada se pojavi, često menja svoje formate, a zatim brzo nestaje ili što je još češći slučaj, prividno nestaje menjajući svoju internet adresu, ali zadržavajući gotovo isti sadržaj. Kako bi se identifikovali teroristički sajtovi, sprovedena su brojna sistematska skeniranja interneta, hraneći ogroman broj imena i termina u pretraživanjima i ulazeći u forume pristalica i simpatizera geodetskih linkova i drugih organizacija[23]. Ovo je veoma naporan trud, pogotovo zbog toga što u nekim slučajevima (npr. *Al Qaide website*) lokacije i sadržaj se menjaju gotovo svakodnevno (Gabriel, 2014).

ZAKLJUČAK

Mnoge međunarodne terorističke grupe sada aktivno koriste računare i internet u cilju komuniciranja gde mogu razviti i steći neophodne tehničke veštine da režiraju koordiniran napad računara u jednoj državi. Napadi ovog vida terorizma na poslovne i državne organe ne poznaje granice i teroristi značajno mogu naneti štetu ekonomiji jedne države. Sajber-terorizam je pretnja koja je u ekspanziji, a dokazi pokazuju da će biti sve intenzivnija i opasnija. Snalažljivost terorista i njihova prilagodljivost stalno menjaju društvo i tehnologije i to je oblik ratovanja koji treba da bude priznat, ponovo procenjen, i zahteva adekvatan odgovor. Informatičko ratovanje je bojno polje budućnosti i mora se ozbiljno uzeti u obzir. Pokazatelji govore da će upotreba novih tehnologija nastaviti i proširiti, sa rastućim uticajem na sprovođenje zakona.

Ne postoje još jasni kriterijumi za utvrđivanje da li je sajber-napad zapravo napad kriminalaca, hakera, terorista ili nacionalne države koji je ekvivalent oružanog napada. Isto tako, još nema međunarodnih, pravno obavezujućih instrumenata koji

[23] Izveštaj počinje nacrtom porekla Interneta, karakteristikama novog medija, koje su tako privlačne i atraktivne za političke ekstremiste, opseg aktivnih terorističkih organizcacija u sajber-prostoru kao i njihovim ciljnim grupama. Srce izveštaja je analiza osam različitih namena interneta u svrhe terorizma koji variraju od korišćenja psihološkog oružja za prikupljanje informacija, obuke i prikupljanju sredstava, pa sve do propagande i regrutovanja, mreža za planiranje i koordinaciju terorističkih akata.

eksplicitno regulišu međudržavne odnose u sajber-prostoru. Na žalost, sajber-terorizam ostaje održiva opcija za bilo kog pojedinca ili grupe koje žele da ga koriste da unaprede svoje ciljeve. Povećana komunikacija, umrežavanje i oslanjanje na digitalnu infrastrukturu u informatičkom dobu osnažuje transnacionalne pokrete otpora i stvaraju nove slabosti za nacionalne države. Sajber-terorizam i sajber-kriminal predstavljaju nove izazove za organe bezbednosti i kreatore politike i zbog svog transnacionalnog karaktera, adekvatan odgovor na takvu pretnju iziskuje međunarodnu saradnju. Međutim, ranjivost proizlazi iz povećanog oslanjanja na tehnologiju, nedostatak zakonskih mera i saradnje na nacionalnom i međunarodnom nivou, što predstavlja realnu prepreku za efikasan odgovor na ovu pretnju. Sve u svemu, nedostatak globalnog konsenzusa u pogledu odgovora na sajber-terorizam i kompjuterski kriminal je opšti, globalni, problem.

Barem u bliskoj budućnosti, bombe će i dalje predstavljati mnogo veću pretnju nego bajtovi, međutim, nikako ne treba zanemariti potencijal i rastuću opasnost sajber-terora. Tokom proteklih nekoliko godina, teroristi i džihadisti su pokazali snažnije interese i sposobnosti za obavljanje sajber –napada i sa velikim uspehom su sprovodili brojne aktivnosti na raznim sajtovima. Neophodno je sumirati nekoliko ideja koje su od suštinskog značaja za unapređenje međunarodne saradnje u borbi protiv sajber-terorizma. Pre svega, prevencija mora biti znatno poboljšana i imajući ovo u vidu, moraju se prevazići dve prepreke efikasnog odgovora na terorizam: teritorijalne granice i tehnička kompleksnost. Ovo drugo bi se moglo rešiti putem obimne obuke aktera uključenih u borbu protiv sajber-terorizma. Dalja istraživanja treba da se razvijaju u onoj meri u kojoj će potencijalni terorista izabrati pre sajber-prostor, nego npr. eksploziv kako bi postigao veliki uspeh i spektakularni uticaj u vezi sa svojim napadima.

Da bi se odgovorilo na istinska pitanja u vezi sa prirodom sajber-terorizma neophodan je jedan radikalan pristup problemu. Strateški uticaj na pitanja sajber-bezbednosti novih tehnologija i njihovo globalno širenje, zahteva dalju i temeljniju analizu. Opasnost ovog vida terorizma, koji je rezultat transformacije terorizma i koji se odvija u virtuelnom svetu i izaziva političke ili ekonomske posledice, ni na koji način treba potceniti. Međunarodna zajednica ima retku i jedinstvenu priliku da putem preventivnog pristupa stvori jedan pravni okvir koji će osigurati međunarodnoj zajednici da se pripremi za "dan posle" napada sajber-terorizma. Veoma je važno da države imaju zajedničku pravnu definiciju termina sajber-terorizma a pravno definisanje ovog pojma na bazi njegovih jedinstvenih karakteristika ne bi samo olakšalo borbu protiv njega već bi i unapredilo saradnju među državama.

LITERATURA

(1) Bogdanski, M, & Petreski, D. (2013) Cyber terrorism – Global secyrity threat International scientific deffence*, Security and peace journal*, pp. 59-71
(2) Bosh, O, Bailes A, & Fromellet I. (2004) (eds.) Defending Against Cyber Terrorism: Preserving the Legitimate Economy Business and Security: Public–Private Sector Relationships in a New Security Environment. SIPRI and Oxford University Press,

2004. 187-196. Juan M. Estevez-Tapiador, The Emergence of Cyber-Terrorism Iee distributed systems online, 1541-4922 Computer Society Vol. 5, No. 10
(3) Brahm, E. (2008) "Propaganda", Beyond Intractability, available from: http://www.beyond intractability.org/essay/propaganda/?nid=6791 22/09/2008
(4) Brantly, A.(2014) "Financing terror bit by bit", CTC Sentinel, Vol 7(10) , pp. 1-5.
(5) Brenner, S, & Goodman, S. (2002) Cyberterrorism: An argument for anticipating cyber ć attacks *Journal of law, technology & policy*, Vol. 2002, No. 1
(6) Brett, P. (2007) Cyber Terrorism and Information Security East Carolina University Retrieved October 14, 2007, from United States Institute of Peace: Available from:http://www.usip.org/pubs/specialreports/sr116.html
(7) Cassim, F. (2012) Addressing the spectre of cyber terrorism: a comparative perspective, *Potchefstroom Electronic Law Journal,* Vol. 15 No 2
(8) Charvat, P. (2014) "Terrorism: A New Dimension in Battlespace" Major J SO2 Course Director Centre of Excellence Defence Against Terrorism
(9) Cohen, A. (2010) "Cyberterrorism: Are We Legally Ready?", *Journal of International Business and Law*: Vol. 9: Iss. 1.
(10) Cohen-Almagor, R. (2012) "In Internet's Way Radical, Terrorist Islamists on the Free Highway". International Journal of Cyber Warfare and Terrorism, 2(3), pp. 39-58.
(11) Conway, M. (2005) The media and cyberterrorism: a study in the construction of reality, Scotland 1-53 Paper presented at the First International Conference on the Information Revolution and the Changing Face of International Relations and Security Lucerne, Switzerland 23-25
(12) Cottim, A. (2010) "Cybercrime, cyber terrorism and jurisdiction: an analysis of article 22 of the COE convention on cybercrime", *European Journal of Legal Studies*, Vol 2, No.3.
(13) Cronnin, A., K. (2003) Globalization and International Terrorism Behind the curve *International Security*,Vol. 27, No. 3 (Winter 2002/03), pp. 30–58
(14) Cyber terrorism and australias terrorism insurance (2016), Sheme psysically destructive cyber terrorism is a gap in current insurance coverage arpc, Australian government; Australian Reinsurance Pool corporation.
(15) Denning, D. E. (2000) "Cyberterrorism," Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.
(16) Denning, D. E. (2001) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy (Rand 2001) (John Arquilla & David Ronfeldt Eds.)
(17) Denning, D. E. (2010) "Terror's Web: How the Internet is Transforming Terrorism," in *Handbook on Internet Crime,* (Y. Jewkes & M. Yar, Eds.), Willan Publishing.
(18) Denning, D. E. (2007) View of Cyberterrorism Five Years Later Center on Terrorism and Irregular Warfare Naval Postgraduate School [Chapter 7 in Internet Security: Hacking, Counterhacking, and Society (K. Himma Ed.), Jones and Bartlett Publishers.
(19) Denning, D. E. (2000) Reflections on Cyberweapons Controls *Georgetown University Computer Security Journal,* Vol. XVI, No. 4, pp. 43-53.
(20) Denning, D. E. (2008), "The Ethics of Cyber Conflict," in *Information and Computer Ethics* (K. E. Himma & H. T. Tavani, Eds.), Wiley.
(21) Denning, D. E, & Baugh, W. (1999) Hiding Crimes in Cyberspace. *To appear in Information, Communication and Society,* Vol. 2, No 3, and in *Cybercrime*, B. D. Loader & D. Thomas (Eds.), Routledge, 1999.
(22) Gable, K. (2010) Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt journal of transnational law*, Vol. 43:57, pp 57—117.
(23) Gercke, M. (2010) "Challenges in developing a legal response to terrorist use of the Internet" in *Defence Against Terrorism Review*, Vol. 3, No 2,

(24) Gordon, S. (2003) "Research Fellow Symantec Security Response and Richard Ford, Ph.D. Independent Consultant Symantec Security Response Cyberterrorism? Research Fellow Symantec Security Response and Richard For, Ph.D. Independent Consultant Symantec Cyberterrorism? 1521-0731, DOI: 10.1080/10576100590905110
(25) Gregory, T, & Kheng, L. (2003) *Cyberterrorism with cyber deception*, Naval postgraduate school Monterey, California,
(26) Herzog, S. (2011) "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* Vol. 4, no. 2: pp 49-60. DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3
(27) Hinnen, T. (2004) "The cyber-front in the war on terrorism: curbing terrorist use of the Internet", *The Columbia Science and Technology Law Review*.
(28) Hunt, L. (2004) Journal of Information Technology Education Volume 3, 2004 Editor: Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks Janet J. Prichard and Laurie E. MacDonald Bryant University, Smithfield, RI, USA
(29) Imran, A. (2014) Debating the term cyberterrorism:Issues and problems, *Internet Journal of Criminology*. ISSN 2045 6743 (Online).
(30) In collaboration with the United Nations (2012) Counter-Terrorism Implementation Task ForceThe use of the Internet for terrorist purposes United Nations New York.
(31) Jihadist use of social media (2011) How to prevent terrorism and preserve innovation hearing before he subcommittee on ocunterterrorism and intelligence of the committee on homeland security house of representatives one hundred twelfth congress first session december 6., 2011, No. 112–62.
(32) Kaplan, E. (2009) "Terrorists and the Internet", Council, on foreighn, relations. Available from: http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005
(33) Keith, S. (2005) Fear-mongering or fact: The construction of 'cyber-terrorism' in U.S., U.K, and Canadian news media A paper presented at Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities sponsored by the Oxford Internet Institute Oxford, England, Ph.D
(34) Kostopulos, G. (2008). Cyberterrorism: The Next Arena of Confrontation communications of the IBIMA, Communications of the IBIMA Volume 6, pp. 165-169.
(35) Kurmnik, B, & Ribnikar, D. (2003) *Asimetrični ratovi*, Beograd: Evro Đunti.
(36) Lewis, J. (2002) Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: Center for Strategic and International Studies CSSIS
(37) Lipshults, J. (2007) "Framing Terror: Violence, Social Conflict and the "War on Terror" Electronic News 1: 21-35.
(38) Lumbaca, S, & Gray, D. (2011) "The Media as an Enabler for Acts of Terrorism", Global Security Studies, Volume 2, Issue 1, pp 45-54.
(39) Moslemzadeh, T. P, & Manap, N.A. (2013) Cyber terrorism challenges, Bhangi, pp. 207-213
(40) NATO: Threat of Cyberterrorism, Prague student summit XVIII , Model NATO/ III, backround reports
(41) Nelson, B., Choi, R., Labbouchi, R., Michel, M., & Gagnon, G. (1999) *Cyberterror: Prospects and Implications*, Center for the Study of Terrorism and Irregular Warfare, Monterey, CA.
(42) Pope, L. (2014) Cyberterrorism and China, United Master of military studies title: Submitted in partial fulfillment of the reyuirements for the degree of master of military studies, *Internet Journal of Criminology,* ISSN 2045-6743
(43) Raghavan, T. (2000) Cyberwarfare and Cyberterrorism: In Brief 2000, *In fear of cyberterrorism: An analysis of the congressional response*.

(44) Rajeev, P. (2003) 5 SANS Institute InfoSec Reading Room This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission. Beyond Conventional Terrorism. The Cyber Assault Copyright SANS Institute Author Retains Full Rights SANS GIAC Security Essentials Certification (GSEC) v1.4b.
(45) Siraj, A. (2009) Cyberterrorism: The Threat of Virtual Warfare, *The Journal of Defense Software Engineering*,pp 16-18.
(46) Starrs, S. (2012) Fight for the Spoils: The Future Role of Syria's Armed Groups. *CTC Sentinel,* Vol. 5, Issue 8.
(47) Terrorism and the Media (2008), July 23, 2008 Deliverable 6, Workpackage 4
(48) Theohary, C, & Rollins, J. (2015) Cyberwarfare and Cyberterrorism:in Brief Congressional Research Service 7-5700. Available from: www.crs.gov
(49) Thomas, T. (2003) "*Al Qaeda and the Internet: the danger of cyber-planning*", Parameters: U.S. armyWar College Quarterly. 33(1), 112-123
(50) United states institute of peace contents (2004) Introduction 2 Cyberterrorism Angst What Is Cyberterrorism?
(51) Mliyanarachchi, F, Wijesinghe, WS, & Jayarathne, H. Cyberterrorism is Sri Lanka ready? Cyber Terrorism Discussion Paper, Defence university syndictate 10 intake 28 Syber terrorism, is Sri lanka ready, General Sir John Kotewala defence university syndicate 10, Intake 28.
(52) Weimann, G. (2014) Special report: New Terrorism and New Media, Wilson centar, *Commons law*. Vol.2.
(53) Weimann, G. (1983) "The Theater of Terror: The Effects of Press Coverage", *Journal of Communication*.Vol. 33, pp. 38 45,
(54) Weimann, G. (2005) "Cyberterrorism: The Sum of All Fears? United States Institute of PeaceWashington, DC, USA and Department of Communication University of Haifa Haifa. Israel Studies in Conflict & Terrorism, 1521-0731 onlineDOI: 10.1080/10576100590905110
(55) Wilkinson, P. (2002) "Terrorism versus Liberal Democracy: The Problems of Response", in Paul Wilkinson, Terrorism v. Liberal Democracy – *The Problems of Response Centre for Security and Conflict Studies*, No. 67, pp. 1-19.
(56) Wilson, G. (2005) Computer Attack and Cuberterrorism:Vulnerabilities and Policy Issues for Congress Updated April 1, Congressional Research Service The Library of Congress

TERRORISM IN SYBERSPACE

This paper presents the research growing threat of cyber-terrorism, where to be addressed by his concept and try to answer why terrorists carried out this type of activity. It seems that among the main motivations of terrorists consider their use of the Internet for different aspects of the terrorist campaign as propaganda and recruiting. It will consider different tactics they use and present the way in which the Internet has provided a new opportunity for terrorists in their implementation of the campaign and how it was adapted to their needs. Cyber-terrorism is a new terrorist tactic in the expansion and using information systems or digital technology, especially the internet, or as an instrument of action or target, where they are a battleground for terrorists where they are trying to use it as a means to improve their campaigns and attacks. It examines the potential threat of cyber-attacks by the terrorist organizations and the ways in which they can use the internet and cyber-space to attack and thereby achieve goals similar to conventional physical attacks. As the developed societies increasingly rely on electronic communications, control systems and trade creates the potential for terrorists to hit their target becomes increasingly realistic possibility. Internet has become more a way of life and making it easier for users to become targets cyberterorism.

KEYWORDS: terrorism / cyber-space / cyberterrorism / cyber-terrorists / internet