UDK: 343.326:004.738.5
323.28::28
Biblid 0543-3657, 67 (2016)
God. LXVII, br. 1162-1163, str. 46–61
Izvorni naučni rad
Primljen: 28.1.2016.

Katarina JONEV[1]

Aktivnosti Islamske države u sajber prostoru

SAŽETAK

Terorizam je početkom XXI veka postao glavna bezbedonosna pretnja savremenog sveta. Dok se međunarodna zajednica suočava s nizom pretnji i izazova, terorističke grupe nastavljaju da šire strah unapređujući svoj metod delovanja. Sajber terorizam je jedan od oblika terorizma i metod koji teroristi mogu potencijalno da koriste u svojoj borbi. Reč je o nelegalnom aktu u kom se kao oružje primenjuju kompjuter i Internet u cilju ugrožavanja ljudskih života i nacionalne infrastrukture. Napadi na računarske sisteme i mreže koji mogu izazvati prekid u radu, gubitak života ili povredu ljudi, fizičko uništenje, finansijske i ekološke posledice, su akti sajber terorizma. Teroristi Islamske države su paralaleno sa fizičkim, osvajali i sajber prostor pre svega širokom upotrebom društvenih mreža za potrebe propagande. Ovaj rad predstavlja pokušaj autora da predstavi razliku između akta sajber terorizma i aktivnosti terorista na internetu kao što je širenje propagandi, kao i da pruži analizu aktivnosti pripadnika Islamske države u sajber prostoru.

Ključne reči: terorizam, sajber terorizam, Islamska država, sajber napadi, propaganda, digitalni džihadizam, sajber teroristi

Uvod

Terorizam predstavlja metod smišljene i sistematske upotrebe nasilja. Cilj je razvijanje straha kod predstavnika vlasti i građana radi ostvarivanja ličnih, političkih, ideoloških ciljeva. Terorizam je jedan od oblika nasilja koji u savremenom svetu ugrožava kako nacionalnu tako i međunarodnu bezbednost. Osnovni elementi koji čine akt terorizma „kao društvene pojave, više-

[1] Diplomirani politikolog za međunarodne odnose, Master Međunarodnog prava, e-mail: jonev.katarina@gmail.com.

dimenzionalnog fenomena po svom značenju, značaju i strukturi"[2] jesu širenje straha i nesigurnosti. To je „složeni oblik organizovanja grupnog, i ređe individualnog ili institucionalnog, političkog nasilja obeležen ne samo zastrašujućim brahijalno fizičkim i psihološkim, već i sofisticirano-tehnološkim metodama političke borbe kojima se obično u vreme političkih i ekonomskih kriza, a retko i u uslovima ostvarene ekonomske i političke stabilnosti jednog društva, sistematski pokušavaju ostvariti "veliki ciljevi" na morbidno spektakularan način, a neprimereno datim uslovima, pre svega društvenoj situaciji i istorijskim mogućnostima onih koji ga kao političku strategiju upražnjavaju."[3] Terorizam je usmeren protiv institucija nekog društva ili države.[4]

Terorizam se kao pretnja nalazi u samom vrhu bezbedonosnih agendi država širom sveta. Vremenom, metode i strategije koje teroristi koriste su napredovale. Terorizam je kao aktivnost evoluirao. Paralelno, raste strah i od sajber terorizma[5] kao jednog od oblika terorizma. Sajber terorizam može biti tumačen i kao "razvojna faza tradicionalnog terorizma."[6] Zloupotreba modernih tehnologija i interneta u terorističke svrhe nije novijeg datuma ali se postavlja pitanje da li je sajber terorizam u današnje vreme realna opasnost po državu i njene građane. Sajber terorizam predstavlja opasnost po međunarodnu zajednicu podjednako kao i svaki drugi oblik terorizma.[7]

Treba uzeti u obzir da se do danas nije desio akt sajber terorizma i da su i praksa i teorija izuzetno podeljene kada je reč o tumačenju sajber terorističkog akta. Na globalnom nivou akademska i bezbedonosna zajednica još uvek nije došla do unificirane definicije niti precizno definisanih akata koje karakterišu sajber terorizam.

Sajber terorizam predstavlja nelegalni akt i pretnju po kompjuterske sisteme, mreže i informacije. Kao i svaki oblik terorizma, ima političku, ideološku, versku, socijalnu dimenziju. Cilj je izazavati paniku i strah državnih organa i građana. Dovoljno obučeni sajber teroristi su u stanju da napadnu infrastrukturu država poremećajem protoka informacija.[8] Centar

---

[2] Dragan Simeunović, "*Terorizam*", Pravni fakultet Univerziteta u Beogradu, Beograd 2009, str. 67.

[3] Ibid., str. 80.

[4] Ibid., str. 80.

[5] United Nations Counter-Terrorism Implementation Task Force (UN CTITF), *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*, 2009, p. 3, http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf

[6] Roland Heickerö, "*Cyber Terrorism: Electronic Jihad*", Strategic Analysis, 2014 Vol. 38, No. 4, pp. 554-565.

[7] Ambassador Gábor IKLÓDY, "*The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities Defence Against Terrorism*", Review Vol.3, No. 2, Fall 2010, p. 5.

[8] Murat Dogrul, Adil Aslan, Eyyup Celik, "*Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*", 2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011, © CCD COE Publications, p. 30.

za Strategijske i međunarodne studije u izveštaju iz 1998. godine sajber terorizam predstavlja kao "politički motivisan napad subnacionalnih grupa i/ili individua na kompjuterske sisteme, kompjuterske programe i podatke koje dovode do nasilja nad nevojnim metama."[9] Sličnu definiciju ima u svojim dokumentima i Federalni Istražni Biro (FBI) definišući ovu aktivnosti kao "smišljen, politički motivisan napad subnacionalnih grupa ili tajnih agenata na informacije, računarske sisteme, računarske programe i podatke , koji dovode do nasilja nad nevojnim ciljevima." Sajber terorizam se može definisati i kao "korišcenje računarskih mreža za isključivanje kritične nacionalne infrastrukture - kao što su energetski sektori, transport, industrijska postrojenja, za zastrašivanja Vlade i civilnog stanovništva."[10] Jedna od definicija je da je ova aktivnost "politički motivisana upotreba kompjutera, bilo kao meta bilo kao oružje subnacionalnih grupa ili tajnih agenata koji žele da na nasilan način utiču na javnost i vlade država."[11]

Najcitiranija definicija sajber terorizma potiče od profesora Doroti Denining. Po njoj, to je "planirana štetna aktivnost, ili pretnja, u sajber prostoru, sa namerom da se ostvare socijalni, ideološki, verski, politički ili slični ciljevi, ili da se zastraše građani u cilju ostvarenja tih ciljeva."[12] Profesor Dening opisala je sajber terorizam kao konvergenciju terorizma i sajber prostora. To je "nezakonit napad na računare, mreže i informacije koji mogu da zastraše ili prisile Vladu ili građana u cilju ostvarenja političkih i društvenih interesa. Napad bi trebalo da dovede do nasilja nad licima ili imovinom ili da bar prouzrokuje dovoljno štete za generisanje straha."[13]

Sajber terorizam je oblik terorizma koji uključuje korišćenje kompjutera "da bi se izazvao kolaps u sistemu javnih servera i kritične nacionalne infrastrukture i izazvalo nepoverenje javnosti u institucije."[14]

Ipak, nužno je podvući razliku između sajber terorističkog akta i upotrebe sajber prostora u terorističke svrhe. Nije svaki sajber napad automatski akt sajber terorizam. Upotreba popularnih društvenih mreža, postavljanje fotografija, video snimaka, vandalizam sajtova (poput promene izgleda na početnoj prvoj strani), neke su od aktivnosti koje terorističke grupe

[9] Center for Stretegic and International Studies, *"Cybercrime, cyberterrorism, cyberwarfare, Averting and Electroinic Waterloo",* CSISM 1998.

[10] James A. Lewis, "*Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats",* Center for Strategic and International Studies, December 2002, p. 27. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf,

[11] Clay Wilson, "*Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*", CRS Report for Congress, October 2003, p. 7.

[12] http://www/iwar.org.uk/cyberterror/resources/denning.htm

[13] Mark M. Pollitt, *"CYBERTERRORISM– Fact or Fancy",* Georgetown University, Department of Computer Science, June 2009, www.cs.georgetown.edu/~denning/infosec/ pollitt.html

[14] K. Soo Hoo, S.Goodman, and L. Greenberg, *"Information technology and the terrorist threat",* Survival, vol. 39, no. 3 1997, pp. 135-55.

primenjuju. Ali propagandne aktivnosti terorista se ne mogu samostalno podvesti kao izvorni akt sajber terorizma.

Stoga se postavlja pitanje da li su teroristi Islamske države ujedno i sajber teroristi ili samo upotrebljavaju prednosti sajber prostora u svoje propagandne svrhe.

Digitalizovani džihadizam Islamske države

Islamska država je sunitska teroristička, pobunjenička, džihadistička, transnacionalna grupa, podjednako poznata i pod ranijim nazivom „Islamska država Iraka i Velike Sirije'" (ISIS). Poznata je i pod nazivima Islamska država Iraka i Levanta (ISIL) i Islamska država Iraka i Šama.[15] Nastala je 2004. godine tokom američke okupacije Iraka. Grupa se povezala sa Al Kaidom i bila njihova produžnica u Iraku, a otcepljenje se desilo deceniju kasnije paralalno sa razvojem sukoba u Siriji. Pored izazivanja destabilizacije Bliskog istoka, ID je izazvala vojna i politička reagovanja cele međunarodne zajednice. Deluje na prostoru Iraka i Sirije na kojem je proglasila "kalifat", a najvažniji cilj koji je ID proklamovala je stvaranje jedinstvene islamske države. ID je formirao oblik državnosti na teritorijama koje je zauzeo i postao u neku ruku "kvazi država" bazirajući svoj način vladavine na poštovanju šerijatskog prava i ugrožavajući teritorijalni integritet država Bliskog istoka.

Njihovi zakoni su strogi i apsolutni. Često koriste arhaične i monstruozne metode kažnjavanja neistomišljenika i neprijatelja. Finansijske prihode koji se broje milionima dolara crpe od preprodaje naftnih derivata, uništavaju spomenika kulture stare i nekoliko milenijuma što dodatno svedoči o njihovom varvastvu, ogroman i nezapamćen talas migracija i izbeglica sa područja ratnih dejstava izazvali su potrese, kako na Bliskom istoku tako i širom Evrope. Talas straha preplavio je svet.

Pored fizičkog osvajanja teroritorije, pripadnici ID postali su prepoznatiljivi i po upotrebi modernih sredstava komunikacije, kompjutera i interneta. Njihovo delovanje prevazilazi geografsko bojno polje, premeštanjem tradicionalne ratne taktike na širenje brutalnosti i uticaj na internet. Grupa je "digitalizovala džihadizam u XXI veku."[16] Od postavljanje visoko kvalitetnih video materijala, upotrebi trending oznake heštag (#) u kombinaciji sa jezivim fotografijama pokolja koje postavljaju na mnogobrojnim profilima najpopularnijih društvenih mreža, ID je uvela ovu revolucioranu vrstu (propagandne) borbe.[17] Aktivnom upotrebom društvenih

[15] Islamic State of Iraq and the Levant (ISIL), Islamic State of Iraq and al-Sham (ISIS).

[16] Charlie Winter, "*The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*", Quilliam, July 2015, p. 5

[17] Thomas Elkjer Nissen, "*Terror.com - IS´s Social Media Warfare in Syria and Iraq*", Royal Danish Defence College, Military Studies Magazine ISSUE 02, VOLUME 02, 2014, pp. 3-5.

mreža poput Tvitera, Fejsbuka, Instagrama, Jutjuba, Vibera, teroristička grupa je uspela da dopre do novih simpatizera i poklonika širom planete.

Pripadnici Islamske države aktivno koriste sajber prostor kroz aktivnosti od kojih su najznačajnije:

1. Propagandne aktivnosti – korišćenje društvenih mreža, internet stranica, postavljanje video i foto materijala, štampanje biltena
2. Regrutacija novih članova
3. Komunikacija – interna među članovima, sa globalnom publikom, simpatizerima, aktivistima
4. Za finansiranje svojih kampanja
5. Za izvođenje sajber napada

Dok aktivnosti na socijalnim mrežama koje članovi, simpatizeri i aktivisti grupe koriste mogu da ostvare efekat straha, bespomoćnosti, panike, širom sveta, potencijalno najveća opasnost preti u slučaju sajber terorističkog napada na državnu odnosno nacionalnu infrastukturu država. Do sada hakeri ID nisu uspeli da izvedu napad velikog intenziteta uprkos mnogobrojnim spekulacijama da je grupa sposobna za to. Sem vandalizacije, ometanja ili postavljanja fotografija i snimaka na internet stranice medijskih kuća, institucija, nije zabeležen primer ozbiljnijeg narušavanja ili prekida rada velikih informacionih sistema.

Upotreba društvenih mreža u terorističke svrhe

Teoristi koriste internet kao izuzetno efikasan medij koji im pruža mogućnost komunikacije sa javnošću, pristalicama, simpatizerima, članovima. Terorističke grupe već više od decenije imaju svoje veb stranice. Tu spadaju između ostalih Al Kaida, Tamilski tigrovi, Hamas, Libanski Hezbolah, Narodni front za oslobođenje Palestine (PLFP), baskijska ETA, Irska republikanska partija (IRA). Na svojim stranicama organizacija objavljuje informacije vezane za rad, vesti, ideološke poruke, aktivnosti grupe i ciljeve, bitne datume za organizaciju, biografije lidera, kao i poruke upućene neprijateljima. Teroristi koriste veb sajtove i društvene mreže da bi promovisali svoja načela i doktrinu. Međutim, za razliku od recimo Al Kaide, pripadnici ID žele da pošalju poruku ne samo istomišljenicima, nego celom svetu. Putem propagande na internetu šalju svoje političke, ideološke i verske poruke, fotografije i video snimke, biltene rađene na nekoliko svetskih jezika u cilju dalje popularizacije načela, naročito kod mlađe populacije.

Propagandna mašinerija Islamske države na društvenim mrežama, napravila je pravu revoluciju kada je reč o terorističkim grupama i njihovom "postojanju" na internetu. Upotrebom najpopularnijih društvenih mreža (Twitter, Facebook, Instagram, Youtube) privukla je pažnju globalne publike ali i masmedija koji su svaku poruku terorista plasirali u javnost. Uspeli su

da zaokupe pažnju vizuelnim efektima odnosno monstuoznim snimcima. Svetski mediji su zapravo i učinili uslugu teroristima dajući im na pažnji i značaju jer su njihove poruke i akcije učinili vidljivijim širom planete.

ID se na revolucionarni, popularistički način, na širem i masovnijem nivou obraćala "svetskoj" publici. Procenjuje se da je tokom 2015. godine grupa postavljala u proseku oko 15 fotografija i 3 video snimka dnevno.[18] Grupa je svesna ogromne moci društvenih mreža i koristi internet komunikacije kao efikasno sredstvo za distribuciju svoje ideologije i slanje političkih poruka. Samo korićenjem haštaga #WorldCup2014 tokom Svetskog prvenstva u fudbalu, ID je milionima ljudi skrenuo pažnju na svoje aktivnosti. Time su postigli efekat da se promovišu korisnicima društvenih mreža koji nisu u pretrazi kucali ime same grupe. Islamska država je kao odgovor na vazdušne napade Sjedinjenih Američkih Država, koju je odobrio predsednik Barak Obama 7. avgusta 2015. godine, uzvratila na virtuelan način kroz haštag kampanju #AMessageFromISIStoUS.

Teroristima je društvena mreža Tviter "omiljeni medij" komunikacije za širenje svoje propagande. Kratke poruke, odnosno tvitove, fotografije, video snimke u kratkom vremenskom periodu vide milioni ljudi. Grupa se oslanja na ovu mrežu da bi povecala domet i uticaj na širi auditorijum. Zahvaljujući sajber kampanjama virtuelnih pristalica i aktivista, fotografije, snimci i poruke su preplavile internet.[19] Prednost Tviter naloga je što su korisnici u mogucnosti da efikasnije sakriju svoj identitet nego što je to slučaj na drugim socijalnim mrežama. Ipak, administratori Tvitera uspeli su da ugase na hiljade naloga ove terorističke grupe, ali skoro uvek bi u kratkom roku komunikacija bila ponovno uspostavljena otvaranjem novih naloga. Tviter i Gugl neprestano ograničavaju uticaj Islamske države u virtuelnom svetu gašenjem naloga i profila koji su u "suportnosti sa uslovima korišćenja." Međutim, ID se uspešno bori sa ovim izazovom konstantno razvijajući stategije kako bi izbegli da budu cenzurisani. Koriste, na primer, spam algoritam Tvitera kako bi omogućili informacijama da normalno teku.[20]

Video snimci masovnih ubijanja, pogubljenja i mučenja sa naloga društvenih mreža grupe našli su se u gotovo svakom domu. Snimci brutalnog odsecanja glave američkog novinara Džejmsa Folija, preplavili su internet u roku od nekoliko sati. Usledili su novi snimci klanja, mučenja, maltretiranja, osakaćenih tela u ratu posle svakog osvajanja. Snimci su ostavili ceo svet u šoku ovakvim divljaštvom i varvarstvom. Uz snimke mučenja stranih novinara, zatvorenika, taoca, neprijatelja, ID je na internet

[18] Charlie Winter , "*The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*", Quilliam, July 2015, p. 15.

[19] http://www.businessinsider.com/isis-is-using-twitter-to-make-threats-to-us-2014-6/2/02/ 2016

[20] Thomas Elkjer Nissen, *"Terror.com - IS´s Social Media Warfare in Syria and Iraq"*,Royal Danish Defence College, Military Studies Magazine ISSUE 02, VOLUME 02, 2014, op.cit., p. 4.

kanale postavljao snimke osvajanja teroritorije, ratnih pobeda koji glorifikuju njihovu borbu. Mnogi postavljeni video snimci kao da su stvoreni i režirani u najboljim filmskim studijima sveta. Teroristi su počeli da obraćaju pažnju i na sitnice poput čiste odeće, ''scenografije'', grafičkih detalja. Takozvani "selfiji" vojnika na bojištu koji poziraju pored ubijenih tela takođe se često mogu videti, što na njihovim privatnim profila, što na "zvaničnim" ID profilima na društvenim mrežama.

Ali, grupa se 2014. godine nije bavila samo postavljanjem video snimaka divljaštva već promocijom "moralnih i verskih vrednosti." Snimci u kojima se pripadnici Islamske države igraju sa decom, šalju verske poruke, civili koji hvale dolazak ID-a, snimani su u cilju približavanja mlađoj generaciji potencijalnih regruta. Takvih "epizoda serije" nije mnogo. Pravo lice ID je pokazao surovim i mučkim ubistvom dvestotine dece u novembru 2015. godine.

Pored snimaka borbe i snimaka dobročinstva, kao treća grupa video klipova mogu se izdvojiti snimci u kojima pripadnici, ratnici i istaknuti članovi ID pričaju hvalospeve o svojoj borbi. I ovi video snimci se efektivno koriste za regrutaciju mladih islamista kao i poziv da se što više ljudi priključi borbi.

Regrutovanje sledbenika i finansiranje

Moderna sredstva komunikacije pružila su teroristima mogućnost lakšeg organizovanja grupe, planiranja napada i sprovođenja istih. Pristalice i članovi mogu da putem elektronske komunukacije dobiju uputstva o sprovođenju napada, mape, zatim uputstva o pravljenju bombi i sličnog oružja.[21]

Takođe, teroristi koristeći moderna sredstva komunikacije uspešno sprovode i regrutaciju novih članova. Teroristi iskorišćavaju faktore poput nepravde, lošeg životnog standarda, osećaja odbačenosti, koji se kod mladih često javlja, ne bi li ih privoleli da se pridruže grupi.[22] Profili individua koji se pridružuju Islamskoj državi su različiti. Razlikuju se po pripadnosti, veroispovesti, porodičnom nasleđu, godinama, socijalnom staležu, obrazovanju.[23] Njihovi motivi za podršku teroristima su takođe različiti. U maju 2015. godine, Savet Bezbednosti Ujedinjenih Nacija objavio je procenu da se više od 25.000 stranih boraca iz 100 država pridružilo Islamskoj državi.[24] Iznenađujući je broj mladih regruta koji dolaze iz Sjedinjenih

[21] Robin Simcox, "*We Will Conquer Your Rome": A Study of Islamic State Terror Plots in the West*," The Henry Jackson Society 2015, p. 52.

[22] European Commission, Expert Group on Violent Radicalisation, *"Radicalisation processes leading to acts of terrorism"* (2008), www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.

[23] Lorenzo Vidino and Seamus Hughes, "*ISIS in America: from retweet to Raqqa",* Program on Extremisms, George Washington University, December 2015, p. 11.

[24] United Nations' Security Council, *"Action Against Threat of Foreign Terrorist Fighters Must be Ramped Up, Security Council Urges in High-Level Meeting,"* 7453rd Meeting (AM), May 29, 2015.

Američkih Država. Prema podacima od marta 2014. godine protiv 71 osobe podignuta je optužnica za saradnju sa ID, 250 je osumnjičeno a protiv više od 900 ljudi se vodi istraga.[25] Tačan broj koliko ljudi se pridružio zahvaljujući "online" kampanjama je nepoznat.

Internet je olakšao komunikaciju terorista kako sa globalnom publikom u vidu aktivnosti na društvenim mrežama, tako i međusobno. Pored foruma, čet soba i različitih naloga, teroristi koriste elektronsku komunikaciju u vidu slanja mejlova. Vešto kriju svoju lokaciju i identitet, IP adrese, koriste kriptovane i šifrovane poruke ali i steganografiju. Bivši zvaničnik CIA Majkl Morel (Michael Morell) rekao je gostujući u medijima da smatra da će biti jako teško ući u trag enkriptovanim porukama koji teroristi koriste u međusobnoj komunikaciji,[26] naročito kada je planiranje napada u pitanju.

Teroristi onlajn kampanjama skupljaju donacije i novac za finansiranje svojih aktivnosti. Al Kaida je, na primer, organizovala kupovinu majica, šolja za kafu, zastava, DVD-ja putem svog veb sajta.[27] Na sajtovima terorističkih grupa često se nalaze brojevi računa na koje se mogu uplatiti novčana sredstva.

Sajber napadi

U februaru 2015. Džejms R. Klaper, direktor Nacionalne obaveštajne agencije rekao je da su sajber napadi najveća opasnost po ekonomiju i nacionalnu bezbednost Sjedinjenih Američkih Država.[28] "Politički motivi iza sajber napada" su po njemu primarna opasnost. Direktor FBI Džejms Komej je na Bezbedonosnom Forumu u Aspenu ponovio da je Biro zabrinut da bi ovakvi napadi mogli da budu izvedeni od strane sajber terorista.[29]

Veštinu manipulacije savremenih kanala komunikacije i tehnologije, poput mreža Fejsbuk, Tviter i Jutjub, pripadnici Islamske države su savladali. Međutim, znanje korišćenja društvenih mreža ne mora nužno da znači da su njihovi hakeri obučeni da izvedu sofisticirani sajber napad velikih dimenzija koji bi ugrozio funkcionisanje državne infrastukture. Čini se ipak da ID ima mnogo veću sposobnost PR-a i sopstvene afirmacije, pre nego realnih kapaciteta za izvođenje sajber terorističkih napada.

---

[25] Lorenzo Vidino and Seamus Hughes, "ISIS in America: from retweet to Raqqa", Program on Extremisms, George Washington University, December 2015, op.cit., p. 12.

[26] http://www.cbronline.com/news/cybersecurity/encryption-isis-and-terrorism-in-cyber-space-4733747/ 7/02/2016/

[27] Awan Imram: "*Debating the term cyber-terrorism: issues and problems*", Internet Journal of criminology, 2014. ISSN 2045 6743, p. 9.

[28] http://www.defense.gov/News-Article-View/Article/604190/intelligence-chief-describes-pervasive-uncertainty-of-worldwide-threats /31/01/2016/

[29] http://www.aspentimes.com/news/17381873-113/fbi-director-reveals-hidden-threat-of-isis /5/02/2016

Stoga je neophodno podvući razliku između sajber terorističkog akta i upotrebe sajber prostora u terorističke svrhe. Sajber terorizam predstavlja nelegalni akt u kom se kao oružje primenjuju kompjuter i internet u cilju ugrožavanja ljudskih života i nacionalne infrastrukture. Napadi na računarske sisteme, mreže koji mogu izazvati prekide ili prekid u radu, gubitak života ili povredu, su akti sajber terorizma.

Godina 2015. bila je obeležena sajber aktivnostima hakera Islamske države ali ako se analiziraju medijski izveštaji i saopštenja zvaničnika, uvidećemo da nije došlo do ozbiljnijeg napada na nacionalnu infrastukturu država iako su hakeri grupe i onlajn aktivisti koji ih podržavaju, proglasili, tzv. "sajber kalifat". Takođe, analizirajući najbitnije slučajeve sajber napada za koje se sumnja da su delo hakera Islamske države, može se zaključiti da veća šteta nije učinjena.

Hakeri ID preuzeli su odgovornost za napad izveden 12. januara 2015. godine na Tviter i Jutjub naloge Centralne Vojne Komande Sjedinjenih Američkih Država.[30] Napad je izazvao svetsku pažnju i stavio sajber pretnje Islamske države u prvi plan. Na početnu stranicu Tviter naloga postavljen je natpis ''I love you ISIS'' i "CyberCaliphate". Ovaj napad, sem što je neprijatan i izgleda pomalo ponižavajuće, nije imao nikakvo destruktivno dejstvo, stoga se pre može okarakterisati kao čin vandalizma pre nego sajber terorizma. Treba uzeti u obzir da sem napada na nalog društvene mreže, funkcionisanje veb sajta, kao i zvaničan mejl - centcom.mil, nisu bili ugroženi niti je bilo prekida rada. Nije bilo promena, preopterećenje saobraćaja, izmene ili uništenje podataka. Jednostavno rečeno – nije bilo znakova napada.

Grupa okupljena oko sajber kalifata objavila je pod velom senzacionalizma imena i brojeve telefona članova Kongresa Sjedinjenih Američkih Država tvrdeći da su do informacija došli hakovanjem servera Kongresa.[31] Sve te informacije su inače dostupne na sajtu Predstavničkog Doma. Nije potreban visoko obučen IT stručnjak da bi kopirao imena sa sajta.

Iako je sajber kalifat, kao pokret poznat i kao #CyberCalipHATE, u nekoliko navrata okrivljen za pojedine sajber napade, sve je više dokaza da su za te akte odgovorni ne direktno članovi ID-a već hakerske grupe koje ih podržavaju. Broj grupa podrške raste što je zabrinjavajuća činjenica. Trend se nastavio i u 2016. godini kada se pridružila grupa iz Palestine AnonGhost.[32]

Simpatizeri su izvršili seriju napada na manje kompanije i na medije uključujući i francusku televiziju TV5 Monde. U aprilu 2015. godine, grupa

[30] http://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack 29/01/2016

[31] http://www.theepochtimes.com/n3/1898608-hackers-trace-locations-of-isis-cybercaliphate-say-their-cyberattacks-are-fake/ 2/02/2016

[32] http://www.ibtimes.co.uk/isis-cyberwar-anonymous-hots-daesh-hackers-team-palestinian-group-anonghost-1537571 /3/05/2016

hakera koja je tvrdila da je deo ID, preuzela je kontrolu nad francuskom TV stanicom i organizovala blokadu emitovanja programa, sajt i naloge na društvenim mrežama u intervalu od 3 sata.[33]

Hakerska grupa Lizard Squad, naklonjena ciljevima ID-a, hakovala je sajt malezijske aviokompanije a sumnja se da je počinila i napad na sajtova Vatikana i produkcijske kuće Sony.[34] Takođe, grupa je DDoS napadom oborila sajt Britanske Agencije za criminal.[35]

Pripadnik IS-a Abu Husain Al Britani je 2012. godine hakovao privatan nalog nekadašnjeg premijera Velike Britanije Tonija Blera.

Da li postoji realna opasnost od sajber terorističkog akta?

Kao što je prethodno istaknuto, treba razlikovati sajber terorizam od aktivnosti koje sprovode teroristi u sajber prostoru. Teroristi Islamske države koriste internet kao globalnu komunikacionu mrežu za širenje svoje propagande, za komunikaciju, regrutaciju svojih članova. Ove aktivnosti su samo jedan od instrumenata delovanja terorista, ali sama po sebi nisu sajber napad koji cilja kompjuterske sisteme.[36] Dakle, može se zaključiti da aktivnosti terorista u sajber prostoru poput plasiranja užasavajućih video i audio snimaka, postavljanje fotografija, objavljivanje vesti, blokiranje rada internet sajtova - mogu izazvati osećanje straha, terora, panike, zatim mogu podići stepen bezbednosti na viši nivo, mogu imati iza sebe političku i ideološku pozadinu ali ne mogu izazvati smrt, povredu ili fizičko oštećenje, ekološku ili finansijsku katastrofu. Stoga je nužno podvući razliku između sajber napada koji mogu da izazovu sajber teroristi direktnom akcijom i aktivnosti koje teroristi spovode u sajber prostoru a koji je uglavnom propagandnog sadržaja.

Sem sajber napada manjeg intenziteta i vandalizacije sajtova, hakeri ID nisu napravili veću štetu. Postavlja se pitanje da li i u kojoj meri ID ima kapacitet da izvede sajber terorističke napade na nacionalne vitalne infrastrukture i time ugrozi funkcionisanje pojedinih sektora država.

Ne zna se mnogo o ofanzivnim sajber kapacitetima grupe niti postoje jasni pokazatelji koji bi pokazali da organizacija ima napredne mogućnosti da izvede sofisticirane napade. Teroristima su se priključili obrazovani, mladi i IT pismeni

[33] http://nationalinterest.org/blog/the-buzz/deadly-mistake-dont-underestimate-isis-cyberspace-13014/ 13/12/2015

[34] http://www.techtimes.com/articles/28654/20150126/malaysia-airlines-website-hacked-by-cyber-caliphate.htm /11/11/2015

[35] http://www.engadget.com/2015/09/01/lizard-squad-national-crime-agency-ddos/ 14/10/2015/

[36] Gabriel Weimann, "*Cyberterrorism: The sum of All Fiers*", Studies in Conflict and Terrorism, 28, Taylor&Francis Inc, 2005, op. cit., p. 130.

pripadnici koji dolaze iz razvijenih zemalja, stoga se može pretpostaviti da grupa poseduju sajber sposobnosti jer u svojim redovima ima članove sa većim razumevanjem tehnologije. Ali mora se uzeti u obzir da, do sada, nisu pokazali da poseduju kapacitete da izvedu sofisticirani napad na kritične infrastrukture država. Ako se uzme u obzir da u nacionalnu infrastrukturu spadaju između ostalog: energetska i nuklerana postrojenja, brane, snabdevanje strujom i vodom, transportni saobraćaj, telekomunikacione mreže, jasno se može zaključiti da bi potencijalni napad poremetio funkcionisanje napadnutog sistema[37] i imao ogromne konsekvence po državu a ponajviše na civile[38]. Mogućnost da teroristi mogu da napadnu sistem, bilo kroz oštećenje funkcija, izmenu načina rada, bilo kroz kontrolu sistema, zastrašujuća je i postaće sve veći nacionalni, regionalni i svetski izazov bezbednosti.

Početkom novembra 2015. godine direktor FBI departmanta za sajber incidente Džon Rigi je izjavio da bi hakeri Islamske države mogli da napadnu infrastrukturu SAD-a. Naročito je izrazio zabrinutost za energetski sector.[39] Međutim, u istoj izjavi za medije Rigi je podvukao da, prema saznanjima FBI, teroristi trenutno ne poseduju sofisticirane hakerske alate koji bi ugrozili funkcionisanje sistema infrastukture SAD-a.[40] Ipak, postoji bojazan da pripadnici ID mogu da dođu u posed dovoljno dobrog softvera koji bi bio u mogućnosti da utiče na rad energetskog sistema i ostavi bez električne energije na stotine hiljada domaćinstava kupovinom na crnom tržištu.[41]

Čini se da sajber teroristi nisu u dovoljnoj meri razvili korišćenje informatičkih i komunikacionih alata[42] koji bi potencijalno izazavali oštećenja prilikom napada, a čije bi posledice bile katastrofalne. Ipak, ne treba grupu potcenjivati kao ni potencijalne opasnosti koje vrebaju od hakerskih grupa koje podržavaju teroriste.

Kako se boriti protiv IS u sajber prostoru?

Dva dana nakon masakra na ulicama glavnog grada Francuske, najpoznatija hakerska grupa na svetu – Anonimusi[43] objavila je (hakerski)

[37] Nathalie Caplan, "*Cyber War: the Challenge to National Security Global Security Studies*", Winter 2013, Volume 4, Issue 1, p. 93.

[38] Jonathan A.Ophandt, "*Cyber Warfere and the crime of sggression: the need for individual accountability on tomorrow's battlefield*", Duke Law & Technology Review, 2010. p. 7.

[39] http://www.windpowerengineering.com/featured/business-news-projects/isis-cyber-attacks-on-u-s-infrastructure/1/12/2015

[40] http://www.windpowerengineering.com/featured/business-news-projects/isis-cyber-attacks-on-u-s-infrastructure/

[41] http://money.cnn.com/2015/10/15/technology/isis-energy-grid/1/12/2015

[42] Poput malvera, virusa, kompjuterskih crva.

[43] Reč je o decentralizovanoj onlajn zajednici koja broji na desetine hiljada 'haktivista" širom sveta i koja koristi računarske veštine za izvođenje napada i obaranje sajtova kao oblik

rat protiv islamista.[44] Ovo nije prvi put da se Anonimusi obračunavaju sa džihadistima – borba je zapravo počela sajber kampanjom #OpIsis nakon terorističkih napada na novinare francuskog magazine Šarli Ebdo u januaru 2015. godine. Anonomusi su, takođe, putem svojih kanala i kampanje #OpParis pozvali sve svoje pristalice da se uključe u borbu protiv Islamske Države. Hakeri su nakon užasnog terorističkog akta u Parizu u novembru 2015. godine proglasili "sajber rat" protiv Islamske države.[45] Grupa daje uputstva za hakovanje internet sadržaja Islamske države čak i ljudima koji nisu tehnički pismeni. Prema izveštaju magazina "Foreign Policy", Aninimusi su od januara do novembra 2015. uspeli da sruše 149 sajtova, 100.000 Tviter naloga, kao i da spreče prikazivanje oko 5.000 propagandnog video materijala Islamske države. Za 24 časa oboreno je čak 5.550 Tviter naloga ID.[46] Borba hakera, medijski pompezno najavljena ostala je, pak, na obaranju sajtova, brisanju naloga i na propagandne objave.

Da bi se aktivnosti Islamske države zaustavila u sajber prostoru, mora se izazvati prekid komunikacija pripadnika ID, kako između sebe tako i sa javnošću. Takođe bitna stavka u borbi jeste upad u datoteke odnosno baze podataka koje Islamska država poseduje. Na takav način može se doći do imena pripadnika Islamske države, do njihovih saradnika i mreža koje su rasprostranjene širom sveta. Potencijalno se mogu otkriti sledeće mete napada. Hakeri mogu doći u posed i vrednih informacija o načinu finansiranju terorista, snabdevanju oružjem i slično.

Jedan od potencijalnih predloga kako se može doći u neposredan kontakt sa hakerima Islamske države je i infiltriranje agenata bezbedonosnih službi na forume i "chat" sobe.[47] I ranije je bilo pokušaja da se na "skrivenom delu Interneta", ispod površinskog dela koji mi koristimo, na takozvanom "Deep Webu" infiltriraju teroristi i sajber kriminalci, ali nisu uvek bili uspešni. Mudrom taktikom i strpljenjem, možda bi naredni pokušaji bili mnogo uspešniji.

Kao što je politika društevnih mreža -Twitter, Facebook, Google-platforma da otklone sadržaj koji promoviše terorizam i terorističke akcije, bilo putem nadzora aktivnosti korisnika ili kroz prijavu takvih aktivnosti, gašenje sajtova terorističkih organizacija koji direktno pripadaju terorističkoj grupi je preporučljivo, kao i sajtovi organizacija koje takve grupe podržavaju.

protesta. Uspeli su u više navrata da dođu do značajnih i poverljivih informacija i baza podataka institucija vlada država širom sveta. Aktivno koriste sajber prostor za širenje svojih stavova i ideja.

[44] http://fortune.com/2015/11/16/anonymous-cyber-war-isis/ 10/12/2015

[45] http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030 /10/12/2015

[46] http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/ 10/12/2015

[47] Roland Heickerö, "*Cyber Terrorism: Electronic Jihad"*, Strategic Analysis, 2014 Vol. 38, No. 4, p. 562.

Uprkos tome što internet predstavlja "globalno dobro", ne pripada nikome a svi mogu da ga koriste, izuzetno nepopularan koncept "cenzure", odnosno medijske izolacije, može biti potencijalno jedno od rešenja kako, makar prividno, može da se zaustavi Islamska država u sajber prostoru. Sloboda izražavanja, sloboda govora, sloboda misli spadaju u osnovna ljudska prava, ali u slučaju kada ta sloboda govora ima za cilj izazivanje panike ili služi kao alat terorističkim grupama u sajber prostoru, mora se pronaći efikasno rešenje kako se takva aktivnost mora ograničiti.

Efektivna borba protiv hakera Islamske države kao i svake druge terorističke organizacije mora biti praćena međusobnim razumevanjem i saradnjom država, međunarodnih i bezbednosnih institucija, IT sektora, akademskog i nevladinog kruga. Jedna od preporuka je i bilateralna saradnja država. Odlične vidove saradnje u oblasti sprečavanja sajber terorizma sprovode Indija i Saudijska Arabija.[48] Ruska Federacija i Izrael takođe su se sporazumele da će se zajedničkim sredstvima boriti protiv terorista na Internetu. Velika Britanija je izdvojila dodatnih milijardu funti da bi poboljšala zaštitu svog sajber prostora od hakera Islamske države.[49]

Zaključak

Poput klasičnog terorizma i sajber terorizam je potencijalna opasnost po državnu bezbednost. Sajber terorizam je globalni problem koji zahteva globalni odgovor i saradnju. Teroristi su svesni benefita koje im delovanje u sajber prostoru donosi i rado ga eksploatišu u svoju korist.

Islamska država je na efektivan način iskoristila uticaj socijalnih mreža i interneta kao globalni medij u cilju promovisanja svojih načela, borbe i ideala. Ali propagandne aktivnosti sem što su umnogome popularizovale grupu širom sveta, ne mogu biti okarakterisane kao akti sajber terorizma. Teroristi još uvek nisu pokazali visok stepen IT obučenosti, niti su njihovi napadi dovoljno sofisticirani da bi naneli veliku štetu. Ipak, države su sve opreznije i pristupaju izradama sajber bezbedonosnih strategija i sistemima odbrane od opasnosti.

Uspešno uništenje Islamske države je moguće i mora se odvijati na više frontova. Borba protiv Islamske države mora da se odvija paralelno u vazduhu, na kopnu ali i u sajber prostoru. Nužno je podvući da su u svakom obliku zaustavljanje ove terorističke grupe neophodna međunarodna podrška i saradnja.

[48] http://thehill.com/policy/cybersecurity/251409-us-allies-pledge-to-combat-isis-in-cyberspace 4/5/2016

[49] http://news.sky.com/story/1589292/how-dangerous-is-the-cyber-caliphate 3/10/2016

Bibliografija

Center for Stretegic and International Studies, ''*Cybercrime, cyberterrorism, cyberwarfare, Averting and Electroinic Waterloo*'', CSISM 1998.

Caplan, Nathalie, "*Cyber War: the Challenge to National Security Global Security Studies*", Winter 2013, Volume 4, Issue 193.

Clay, Wilson, "*Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*", CRS Report for Congress, October 2003.

Dogrul, Murat, Aslan, Adil, Celik, Eyyup, "*Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*", 2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011 © CCD COE Publications.

European Commission, Expert Group on Violent Radicalisation, "*Radicalisation processes leading to acts of terrorism*" (2008). www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.

Heickerö, Roland, "Cyber Terrorism: Electronic Jihad", Strategic Analysis, 2014 Vol. 38, No.

Hoo Soo, K., Goodman, S. and Greenberg, L., *"Information technology and the terrorist threat"*, Survival, vol. 39, no. 3, 1997.

Iklody, Gabor, "*The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities Defence Against Terrorism*", Review Vol.3, No. 2, Fall 2010.

Lewis, James, "*Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*", Center for Strategic and International Studies, December 2002.

Nissen, Thomas Elkjer, "*Terror.com - IS´s Social Media Warfare in Syria and Iraq*", Royal Danish Defence College, Military Studies Magazine ISSUE 02, VOLUME 02, 2014.

Simeunović, Dragan, "*Terorizam*", Pravni fakultet Univerziteta u Beogradu, Beograd 2009.

Simcox, Robin, "*We Will Conquer Your Rome*": A Study of Islamic State Terror Plots in the West", The Henry Jackson Society 2015.

Pollitt, Mark M., *"CYBERTERRORISM– Fact or Fancy."* Georgetown University. Department of Computer Science, June 2009, www.cs.georgetown.edu/~denning/infosec/ pollitt.html

United Nations' Security Council, "Action Against Threat of Foreign Terrorist Fighters Must be Ramped Up, Security Council Urges in High-Level Meeting," 7453rd Meeting (AM), May 29, 2015.

Vidino, Lorenzo, Hughes, Seamus, "ISIS in America: from retweet to Raqqa", Program on Extremisms, George Washington University, December 2015.

Winter, Charli, "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy", Quilliam, July 2015.

Elektronski izvori:

http://www.cbronline.com/news/cybersecurity/encryption-isis-and-terrorism-in-cyber-space-4733747

http://www.businessinsider.com/isis-is-using-twitter-to-make-threats-to-us-2014-6

http://www.defense.gov/News-Article-View/Article/604190/intelligence-chief-describes-pervasive-uncertainty-of-worldwide-threats

http://www.aspentimes.com/news/17381873-113/fbi-director-reveals-hidden-threat-of-isis-at

http://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack

http://www.theepochtimes.com/n3/1898608-hackers-trace-locations-of-isis-cybercaliphate-say-their-cyberattacks-are-fake/

http://www.ibtimes.co.uk/isis-cyberwar-anonymous-hots-daesh-hackers-team-palestinian-group-anonghost-1537571

http://nationalinterest.org/blog/the-buzz/deadly-mistake-dont-underestimate-isis-cyberspace-13014

http://www.techtimes.com/articles/28654/20150126/malaysia-airlines-website-hacked-by-cyber-caliphate.htm

http://www.engadget.com/2015/09/01/lizard-squad-national-crime-agency-ddos/

http://www.windpowerengineering.com/featured/business-news-projects/isis-cyber-attacks-on-u-s-infrastructure/

http://www.windpowerengineering.com/featured/business-news-projects/isis-cyber-attacks-on-u-s-infrastructure/

http://money.cnn.com/2015/10/15/technology/isis-energy-grid/

http://fortune.com/2015/11/16/anonymous-cyber-war-isis/

http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030

http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/

http://www.mirror.co.uk/news/technology-science/technology/anonymous-publishes-details-isis-recruiters-6848502

https://www.rt.com/news/322427-anonymous-isis-twitter-accounts/

http://thehill.com/policy/cybersecurity/251409-us-allies-pledge-to-combat-isis-in-cyberspace

http://news.sky.com/story/1589292/how-dangerous-is-the-cyber-caliphate

Katarina JONEV

THE ACTIVITIES OF ISLAMIC STATE IN CYBERSPACE

ABSTRACT

At the beginning of the 21st century, terrorism has become a major security threat to the modern world. As the international community faces a number of threats and challenges, terrorist groups continue to spread fear by improving their operating methods. Cyber terrorism is a form of terrorism and potentially the method that terrorists could use in their fight. It is an illegal act in which the weapons implemented, in order to endanger human life and national infrastructure, are computers and the Internet. Attacks on computer systems and networks that can cause disruption or interruption of work, loss of lives or injury to people, physical destruction, as well as financial and ecological consequences are the acts of cyber terrorism. The terrorists of the Islamic State parallel with the physical conquered also cyberspace, especially in a way of extensive use of social networks for the propaganda purpose. This paper presents the authors' attempt to distinguish differences between the acts of cyber terrorism from simple terrorist activities on the Internet such are spreading propaganda and also to analyze the activities of members of the Islamic State in cyberspace.

Key words: terrorism, cyber terrorism, Islamic state, cyber attacks, propaganda, digital jihadism, cyber terrorists.