Sanja Klisarić*

UDK 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2102247K
Stručni članak
Primljen 14.04.2021.
Odobren 20.04.2021.

SAJBER TERORIZAM KAO OKIDAČ SVE INTENZIVNIJE POTREBE ZA BEZBEDNOST SISTEMA OD OPASNOSTI KOJA DOLAZI SA INTERNETA**

Sažetak: *U svetu sve intenzivnijeg sajber sadržaja koji se oslanja na nove tehnologije bezbednost svih sistema je izložena riziku. U ovom članku biće prikazane opasnosti i bezbednosne opcije u cilju zaštite ne samo podataka već i čitavih sistema koji su povezani na nove tehnologije. Takodje, biće istaknut značaj lica koja se bave bezbednosnim pitanjima na internetu. Analizom sadržaja uočava se mogućnost za predikciju koja se u radu izlaže, a povezana sa zaključkom da će se tehnologija sve više razvijati, a samim tim i opasnost od sajber napada biti sve intenzivnija. Rad se fokusira na suštinu odbrane od terorizma koja je neophodna na internetu. Ovim putem ukazuje se one opcije odbrane koje su usaglašene sa ulogama lica zaduženih za bezbednost na internetu kao otvorenom polju za terorističke sajber napade.*

Ključne reči: *Sajber napad, sajber terorizam, internet bezbednost, odbrana na internetu, teroristi, opasnost bezbednosnih sistema na internetu*

* Pravni fakultet, Megatrend univerzitet, Beograd, Srbija; sanja_klisaric@yahoo.com

** Ovaj rad je rezultat projekta FPMIRS – Znanjem do integrisanja u društvene i ekonomske tokove. Projekat je pokrenut sporazumom Pravnog fakulteta sa Međunarodnim institutom za romološke studije.

1. Uvod

Ukoliko znamo da se svakodnevica definitivno sve brže i brže odvija, kao i da tehnologija napreduje doslovno iz dana u dan, neodgovorno je smatrati da je bezbednost isključena iz opsega razvoja koji za cilj pored svih drugih ima i onaj deo naše stvarnosti koji se odnosi na destabilizaciju sistema i opasnost od sajber napada. Naime, logično je smatrati da razvoj tehnologija mora da prati i razvoj bezbednosnih sistema i odbrane od opasnosti koja preti na internetu. Zadatak sistema bezbednosti i službi bezbednosti nije samo da prate razvoj novih tehnologija već i da implementiraju adekvatnu odbranu. Ovaj zadatak ni malo nije lak i to ne samo što u pitanju nije samo praćenje tehnologija kao vid aktivne zainteresovanosti za sajber novosti, već i pravovremena realizacija projekata odbrane usklađene sa razvojem novih tehnologija i modela odbrane. Ako nam je poznato da se sve više naše stvarnosti odvija na internetu, ne treba zaboraviti da opasnost koja preti odatle može imati jednaku ubojitost kao i terorizam. Ako znamo da i životi direktno zavise od interneta jer se sve više medicinskih operacija obavlja ovim putem značaj bezbednosti na internetu je neshvatljivo veliki.[1] Primena je preširoka. Gotovo da nema polja u kom je internet nije zastupljen.

Sada već sasvim očigledno živimo u vremenu kada je sajber tehnologija svakodnevica koja uplivava u sve segmente naših života. Što pre se okrenemo tome kao stanju koje nam je poznato i prihvatljivo, to ćemo pre imati strategiju odbrane od takve opasnosti. Danas ono što se ne vidi može i te kako da ima razornu i opasnu moć jer tehnologija upravo omogućava napad iz daljine, devastaciju bez fizičkog učestvovanja. Ako znamo da danas imamo i slučajeve gde deca od samo pet godina starosti imaju sposobnost da hakuju sisteme, šta možemo da očekujemo od obučenih hakera.[2] Ovakve činjenice treba da pobude interesovanje za implementaciju svih onih sadržaja koji bi na neki način mogli da naprave adekvatnu zaštitu, ali sa stalnom svesnošću da sistem mora neprekidno da se prati, nadgleda i ponovo obezbeđuje unapređivanjem svih tehnologija koje su neophodne u cilju bezbednosti. Ukoliko prihvatimo činjenicu da je sajber terorizam jednako opasan iako se odvija u računarskom prostoru kao i bilo koji drugi vid terorizma na dobrom smo putu da razvijemo tehnologije za borbu protiv njega, ali samo ukoliko hodamo korak ispred terorista, a za to je neophodan značajan broj inteligenthnih resursa u vidu ljudskog i tehnologijskog karaktera. Za ova dva elementa značajno je neprekidno razvijati uporedne sisteme bezbednosti sa fokusom na zaštitu sajber prostora kao ranjivog onim teroristima koji su obučeni upravo za takav vid napada.[3]

Onda kada se orijentišemo ka sajber opasnosti kao onoj koja je istovremena odbrana od istog, ali i meta napada, shvatićemo ugroženost i osetljivost sajber

[1] https://www.bbc.com/future/article/20140516-i-operate-on-people-400km-away

[2] https://www.appknox.com/blog/famous-child-hackers

[3] https://www.bbc.com/news/world-europe-39907965

sistema.[4] Kada se osvrnemo na dešavanja u svetu sasvim nam je jasno da teroristi uočavaju svoju prednost u mogućnostima terorističkih napada, i oni je itekako koriste.[5] U pitanju nisu samo preteći napadi koji su do sada imali za cilj prestrašivanje populacije kojoj su namenjeni, sada se odvija novi vid opasnosti koji preti da ovim putem uruši čitave države i njihove ekonomije. Svet će morati da ostane uvek korak ispred terorista ukoliko ima cilj da opstane. To je naša sadašnjost, to će biti naša budućnost. Jer borba u sajber prostoru ima tendenciju samo da bude sve veća, ni sa kakvim naznakama da će jenjavati.

2. Sajber opasnost kao igla u plastu sena – veština sajber inženjera kao antiteroristički faktor bezbednosti

Naivno je verovati da se sajber opasnost kao okidač terorizma krije samo iza nevidljivih sistema ili individua. Neretko su to i one platforme koje su dostupne široj populaciji jer na taj način može da se pristupi uz pomoć tehnologije onim sadržajima koji za cilj imaju da budu kompromitovani. Supstanca dešavanja u sajber prostoru nije eliminisanje i eksternimacija, već poništavanje validnosti, krađa informacija, novčanih sredstava i onih sadržaja koji bi doveli do kolapsa industrija, ekonomija svih ostalih grana države ili sistema ka kojima su usmereni. U ovako jasno koncipiranom sadržaju problematika se usložnjava samom činjenicom da je to jedan ogroman prostor sa kog napad može biti ostvaren. Ovde se više ne postavlja pitanje na koji način i kada će napad biti realizovan. Sada se jasno zna da je svaki sistem dovoljno izložen opasnosti svakog trenutka i da je jedini način da se pohranjene informacije i sadržaji sačuvaju od terorističkog napada neprekidna zaštita koja se bazira na stalnom napredovanju sistema bezbednosti u ovoj oblasti. Da je ovaj posao težak, jasno pokazuje i činjenica da se sajber prostor neprekidno uvećava i svakim danom zauzima sve veći značaj u našim životima, a samim tim i sve atraktivniju tačku napada.

Sajber terorizam nastaje razvojem interneta i njegovim uplitanjem i ukorenjavanjem u svakodnevicu kojoj pripadamo. Sajber terorizam možemo da tumačimo kao vrstu nasilja koja se manifestuje kao svaki ilegalni napad ili opasnost usmerena na kompjutere, mobilne telefone, medicinske i druge tehnologije vidljive na sajber prostoru, mreže, informacije i sisteme informacija uskladištene unutar računarskog i mrežnog prostora koji je počinjen radi kompromitovanja vlada i građana u cilju političke, ekonomske, i svake druge destabilizacije, a sa namerom postizanja ličnih ciljeva i ideologija terorista. Kada imamo ovakvu svest, širina prostora na kom je napad moguć je nesagledliva. U potpunosti

[4] Vidi: Toffler, A., Toffler,H. (1993):*War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown and Company, Boston.

[5] Sullivant, J. (2007): *Strategies for protecting critical infrastructure assets,* Hoboken, NJ: Wiley.

treba razumeti sajber terorizam samo kao novu taktiku terorizma, a nikako kao sasvim nov oblik terorizma.[6] Tome u prilog govori i činjenica da su motivi i ciljevi napada ostali isti, ali da je sam razvoj tehnologije uslovio evoluciju terorizma, stoga je racionalno zaključiti da se i sam terorizam razgranava u opcijama svog manifestovanja u sajber prostoru. Ne možemo da diskutujemo o novom tipu terorizma jer se na osnovu tiplogije ništa suštinski nije izmenilo. Mete napada i ciljevi su isti, a alat kojim se to postiže ukazuje na stalnu visoko frekventnu adaptabilnost terorista u nemoralnoj borbi koju vode. Sama činjenica da tehnološka revolucija zauzima sve veći prostor i da se odigrava neprestano pred našim očima je dokaz da smo istorijski suočeni sa nečim što je veoma realan i živ prostor i ne postoji ni jedan razlog zašto teroristi to ne bi isto tako posmatrali. Treba imati svest o tome da internet predstavlja ogromnu zonu gde danas svako može da radi doslovno šta želi, od najbanalnije zabave do organizovanja terorističkih napada. Internet omogućava kolektivizaciju ljudi udruženih na osnovu istog interesovanja ili cilja. Poznato je da teroristi koriste internet da objavljuju svoje ciljeve, razloge borbe i motive, jednako kao i podizanje materijalnih sredstava i regrutovanje novih članova.[7] U nepreglednom moru svih mogućih informacija velika je veština izdvojiti one koje nose težinu značajnu za odbranu od terorizma. Ali baš ta veština prepoznavanja opasnosti je prvi korak u zaštiti državnog interesa u sajber prostoru. Činjenica da broj napada, sajber virusa i hakerskih napada neprestano narasta predstavlja veliki izazov svih službi bezbednosti koje se bave zaštitom sajber prostora.

Širina izvedenog prostora u sajber okvirima ima višestruku dimenzionalnost ne samo u smislu opcionog delanja već i vidova komunikacije i finansiranja terorizma. Angažujući stručnjake za sajber demonstraciju svojih agendi, terorističke organizacije imaju veoma veliki potencijal da ostvare svoje namere jer je sam prostor delanja dovoljno veliki da ga je teško kontrolisati. Postaje veoma interesantno zaključiti da je tehnologija primarno fokusirana na pojednostavljenje života i svakodnevice, pronašla svoj smisao u razvoju sajber napada koje ostvaruju terorističke organizacije. Nije u pitanju sam napad, nego i organizacija, regrutovanje novih kandidata, širenje ideologije, finansiranje. Dakle, terorizam se prelio na tehnologije koristeći ih na najbolji način na koji one mogu da služe ma kom sistemu. Ovde je problem ići korak ispred opasnosti jer je opasnost neretko veoma lukavo kamuflirana i predstavlja mogućnost da se ne primeti sve do postizanja svog zadatka. Svakako da su Vlade država svesne opasnosti ovog tipa i da mogu da odgovore izazovu, ali je i činjenica da opasnost svakog dana narasta usklađena sa razvojem i napredovanjem tehnologije. Ono što je veoma

[6] Flemming, P., Stohl, M. (2001): "*International Scientific and Professional Advisory Council of the United Nations*", in Crime Prevention and Criminal Justice Program Countering Terrorism Through International Cooperation, Alex P. Schmid (ed.), ISPAC, Vienna,pp: 70-105.

[7] Mockaitis, T. R. (2007): *The "new" terrorism: myths and reality*, Westport, Conn: Praeger Security Internacional.

uočljivo je i trancendentovanje same filozofije borbe. Još 2002.godine pamtimo izjavu Al Qaide koja kaže da mimo činjenice da se njihova borba zasniva na tradicionalnom borenju, internet predstavlja novo i poželjno polje na kom treba pokazati svoju snagu, agendu i moć.[8] Tu se naglašava značaj i ogromna mogućnost ratovanja u sajber prostoru ističući mogućnost udaljenog napada kao značajnu opciju za anonimnost, navodi se veoma jeftina oprema koja je potrebna da bi se izveo napad, ukazuje se na činjenicu da za napad nije potrebna specijalna vojna obuka, kao ni značajan broj uključenih lica da bi se napad izveo.[9] Onda kada jedna teroristička organizacija deklariše svoje stavove na ovaj način, sasvim nam je jasno da je u pitanju njihova sigurna infiltracija u sajber prostor. Posledice ovoga su nesagledive i to zbog velikog broja faktora. Naime, teroristi u sajber prostoru mogu biti nevidljivi i sasvim neopaženo organizovati napade. Oni imaju veoma puno alatki koje im pomažu da se napad izvede, a jedna od lako dostupnih je sam protok informacija na internetu koji je dostupan svakoj osobi. Više im nije potrebno veoma mnogo vremena da prikupe i obrade informacije kao pre pojave interneta. Sada ih imaju gotovo istovremeno klikom na dugme. Ovo predstavlja veoma veliku pretnju po sve sisteme u svetu jer teroristi sada imaju sva informaciono raspoloživa sredstva da dođu do onoga do čega imaju cilj da se približe kako bi ostvarili svoje planove. Činjenica je da je čitav svet sve više orjentisan na internet i kako je pandemija pokazala doslovno postao zavisan od rada interneta. Sada smo tokom pandemije COVID-19 koja je proglašena 2020.godine po prvi put suočeni sa enormnim značajem interneta i opasnosti ali i neophodnosti sajber prostora. Kada znamo da čitave korporacije, sistemi školstva i ostalih sektora naše kulture i civilizacije su se preorijentisali na funkcionisanje preko interneta, sasvim je logično da odatle preti i napad koji može i za cilj ima da nanese dramatične udarce. Svet danas ne može da funkcioniše na način na koji smo navikli bez interneta. To isto znaju i teroristi. Njihove agende su se preorijentisale na vid borbe koji u sajber prostoru daje dovoljno opasnosti po sve oblasti napada koji su kadri da izvrše. Međutim, treba biti svestan da sama konstrukcija stvarnosti koju današnji svet prihvata kao merilo života u internet prostoru ostavlja neshvatljivo mnogo informacija koje značajno olakšavaju posao teroristima. Današnja kultura je takva da je internet realan prostor na kom se odvija racionalna stvarnost sa koje je život izložen ne samo svojoj manifestaciji već i terorističkom pogledu čija aspiracija uvek za cilj ima devastaciju i kompromitovanje targetiranih meta. Mi kao društvo smo u situaciji kada treba da budemo svesni da tražiti teroristu u sajber prostoru je teže nego tragati za iglom u plastu sena. Stručnjaci sajber bezbednosti su snage koje treba neprekidno da budu nekoliko koraka ispred same tehnologije što nimalo nije lak zadatak i ni u koju ruku ne možemo reći da nije ne samo životni već i karijerijski izazov. Svaki

[8] Venzke, B., Ibrahim, A., (2003): *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets*, Tempest Publishing, LLC, Alexandria.

[9] Ibid.

sajber inženjer zna da sa druge strane sedi jedan poput njega ko zna koliko sličan ili informaciono i tehnološki jači. Utrka za ovladavanjem veština u sajberbezbednosti i sajber napadu postaje gotovo nekontrolisana gde one tehnologije koje danas ugledaju svetlost dana, sutra već postaju prevaziđene i gotovo svaki dan se plasiraju sve novije tehnologije i metode u sajber prostoru kojima se utiče na hakovanje i bezbednost sistema. Stručnjaci iz oblasti sajber inženjeringa su osobe od najvećeg profesionalnog informacionog pritiska jer protok znanja iz ove oblasti ima neprekidnu inerciju ka širenju i uvećavanju svih mogućih informacija, veština, aktuelnosti i činjenica. Ovome u prilog treba dodati i to da su i teroristi sajber inženjeri samo u ulozi agresora, dok odbranu čine njihove kolege osiguravajući sisteme od napadača. U pitanju je jedna te ista struka koja doslovno odmerava snage na internetu.

3. Internet kao poligon borbe protiv terorizma

Ako nam je jasno da je internet poligon za borbu protiv terorizma, postajemo svesni celokupne svetske ranjivosti koja je izložena na internetu. Naime, onda kada znamo da se internet koristi za vrbovanje novih članova, za širenje propaganda, obezbeđivanje materijalnih sredstava, imamo sajber napade na države, vladine institucije, direktnu ugroženost građana napadom na vladine sektore, hakovanje bankovnih računa i informacija od značaja, postajemo svesni da borba sa terorizmom preuzima jedan veoma sofisticiran tip sukoba u kome više nema sadržaja koji bi se poistovećivali sa tradicijom ni u najmanjem slučaju. Sama činjenica da su softeverski sistemi umreženi i da su informacije raspoložive u svakom trenutku, same vlade i državne institucije izlaže opasnosti od napada koji adekvatnim radom službi bezbednosti može biti predupređen. Ovo zahteva veoma dinamičnu i konstantnu borbu ne samo sa hakerima i sajber teroristima, već i sa sve novijim tehnologijama koje osvajaju svet nezapamćenom brzinom.

Svet sajber tehnologije postao je poprište idealne terorističke manifestacije jer na osnovu svih raspoloživih informacija teroristi ne moraju da ulažu ni vreme, ni novac u operacione poslove na terenu kako bi sakupili potrebne informacije. Njihov prostor je svet računara, interneta i novih tehnologija uz pomoć kojih ostvaruju svoje planove. Veoma sofisticiranom tehnologijom sajber teroristi nisu samo sakupljači velikog broja informacija, niti im internet služi samo za razmenu ideologija, vrbovanje i novčane transakcije. Oni su zahvaljujući ovladavanju sajber svetom pristupili jednom veoma ozbiljnom polju znanja kom vladaju i sa kog maskirani poput nekog drugog programa ili obične alatke u nekoj od mreža interneta mogu da dopru do onih informacija do kojih im je cilj da prođu, istovremeno izazivajući napad nesagledivih razmera. Ukoliko ukucate sajber napade uživo bićete doslovno zaprepašćeni koliko napada se dešava u sekundi. Na današnji dan u trenutku posmatranja ovog fenomena bilo je 11.245.779

napada i svake stotinke broj napada se uvećavao za trocifren broj.[10] Dakle, ukoliko u jednom danu imamo preko 11 miliona sajber napada širom sveta čiji se broj svake stotinke uvećava, jasno je da je ovaj vid sukoba postao definitivno najdominantniji. Naime, nikada pre u istoriji čovečanstva nije zabeležen toliki broj sukoba širom sveta u jednom danu. Ovaj podatak jasno ukazuje na eskalaciju sajber terorizma kao ozbiljnog i dramatičnog oružja terorista. Na pomenutom sajtu stoji istaknuto da je najveći broj sajber napada izvršen na obrazovanje i na državne institucije, a kao države koje su pretrpele najveće napade nabrojane su: Nepal, Bolivija, Mongolija, Čile i Gruzija. Posmatrajući hakerske napade uživo, stiče se utisak da se posmatra nekakva video igra, a ne realan teroristički napad pred našim očima. Razlog za takav utisak je nadrealnost frekvence napada koji se ostvaruju svake stotinke širom sveta. Interesantno je istaći da su očito najviše osetljive države sa najslabijom sajber odbranom i da hakerski napadi targetiraju najviše one vlade koje nemaju adekvatnu odbranu. Na samom sajtu u trenutku posmatranja neprekidno se vide napadi između najmoćnijih država, ali kako najverovatnije stoje stvari, većina tih napada se ne ostvaruje upravo zbog snažne odbrane sajber prostora tih država. Na samom sajtu u trenutku pristupa stoji podatak da je 4. aprila 2021.godine u danu zabeleženo 300 miliona napada širom sveta. Ovaj detalj neprikosnoveno ukazuje da je terorizam našao gotovo neuništivo polje sa kog može da dela ne ukidajući svoju razornu moć i ne pomerajući se od svojih ideologija, naprotiv koristeći tehnologiju koja je nastala u Zapadnim državama kao sredstvo protiv nje. Imajući ove podatke u vidu, veoma je neodgovorno verovati da teroristi nisu dovoljno edukovani ili tehnički poduprti da organizuju napade koji ugrožavaju bezbednost sajber prostora. Ako u jednom danu imamo 300 miliona napada, neka je samo 1% tih napada od strane ozloglašenih terorističkih organizacija, to je 3 miliona napada. Dakle, može li iko da zamisli 3 miliona terorističkih napada u istom danu? To je sa ovom tehnologijom danas moguće samo u sajber prostoru i teroristi kako stvari stoje veoma dobro koriste taj prostor za svoje namere.

Veoma intenzivan doprinos sajber terorizmu i uopšte razvoju sajber tehnologija unutar terorističkog ispoljavanja, tačnije, ovladavnju sajber tehnologija drastično su pomogli islamisti unutar Evrope koji su napravili veliki proboj u ovoj oblasti aktivirajući značajan i alarmantan broj novih sajber terorista. [11] Ovu činjenicu treba razumevati u kontekstu one stvarnosti koja nam je svima poznata, a tiče se socijalizacije unutar sajber prostora. U tom svetu potraga za sadržajima od interesa daleko je lakša od iste na bilo kom drugom mestu sa kog bi se potražile pohranjene informacije. Dakle, sama struktura sajber prostora omogućava razvoj sajber terorista od političkih stavova, do praćenja svih dešavanja, samoedukacije i razvoja sajber veština, do finalnog izvođenja napada. Sada, po prvi put u istoriji imamo nezapamćen fenomen da običan civil može da

[10] https://threatmap.checkpoint.com/ pristupljeno 5.4.2021.

[11] La Guardia, A. (august 10. 2005): *Al Qaeda Places Recruiting Ads*, The London Telegraph.

postigne potpuno samostalno ono znanje neophodno za sajber napad, da ista ta osoba može da prikupi informacije i konačno potpuno samostalno izvrši sajber terorizam na sajber prostoru ne pomerajući se sa svog radnog prostora. Ovakva činjenica upućuje na logičnu zabrinutost jer onda kada je neprijatelj nesagledliv, on je onda svuda pretpostavljen. A kada je opasnost na svakom koraku, potrebna su ogromna materijalna i resursna sredstva da bi se omogućila adekvatna armija sajber vojnika koji će štititi sisteme neprekidno. Ako je još 2003.godine uočena realna opasnost od sajber terorizma ukazujući na to da teroristi mogu da ovladaju novim tehnologijama i prodru u sajber prostor Vlada, Vladinih sektora, banki, bezbednosnih sistema i tajnih podataka, danas je to jasna realnost sa kojom se suočavamo na više stotina milionskom broju napada samo u jednom danu.[12] Zbog ovoga sam internet nastavlja da bude polje terorističkih pretnji i izazova za službe bezbednosti.

Zaključak

Ukoliko se osvrnemo na dešavanja samo od početka COVID-19 pandemije, biće nam jasno da je sajber prostor postao osnovni prostor za rad svih vladinih institucija i privatnih kompanija. Upravo proglašenjem pandemije značaj interneta je dostigao alarmantnu tačku sa koje vidimo da ne bismo mogli ni na koji način da funkcionišemo ni u svom radnom, ni u svom privatnom prostoru. Ovaj aspekt je pojačao svest o opasnostima koje su prisutne od strane terorista u sajber prostoru kao prostoru koji je formulisan za ne samo komunikaciju i bezazlene sadržaje, zabavu i društvene ‚mreže, već i pohranjivanje veoma proverivih informacija, podatka i sadržaja koji su od koristi sajber terorizmu kao pošasti našeg doba i to u sve većoj meri. Onda kada je sajber prostor postao zona terorizma suočili smo se sa sajber terorizmom. Ova pošast ima inerciju razvoja jednako kao tehnologija jer danas veoma jasno uviđamo transparentnost sajber terorizma i opasnosti koju nose sa sobom teroristi na internetu. Posao službi bezbednosti je nedvosmislen i ovoga puta pored kontunuirane odbrane države su suočene sa značajnim napretkom tehnologije koja mora biti ispraćena stručnjacima za sajber sisteme, inženjerima i ekspertima za bezbednost sistema kako bi se vlade, državne institucije, ekonomija, banke i bezbednost građana očuvali. Sajber terorizam pogađa sve segmente života od obrazovanja do medicine i kada znamo da je terorizam ovladao veštinom hakovanja na državama je da obezbede maksimalna sredstva da svojim zaposlenima daju najadekvatnije obrazovanje u ovoj oblasti jer ona ima neprekidno narastanje, a onda kada se ukaže prilika za napad svaka vlast ma gde na svetu treba da bude svesna da će se taj napad i realizovati. Uslovi pandemije ukazali su pun značaj naše zavisnosti od interneta, a

[12] Cullather, N. (Winter 2003):"*Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar*", Intelligence and National Security, Vol.18, No.4, pp.141–154.

samim time i opasnost koja preti sistemima koji nisu adekvatno obezbeđeni time potencijalno ili konkretno devastirajući ne samo državne institucije, već sve sadržaje do kojih mogu da dođu tokom hakerskog napada, a u cilju sprovođenja svojih terorističkih agendi. Svet kom pripadaju vlade svih država sveta ukoliko želi da pobeđuje terorizam moraće u sajber utrci da bude neprekidno nekoliko koraka ispred terorista jer tehnologija je oružje koje koriste najinteligentniji i najuigraniji i pravovremeno informisani akteri našeg sajber doba.

Literatura:

- Cullather, N. (Winter 2003):"*Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar*", Intelligence and National Security, Vol.18, No.4
- Flemming, P., Stohl, M. (2001): "*International Scientific and Professional Advisory Council of the United Nations*", in Crime Prevention and Criminal Justice Program Countering Terrorism Through International Cooperation, Alex P. Schmid (ed.), ISPAC, Vienna
- La Guardia, A. (august 10. 2005): *Al Qaeda Places Recruiting Ads*, The London Telegraph
- Mockaitis, T. R. (2007): *The «new» terrorism: myths and reality*, Westport, Conn: Praeger Security Internacional.
- Venzke, B., Ibrahim, A., (2003): *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets*, Tempest Publishing, LLC, Alexandria..
- Sullivant, J. (2007): *Strategies for protecting critical infrastructure assets,* Hoboken, NJ: Wiley.
- Toffler, A., Toffler,H. (1993):*War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown and Company, Boston
- https://www.bbc.com/future/article/20140516-i-operate-on-people-400km-away
- https://www.appknox.com/blog/famous-child-hackers
- https://www.bbc.com/news/world-europe-39907965
- https://threatmap.checkpoint.com/

Sanja Klisarić

UDC 343.533::004
004.738.5.056.53

DOI: 10.5937/MegRev2102247K
Expert article
Received 14.04.2021.
Approved 20.04.2021.

CYBER TERRORISM AS A TRIGGER FOR THE GROWING NEED FOR SECURITY OF THE SYSTEM FROM THE DANGERS THAT COME FROM THE INTERNET

Summary: *In a world of increasingly intense cyber content that relies on new technologies, the security of all systems is at risk. This article will present the danger and security options in order to protect not only data but also the entire system connected to the new technologies. Also, the importance of persons dealing with online security issues will be emphasized. The analysis of the content reveals the possibility for prediction that is presented in the paper, and connected with the conclusion that technology will develop more and more, and thus the danger of cyber attacks will be more and more intense. The paper focuses on the essence of the defense against terrorism that is necessary on the Internet. This indicates those defense options that are in line with the roles of those in charge of Internet security as an open field for terrorist cyber attacks.*

Keywords: *Cyber attack, Cyber terrorism, Internet security, Internet defense, Terrorists, Danger of internet security systems*