Western Balkans Security Issues

No. 2/2016

Research Center for Western Balkans Security Issues

September 2016.

ISTRAŽIVAČKI CENTAR ZA PITANJA BEZBEDNOSTI ZAPADNOG BALKANA
RESEARCH CENTER FOR WESTERN BALKANS SECURITY ISSUES

WESTERN BALKANS SECURITY ISSUES No. 2/2016

BEZBEDNOSNI PROBLEMI ZAPADNOG BALKANA
Br. 2/2016

September 2016. BELGRADE
ISSN 2334-6647(Online)

ISTRAŽIVAČKI CENTAR ZA PITANJA BEZBEDNOSTI
ZAPADNOG BALKANA

AUTORI:

WBRC Tim

ADRESA: Istraživački centar za pitanja bezbednosti Zapadnog Balkana,
11000 Beograd, Odabašićeva 3

www.wbrc.rs,

contact@wbrc.rs

Predsednik Upravnog odbora:

mr Tešić Vladimir

+381 66 00 77 59,

vladimir.tesic@wbrc.rs

TEHNIČKA PODRŠKA

Matić Dejan

Publikacija izlazi šestomesečno.

Društvene mreže u funkciji terorista

SADRŽAJ

Uvod	**7**
Sajber terorizam	**8**
Društvene mreže	**10**
Zaključak	**16**
Literatura	**18**

Da li su društvene mreže poligon za regrutaciju terorista, širenje mržnje i komunikaciju terorista?

Uvod

Razvoj informacionih tehnologija poslednjih dvadeset godina izmenio je skoro sve pore društvenog života. Neke promene su pozitivne, a neke su negativne i krajnje nepoželjne. Virtuelni prostor, odnosno internet i društvene mreže su pogodne za radikalizaciju grupa i pojedinaca i slanje poruka koje mogu neposredno ugroziti bezbednost pozivajući pojedince da učine terorističke akcije bez podrške terorističkih organizacija. Islamski ekstremisti sve intenzivnije koriste društvene mreže za vrbovanje i propagiranje svojih aktivnosti i ciljeva.

Nova forma terorizma, poznata pod nazivom sajber terorizam, je sigurno jedna od najopasnijih neželjenih promena. U razvijenom tehnološkom svetu, sajber terorizam dobija nove mogućnosti organizovanja i delovanja, nove ciljeve i oružje. Obzirom na navedeno, strah od sajber terorizma je opravdan, naročito ako se ima u vidu da ovaj vid terorističkih aktivnosti koristi teroristička organizacija „Islamska država“.

U ovom radu pokušaćemo da objasnimo na koji način terorističke organizacije koriste društvene mreže, pre svega, za regrutovanje novih „ratnika“ i širenje straha i panike u društvu, i to na osnovu analize medijskih objava i pregleda stručne literature.

Sajber terorizam

Sajber terorizam u poslednjih nekoliko godina postaje realna opasnost po državu i njenu infrastrukturu. Ipak, mogu li teoristi da ugroze funkcionisanje čitavih sistema kao što su to do sada radili sajber napadači različitih profila. Savremeno društvo se umnogome oslanja na internet i računarske mreže (transportni saobraćaj, finansijske transakcije, elektromreža, sistem odbrane i slično) i postoji veliki rizik da sajber napad terorista može ozbiljno da ugrozi sistem i živote ljudi. Do sada nije zabeležen takav napad, što ne znači da neće i da ne treba biti spreman.

Terorističke organizacije koriste sajber prostor za regrutaciju, propagandu i organizaciju svojih aktivnosti. Islamska država je naptravila revoluciju u korišćenju društvenih mreža poput „Twiter“, „Facebook“, „Instgram“, „You Tube“ za širenje svoje propagande što većem krugu ljudi. Ipak, ove aktivnosti ne možemo podvući pod pojam sajber terorizam.

Sajber terorizam je nelegalan akt i odnosi se na unapred isplanirane, politički motivisane napade na podatke, računarske sisteme i programe, u cilju da se izazove osećaj straha i nesigurnosti. Obzirom da se odvija u sajber prostoru, podrazumeva se da je sam teroristički akt planiran, izvršen ili koordinisan pomoću računarskih mreža. Kao i svaki oblik terorizma, ima političku, ideološku, versku, socijalnu dimenziju.

Najopasniji oblik sajber terorizma je ugrožavanje kritične nacionalne infrastrukture. Međutim, nije svaki sajber napad automatski teroristički akt. Teroristi žele da prenesu svoju poruku većoj grupi ljudi, odnosno njima je potrebna

globalna publika za širenje propagande, za komunikaciju i regrutaciju novih članova. Internet im kao globalni komunikacioni medij to omogućuje. Ova dejstva nisu sajber napadi koji ciljaju sisteme nacionalne infrastrukture. Aktivnosti terorista u sajber prostoru, kao što su postavljanje „horor“ video-snimaka, objavljivanje vesti, blokiranje sajtova mogu izazvati osećanje straha i panike, i mogu imati i političku i ideološku pozadinu, a ne izazivaju smrt, povredu ili fizičko nasilje, ekološku ili finansijsku katastrofu.

Teroristi u novije vreme sve više napuštaju klasične terorističke akte i prelaze na kompjuterski terorizam, koji je veoma efikasno sredstvo u rukama terorista jer im omogućava načine delovanja o kojima ranije nisu ni sanjali. Do sada im je nedostajao odgovarajući talenat i veštine. U današnje vreme koriste veoma visoke tehnologije i tehnike, stalno postavljaju nove „web“ stranice na kojima propagiraju svoje ideje. Iako kompjuteri u dogledno vreme neće zameniti klasična sredstva koja koriste teroristi, poput eksploziva i oružja, sajber teorizam je u stalnom razovju i sve više će se javljati u budućnosti, kao realna opasnost po državu i njenu infrastrukturu.

Društvene mreže

Terorizam dobija nove mogućnosti organizovanja i delovanja, nove atraktivne ciljeve i novo oružje razvijanjem društvenih mreža na internetu. Prema rečima predsednika Društva za informacionu bezbednost Srbije, u informacionom ambijentu nije neophodno delovati na način da se javnost prestraši, izazove nasilje nad ljudima ili unište dobra radi ostvarivanja terorističkih ciljeva. Akcijama sajber terorizma moguće je postići sve navedeno i još mnogo toga lošeg tako da se spreči pristup do baza podataka i/ili prekinu tokovi podataka i na taj način onesposobi društvo.

Računarski virus pod nazivom „Stuxnet“, ubačen u informacioni sistem iranskog postrojenja za obogaćivanje uranijuma izazvao je velike tehničke probleme, koji su kao krajnji rezultat imali znatno kašnjenje u daljem razvoju iranskog nuklearnog programa. Ovaj slučaj svrstan je među prve otkrivene sajber terorističke napade u svetu.

Internet pruža brojne mogućnosti za klasične vidove terorizma, kao što su prikupljanje informacija, regrutovanje novih članova, kupovina oružja i eksploziva, komuniciranje.

Dokumenti koje je otkrio Edvard Snouden te podaci objavljeni u okviru Vikiliksa jasno ukazuju da živimo u vreme "velikog brata", gde svetske obaveštajne agencije nadziru svoj, ali i narod tuđih zemalja, "iz bezbednosnih razloga", te stoga teroristi moraju da koriste razne trikove kako bi ostali neopaženi, a pre svega moraju da budu „potkovani“ znanjem da to urade.

Kao delovi interneta posebno pogodni za namere terorista ističu se tzv. pojmovi „deep web“ i „dark net“.

„Deep web“ je onaj deo interneta koji nije dostupan uobičajenim alatima za pretraživanje, niti uobičajenim metodama pregledavanja, odnosno pristupanja. Radi se o delu interneta utemeljenom na standardnim servisima i protokolima, ali za pristup do kojega je potrebna dodatna autentikacija. Svi zaštićeni servisi poput internet bankarstva čine deep web. Radi se o potpuno legalnim, ali ne i javnim servisima.

„Dark net“ je deo interneta koji također nije dostupan uobičajenim alatima za pretraživanje, a za pristup u njega potrebni su posebni alati, posebne veštine ili podaci. Povezuje se sa raznim ilegalnim aktivnostima kao što su hakovanje, dečja pornografija, trgovina drogom i oružjem, prostitucija i tako dalje. Postoji i deo „dark net“ koji nije nelegalan, već služi za razne oblike zaštite privatnosti, komunikaciju i aktivnosti koje žele ostati neotkrivene. Smatra se da je Islamska država upravo korišćenjem „dark net“ osigurala naoružanje za napade u Parizu i Briselu.

Internet teroristima može poslužiti i u druge svrhe, osim direktnih sajber napada. Jedna od upotreba interneta u terorističke svrhe odnosi se na vrbovanje i regrutovanje novih snaga, uglavnom mlađe populacije, širenjem propagandnih materijala kao što su Jutjub snimci u kojima opisuju ciljeve za koje se bore, načine borbe i značaj njihovog rata.

Neposredan kontakt sa ljudima ostvaruje se i putem društvenih mreža, kao što je Fejsbuk, gde se dalje vrši uveravanje novih članova. Putem društvenih mreža se dogovaraju i transferi novih snaga do same teritorije koje kontrolišu takve grupe.

Takođe, internet je veoma brzo i efikasno oruđe koje se može koristiti za širenje panike. Pripadnici ID neretko objavljuju video ili audio klipove u kojima prete svim nevernicima, odnosno svima koji nisu islamske veroispovesti ili nisu dovoljno dobri muslimani. Neretko se dešava da snimke mučenja i egzekucije postavljaju na internet, pa čak i organizuju i prenose uživo egzekucije.

Arapske vlade su od 2012. ustale protiv "pretnje društvenih medija" i počele da nameću oštre kazne za aktiviste. Nastupila je podela i među samim aktivistima. Društveni mediji više nisu bili otvoreni prostor gde su regionalni aktivisti mogli da se iskažu slobodno i bez inhibicija. Internet policija, čiji je posao bio da nadgleda "opsceni sadržaj", svoju pažnju je preusmerila na političke aktiviste na Tviteru i Fejsbuku. Društvene medije u kojima su delovali liberalni i sekularni aktivisti obilato su počele da koriste ekstremističke grupe.

Prema Međunarodnoj organizaciji rada, nezaposlenost u regionu je pre Arapskog proleća iznosila skoro 25 procenata. Danas bi ove brojke bile veće imajući u vidu lošu situaciju u industriji turizma u zemljama kao što je Egipat, prestanak prodaje nafte u Libiji i milione izbeglica zbog građanskog rata u Siriji i drugih sukoba u regionu.

Pet arapskih država se nalazi u deset najkorumpiranijih zemalja na svetu dok je u izveštaju organizacije Transparency International zaključeno da se "endemska" korupcija zapravo pogoršava u arapskom svetu od pobuna 2011. godine. Nema sumnje da je tako loša situacija olakšala ekstremistima onlajn regrutovanje nezaposlene omladine u regionu.

Iako je Al Kaida poslednjih nekoliko godina do određene mere koristila društvene medije postavljajući snimke na Jutjub, ID je to podigla na sasvim drugi

nivo. Za početak, video-snimci ID-a su mnogo boljeg produkcijskog kvaliteta nego što je to bio slučaj kod Al Kaide, a koriste čak i specijalne efekte. U jednom od videa objavljenom na internetu, ubica ID-a povlači nož i odseca glavu taocu, a sve je prikazano na usporenom snimku da bi se pojačala dramatičnost situacije. Na sledećem snimku u produkciji ID-a, odrubljivanju glava osamnaest sirijskih režimskih vojnika dodat je zvučni efekat lupanja srca.

U najužasnijem videu koji je ID pustio do sada, na snimku koji traje 21 minut prikazuje se spaljivanje živog jordanskog pilota, a sam video imitira produkciju dokumentaraca koji se prikazuju na kanalu History. Snimak se završava prikazivanjem kuća koje navodno pripadaju drugim jordanskim pilotima, identifikovanim tehnologijom vazdušnog mapiranja.

Od jula 2014, ID izdaje onlajn časopis "Dabig" na engleskom jeziku koji može da se preuzme u PDF formatu. Propagandna publikacija, koja bi bez jezivih sadržaja izgledala kao life-style magazin, prikazuje intervjue sa borcima i priče o nedavnim osvajanjima terorističke organizacije.

ID je 2014. godine razvio aplikaciju za android „Fajer Al Bashayer“ (Zora Božijih znamenja) koja, kada se preuzme, ne samo što korisnicima automatski šalje nove informacije o grupi, već takođe preuzima njihove Tviter naloge i na njima postavlja tvitove i apdejtove koji veličaju ID. Kada su snage ID-a ušle u irački grad Mosul, preko aplikacije je poslato 40.000 tvitova u periodu od 24 sata.

Ovo, kao i sve veći broj užasnih videa, navelo je firme koje upravljaju društvenim medijima kao što su Jutjub, Fejsbuk i Tviter da suzbijaju poruke i objave terorista. Njihova politika je bila najočiglednija u slučaju snimka odrubljivanja glave američkog novinara Džejmsa Folija u avgustu 2014. Giganti su

molili svoje korisnike da ne šire taj video i gasili su naloge onih koji su to radili, čim bi ih neko od drugih korisnika prijavio. Bela kuća je takođe intervenisala tražeći od društvenih medija da ne dozvole da se video širi. Uz to, pokrenuta je uspešna kampanja na Tviteru „user@LibyaLiberty“ sa heštegom „ISISMediaBlackout“ koja poziva korisnike društvenih mreža da ne dele video-snimke ID. Prva dvadeset i četiri sata pod ovim heštegom objavljeno je više od 11.000 tvitova.

Društvene mreže mogu biti mač sa dve oštrice za ID. Kada je ova organizacija prikazala prvi video takozvanog kalifa Al Bagdadija koji drži propoved u džamiji, muslimani su iskoristili mreže da se podsmevaju, jer je Al Bagdadi nosio luksuzni švajcarski sat, objavljujući tvitove poput: "Omega: Bagdadijev izbor".

Promena politike društvenih medija, koji su načelno odbojni prema političkim onlajn sadržajima, bila je očigledna u poslednje dve godine. Američka vlada je 2012. pokušala da ugasi Tviter nalog somalske terorističke grupe Al Šabab. Tviter je konačno ugasio nalog Al Šababa nakon što ga je grupa koristila da se hvali napadima. Društvene mreže objavile su seriju novih pravila korišćenja usmerenu protiv eksplicitnih prikaza i slika nasilja.

ID shvata potencijalni domet društvenih mreža i koristi ih za regrutovanje, širenje straha i propagiranje ekstremističke ideologije. Ove platforme se takođe koriste za prikupljanje novca i potragu za simpatizerima i ljudima koje bi mogli da preobraze u napadače tipa "usamljeni vuk". Jedan od ovakvih Tviter naloga se zvao „ShamiWitness“. Pre nego što ga je administrator ugasio u decembru 2014, imao je preko 17.000 pratilaca. Korisnik koji je bio direktor marketinga i živeo u Bangaloru u Indiji, rekao je britanskom Kanalu 4, čije je istraživanje okončalo

njegovu karijeru propagatora terora, da bi se "on priključio ID-u i sam, ali da je njegova porodica finansijski zavisna od njega".

Incidenti kao što je ovaj mogu naterati firme i vlade da uvedu dodatne zabrane za društvene mreže i tako ponovo promene do neprepoznatljivosti nekada slobodan i otvoren sajber-prostor.

Možemo zaključiti da internet ima svoju tamnu (negativnu) stranu iako predstavlja možda i najveće dostignuće današnjeg drušva.

Zaključak

Društvene mreže i internet imaju svoje pozitivne i negativne strane. Mnogo više je pozitivnih, ali negativne se veoma lako mogu iskoristiti u svrhu terorizma i to na dva osnovna načina: regrutacija novih članova, propagandne aktivnosti i komunikacija terorista preko društvenih mreža i izvođenje terorističkih napada u sajber prostoru.

Poslednjih nekoliko godina terorističke orgnizacije sve više koriste internet i društvene mreže kako bi sprovodili propagandne aktivnosti u cilju regrutacije novih članova ali i širenja straha i panike u drštvu. Takođe, presretani su i mnogi slučajevi zaštićene komunikacije između članova terorističkih grupa. Obaveštajno-bezbednosni sistemi država preduzimaju mere za sprečavanje korišćenja društvenih mreža u navedene svrhe, kao i sami autori i osnivači različitih društvenih mreža podizanjem bezbednosnih protokola na viši nivo.

Međutim, terorističke organizacije i pojedinci koriste internet, ne samo za regrutaciju i međusobnu komunikaciju, nego i za nanošenje velikih šteta državnim sistemima putem sajber napada i sabotaža, što većina država i međunarodnih organizacija karakteriše kao sajber terorizam.

Sjedinjene Američke Države i još neke druge države u svetu sajber napade na njihovu kritičnu infrastrukturu izjednačili su sa ostalim oblicima napada i u svojim pravnim aktima predvideli sa se na takve napade odgovori sa raspoloživim snagama. To upućuje da se u bliskoj budućnosti može očekivati i prvi lokalni rat ili vojna intervencija kao odgovor na sajber napad.

Pored država koje pokušavaju da se na navedeni način bore protiv eventualnih sajber napada, imamo i nedržavne „organizacije“ ili u ovom slučaju hakerske grupe, kao što je to grupa „Anonimusi“, koja je objavila sajber rat ID. Grupa je saopštila da će “ujediniti čovečanstvo” i poručila teroristima da ih “očekuju”. Kao glavnu metu označili su kanale komunikacije pripadnika ID i naloge koje koriste ekstremisti[1]. Takođe, grupa je poručila da će raditi zajedno sa drugim hakerima u sajber napadima na ID.

Na kraju, zaključujemo da su sajber napadi ili sajber terorizam realne pretnje po bezbednost pojedinaca, grupa i država, kao i da neke države ozbiljno „ulažu“ u formiranje snaga koje će odgovoriti pre svega preventivno na takve napade. Inicijativa nedržavnih aktera (hakera) može biti samo plus u borbi protiv sajber terorizma.

[1] “Anonimusi iz celog sveta će vas loviti. Znajte da ćemo vas naći i da vas nećemo pustiti. Protiv vas ćemo voditi najveću operaciju u istoriji”, rekao je na francuskom u klipu okačenom na YouTube čovek iza maske Gaja Foksa, tradicionalnog obeležja Anonimusa.

Literatura

- Putnik N.: Sajber-terorizam - potencijalna ili realizovana pretnja, Godišnjak fakulteta Bezbednosti 2008, Fakultet bezbednosti, Beograd, 2009.
- Putnik N.: Sajber prostor i bezbednosni izazovi, monografija, Fakultet bezbednosti, 2009.
- http://www.politika.rs/sr/clanak/348284/Pogledi/Sta-je-sajber-terorizam
- http://www.kurir.rs/planeta/otkrivamo-mracnu-tajnu-interneta-pazite-se-sajber-terorizam-sve-vise-preti-clanak-2269819
- http://www.androidmarket.rs/tag/islamska-drzava/
- http://www.novosti.rs/vesti/naslovna/tehnologije/aktuelno.236.html%3A444049-Sajber-kriminal-Racunar-u-rukama-teroriste-kao-bomba
- http://www.androidmarket.rs/android-vesti/anonimusi-ako-hocete-da-hakujete-id-evo-vam-prirucnik/

Beograd, 2016.

Istraživački centar za pitanja bezbednosti Zapadnog Balkana
Odabašićeva 3
11000 Beograd
www.wbrc.rs
contact@wbrc.rs
Tel: 00 381 66 00 77 59