FBIM Transactions
DOI 10.12709/fbim.07.07.02.01

MJERE PREVENCIJE I SIGURNOSNE POLITIKE PROTIV CYBER TERORIZMA

PREVENTION MEASURES AND SECURITY POLICIES AGAINST CYBER TERRORISM

Vladica Babić
Visoka Škola Logos, Mostar, Bosna i Hercegovina

JEL kategorija rada: **L86**

Apstrakt

Cyber terorizam predstavlja možda i najveću prijetnju nacionalnoj i međunarodnoj sigurnosti država od vremena stvaranja oružja za masovno uništenje. Kako države i njihova privreda postaju sve umreženiji, uglavnom putem informacijskih mreža, te Interneta, i na međunarodnom financijskom sustavu globalne trgovine, učinci cyber terorističkih napada će imati sve veći utjecaj. Isto tako, važno je kako će cyber teroristi steći iskustvo u narušavanju nacionalne sigurnosti i otvorenosti informacijske infrastrukture, njihovi napadi će vjerojatno postati sve uspješniji. Iako su države, privatne industrije i međunarodne organizacije učinile značajne napore za povećanje međunarodne suradnje, još puno toga treba biti učinjeno. Pri tome moramo shvatiti da je, s obzirom na temeljne slabosti u strukturi Interneta, potrebno načiniti i dodatne napore kako bi u potpunosti spriječili cyber terorizam. U vezi s tim, a i u svrhu otkrivanja ovakve prijetnje na pravi način, neophodna je obavještajna i sigurnosna suradnja, kako bilateralno tako i multilateralno, uključujući i razmjenu iskustava i relevantnih informacija iz ovog područja.

Ključne riječi: *Terorizam, cyber kriminal, prevencija, sigurnosna politika.*

Abstract

Cyber terrorism is perhaps the biggest threat to the national and international security of states since the time of mass destruction. As the state and their business become more and more networked, mostly through information networks, the Internet, and the international financial system of global trade, the effects of cyber-terrorist attacks will have an increasing impact. Likewise, it is important that cyber terrorists gain experience in disrupting national security and openness of information infrastructure, and their attacks will probably become more successful. Although the state, private industry, and international organizations have made significant efforts to increase international co-operation, much more needs to be done. We must realize that, given the fundamental weaknesses in the structure of the Internet, further efforts are needed to fully prevent cyber terrorism. In this respect, and in order to detect this threat in the right way, intelligence and security cooperation, both bilaterally and multilaterally, including exchange of experience and relevant information in this area is necessary.

Keywords: *Terrorism, cybercrime, prevention, security policy.*

Adresa autora:
Vladica Babić
vladica.babic@net.hr

1 UVOD

Terorizam je jedan od najsloženijih, najizazovnijih i najopasnijih političko-sigurnosnih fenomena današnjice. Cyber terorizam, kao njegov poseban oblik zahtijeva specifičnu pozornost pri njegovom suzbijanju. Kao spoj politike i nasilja, kao uporaba terora (nasilja, zastrašivanja), i pri tome još uključenost u suvremene tehnologije, cyber terorizam je uvijek u cilju udara na državni, politički i društveni sustav, te građane jedne države. Stoga odgovor na cyber terorizam i sam terorizam zahtijeva ukupnost koordiniranog državnog i društvenog djelovanja. Da bismo se uspješno branili od cyber terorizma potrebne su mjere preventivnog djelovanja, mjere suzbijanja cyber terorizma, mjere zaštite od cyber terorizma, saniranje posljedica nastalih djelovanjem cyber terorizma, izgradnja pravnog sustava za borbu protiv cyber terorizma, zatim edukacija, osposobljavanje i trening za borbu protiv cyber terorizma, te provođenje koordinacije i međunarodne suradnje.

Donošenje ključnih dokumenata kao što su Strategija, Akcioni planovi, Konvencije, te drugi pravni akti po pitanju rada na prevenciji i suzbijanju cyber terorizma predstavljaju upravo takav pristup i okvir djelovanja svake države prema ovoj pojavi. Sustavni pristup u takvim dokumentima bi sigurno smanjio mogućnost pojave, djelovanja i u dobroj mjeri pomogao u suzbijanju cyber terorizma. Ove mjere predstavljaju detaljno razrađene postavke i aktivnosti koje bi svakako trebale biti provedene. Pri tome, pod pojmom cyber terorizam svrstavamo osmišljenu, sustavnu, namjernu uporabu nasilja, ili prijetnje nasiljem protiv ljudi i/ili materijalnih dobara, uključujući i informacijske mreže i sredstva, kao sredstvo za izazivanje straha ili usmjerenog protiv njega, a sve unutar neke etničke ili vjerske zajednice, javnosti, države ili cijele međunarodne zajednice, u cilju ostvarenja političkih, vjerskih, ideoloških ili društvenih ciljeva. Jedna od glavnih karakteristika cyber terorizma je da se za djelovanje koristi cyber prostor, da ga prakticiraju najčešće nedržavne organizacije ili grupe, koje mogu imati potporu izvana od strane neke države ili država, a često i od organizacije čija javno deklarirana namjera i ciljevi nemaju veze s terorizmom, ali svojim prikrivenim ciljevima i djelovanjem služe kao potpora terorističkom djelovanju. Cyber terorizam je određen namjerom izazivanja razornih političkih i psiholoških posljedica koje mogu značajno nadilaziti sam cilj nekog pojedinog terorističkog čina, te namjerama onih koji pribjegavaju stvaranju klime bezvlašća ili izazivanja represivnog i neselektivnog odgovora vlasti s ciljem njenog kompromitiranja u očima javnosti i opravdanja terorističkih sredstava i namjera.

2 STANJE U BOSNI I HERCEGOVINI

Bosna i Hercegovina je ratificirala Konvenciju o cyber kriminalu („Službeni glasnik BiH – Međunarodni ugovori“, br. 6/206) i Dodatni protokol Konvenciji o cyber kriminalu, a u svezi s kažnjavanjem djela rasističke i ksenofobske prirode počinjenih putem računalnih sustava („Službeni glasnik BiH – Međunarodni ugovori“, broj 6/206) 2006. godine. Kada je u pitanju implementacija Konvencije u kaznene zakone, posebna napomena je da se u Bosni i Hercegovini primjenjuju četiri kaznena zakona s obzirom na podijeljenu nadležnost u propisivanju kaznenih djela između države i entiteta. Kazneni zakon Bosne i Hercegovine („Službeni glasnik BiH“, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15) sadrži kaznena djela kojima se štite vrijednosti čija zaštita je u isključivoj nadležnosti države, dok su u kaznenim zakonima entiteta i Brčko Distrikta propisana sva ostala kaznena djela uključujući i kaznena djela iz domena cyber kriminala. Zakoni o kaznenom postupku, kojih je u Bosni i Hercegovini četiri, su kao i kazneni zakoni donekle usklađeni sa kazneno procesnim odredbama iz Konvencije.

Na državnom nivou Bosne i Hercegovine ne postoji strategija ili akcioni plan za borbu protiv cyber kriminala, no u Strategiji za borbu protiv organizovanog kriminala u Bosni i Hercegovini (2017 – 2020) i Strategiji Bosne i Hercegovine za prevenciju i borbu protiv terorizma (2015 – 2020) utvrđene su mjere za borbu u oblasti računarskog kriminaliteta, a koje se ogledaju u:

I. donošenju strateških dokumenata u borbi protiv visokotehnološkog kriminala u Bosni i Hercegovini,
II. poboljšanju suradnje sa privatnim sektorom u borbi protiv računarskog

kriminala kroz razvijanje konkretnih sporazuma,

III. podizanju svijesti vezano za korištenje informacionih tehnologija,

IV. edukaciji policijskih službenika i tužitelja o savremenom visokotehnološkom kriminalu i njihovim trendovima i modusima, te pojavnim oblicima,

V. kontinuiranom unaprjeđenju tehnologija koje koriste agencije za provedbu zakona u Bosni i Hercegovini,

VI. opremanju i razvoju sigurnosti računarskih sistema u institucijama Bosne i Hercegovine,

VII. provedbi međunarodnih direktiva i najboljih praksi u ovoj oblasti,

VIII. jačanju suradnje sa nevladinim organizacijama u oblasti cyber sigurnosti i zaštite autorskih prava,

IX. potpunoj implementaciji međunarodnih standarda koji se odnose na uspostavljanje Tima za odgovor na računarske incidente (*Computer Emergency Response Team*, CERT) u Bosni i Hercegovini i mehanizama za praćenje i suzbijanje zloupotrebe Interneta u terorističke svrhe.

Sukladno sa prethodno navedenim stanjem, na 80. sjednici Vijeća ministara BiH, održanoj 10. 11.2016. godine, na prijedlog Ministarstva sigurnosti BiH (MSBiH), donijeta je odluka o uspostavi Interresorne radne grupe, koja će u ime Bosne i Hercegovine biti zadužena za provođenje projekta Vijeća Evrope i Evropske unije koji za cilj ima izgradnju kapaciteta zemalja Jugoistočne Evrope u borbi protiv cyber kriminala - iPROCEEDS. Evropska unija i Savjet Evrope su u januaru 2016. godine potpisali ugovor o regionalnom projektu koji će trajati 42 mjeseca. Članovi tima su predstavnici svih zainteresovanih strana u ovoj oblasti, tj. ministarstva pravde nadležnog za predmetnu kaznenu oblast, predstavnika tužilaštva, policije, financijsko obavještajnog odjeljenja i drugih. Također, na istoj sjednici je Vijeće ministara BiH dalo podršku Ministarstvu sigurnosti BiH i policijskim tijelima da se u okviru IPA 2017 državnog paketa zatraži pomoć Evropske unije u daljem razvoju i jačanju kapaciteta nadležnih tijela u Bosni i Hercegovini u oblasti borbe protiv cyber kriminala. Dodatno, MSBiH vrši koordinaciju i kontakt tačka je za: (I) implementaciju dodatnih mjera za izgradnju povjerenja u oblasti cyber sigurnosti (OSCE), (II) International Telecommunication Union (ITU) Global Cybersecurity Index (GCI), te (III) NATO Science for Peace and Security Programme – specijalizirani treninzi cyber sigurnosti za državne službenike Bosne i Hercegovine.

3 CYBER TERORIZAM U BOSNI I HERCEGOVINI I NJEN ZAKONDAVNI OKVIR

Cyber terorizam, odnosno *zlouporaba Interneta u terorističke svrhe* predstavlja jedan od najopasnijih uzroka narušavanja globalne sigurnosti. U svijetu Internet prostora aktivnosti terorističkih organizacija se svode na traženje talenata koji su već osposobljeni za djelovanje u cyber prostoru.

„*Cyber terorizam je svaki oblik terorističke aktivnosti u sprezi sa cyber tehnologijom.“* Prema autoru Babiću, Cyber terorizam se isto tako može definirati i kao „*klasična teroristička aktivnost uz uporabu kompjutora i kompjutorskih sustava*." (Babić, 2009, str. 58)

Preporuke međunarodne zajednice u borbi protiv terorizma, koje je Bosna i Hercegovina,, implemenatirala u svoj zakonodavni okvir na državnom nivou, odnose se na kaznena djela vezana za terorizam.[1]

Različitosti od drugih kaznenih zakona i specifičnosti propisanih kaznenih djela terorizma u Kaznenom zakonu Bosne i Hercegovine su navedena u glavi XVII, pod naslovom *Kaznena djela protiv čovječnosti i vrijednosti zaštićenih međunarodnim pravom*. Pored kaznenih djela koja su u oblasti ratnog zločina i humanitarnog prava, u toj glavi nalaze se i djela trgovine ljudima, djela koja se odnose na međunarodne službenike, piratstva i otmice, te kaznena djela terorističkih aktivnosti propisana za obavljanje sljedećih radnji:

- Terorizam (čl.201. KZ BiH),

[1] Kazneni zakon Bosne i Hercegovine (Sl. gl. BiH br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14)

- Financiranje terorističkih aktivnosti (čl.202. KZ BiH),
- Javno poticanje na terorističke aktivnosti (čl.202.a KZ BiH),
- Vrbovanje radi terorističkih aktivnosti (čl.202.b KZ BiH),
- Obuka za izvođenje terorističkih aktivnosti (čl.202.c KZ BiH),
- Organiziranje terorističke grupe (čl.202.d KZ BiH),
- Protuzakonito formiranje i pridruživanje stranim paravojnim ili parapolicijskim formacijama(čl.162.b KZ BiH),

Pojedinačna objašnjenja svakog od nabrojanih kaznenih djela su rečena i kroz temeljne odrednice članaka KZ BiH, na početku KZ BiH je i čl.1. čijim je st.21. propisano što to čini terorističku grupu prema KZ BiH. Tako tim stavkom se kaže da je: "*Teroristička grupa organizirana grupa koju čine najmanje tri osobe, koja je formirana i djeluje u određenom vremenskom periodu s ciljem izvršenja nekog od kaznenih djela terorizma.*" Također, istim člankom st.22. KZ BiH podrobnije se određuje što to čini osoba koje sudjeluje u aktivnostima terorističke grupe, te tako: „*Učestvovanje u aktivnostima terorističke grupe je pristupanje ili uključivanje u aktivnosti terorističke grupe ili pružanje informacija ili materijalnih resursa ili financiranje njenih aktivnosti na bilo koji način, sa znanjem da će takvo učešće doprinijeti kriminalnim aktivnostima terorističke grupe.*"

U zakonodavstvu Bosne i Hercegovine nema posebne odredbe vezane za kazneno djelo cyber terorizma, ali postoji mogućnost za sankcioniranje kroz kaznena djela čl.201.st.5.toč.d), gdje se: "*s ciljem ozbiljnog zastrašivanja stanovništva, ili prisiljavanja organa vlasti BiH ili vlade druge zemlje ili međunarodne zajednice da što izvrši ili ne izvrši, ili ozbiljne destabilizacije ili uništavanja temeljnih ustavnih, političkih, gospodarskih ili društvenih struktura BiH, druge zemlje ili međunarodne organizacije, počini jedno od sljedećih djela koje može ozbiljno naštetiti državi ili međunarodnoj organizaciji…uništenje državnih ili javnih…uključujući i informacijski sustav*" čime se uvodi teroristično djelovanje kroz informacijski sustav.

Također po pitanju zakona o kaznenom postupku može se reći da počinitelj kaznenog djela čl.162b. u st.3. stoji da "nabavlja ili osposobljava sredstva, uklanja prepreke, stvara plan ili se dogovara s drugima ili vrbuje drugoga ili poduzme bilo koju drugu radnju kojom se stvaraju uvjeti za direktno počinjenje ovog kaznenog djela," isto tako u st.4. istog članka onaj koji "javno, putem sredstava informiranja, distribuira ili na bilo koji drugi način uputi poruku javnosti, koja ima za cilj poticanje drugog na izvršenje ovog kaznenog djela," se može inkriminirati kao djelo cyber terorizma.

4 MJERE PREVENCIJE CYBER TERORIZMA

U tom kontekstu, mjere za borbu protiv cyber terorizma sastoje se od dva stuba kojima bi se taj problem znatno smanjio ili u dobroj mjeri suzbio. Kao prvi stup navodi se *Prevencija cyber terorizma* koja se odnosi na stvaranje takvih političkih, društvenih i ekonomskih okolnosti koje uklanjaju preduvjete nastanka i širenja cyber terorizma u svim segmentima njegove pojave. Ove mjere prevencije prvenstveno se odnose na:

- onemogućavanje promoviranja i pozivanja na terorizam putem informacijskih sustava;
- prepoznavanje i eliminacija pojava koje uvjetuju nastanak cyber terorizma na lokalnoj razini i međunarodnoj razini;
- onemogućavanje širenja ekstremističkih ideologija, te povećanje razumijevanja i tolerancije društva na nacionalnoj i međunarodnoj razini;
- koordinacija i suradnja svih državnih i međunarodnih institucija usmjerenih na eliminiranje sociooloških, političkih i ekonomskih izvora koji uvjetuju nastanak cyber terorizma.

Suzbijanje cyber terorizma podrazumijeva poduzimanje mjera i postupaka usmjerenih protiv stvaranja, širenja i djelovanja terorističkih mreža i organizacija u cyber prostoru, kao i blagovremeno otkrivanje planiranja, pripremanja, organiziranja i/ili provođenja aktivnosti s obilježjima cyber terorizma, te aktivnosti se ogledaju kroz:

- organizacijsko i logističko djelovanje,
- iskorištavanja teritorija BiH za uspostavljanje i rad cyber terorističkih grupa, njihovu obuku i educiranje,
- kontrola, nadzor i evidencija:
- prolaska i dolaska osoba sumnjive i potencijalne terorističke prošlosti,
- prijenosa i nabave oružja i opreme, te drugih materija namijenjenih potencijalnim cyber terorističkim aktivnostima,

- prikupljanja financijskih sredstava ili pomaganja na drugi način cyber terorističkih organizacija i pokreta,
- onemogućavanja vrbovanja i novačenja pojedinaca za cyber terorističke organizacije i pokrete,
- druge kriminalne aktivnosti u vezi sa cyber prostorom.

5 MJERE SIGURNOSNE POLITIKE PROTIV CYBER TERORIZMA

Osnovne mjere suzbijanja terorističkih aktivnosti koje se mogu dovesti u vezu sa fenomenom cyber terorizma su ostvarive kroz dosljednu primjenu nacionalnog zakonodavstva i propisanih kaznenih djela terorizma i njemu sličnih djela, kao i onim djelima za koja nisu propisane norme unutar državnog zakonodavstva, ali postoje međunarodne preporuke za njihovo donošenje, te ratifikaciju i usvajanje univerzalne nadležnosti za navedena djela. Unutar postojećeg zakonodavstva potrebno je uskladiti mjere koje se tiču:

- onemogućavanja organizacijskog i logističkog djelovanja terorističkih organizacija i pojedinaca u cyber prostoru;
- sprječavanja korištenja cyber prostora unutar teritorija države za organiziranje, uspostavljanje i djelovanje terorističkih grupa, njihovu obuku i uvježbavanje, te pojedinaca i subjekata koji se dovode u vezu s terorizmom, čije je djelovanje usmjereno protiv država i/ili međunarodnih organizacija;
- onemogućavanja svih oblika regrutiranja i mobilizacije terorističkih grupa putem cyber prostora;
- sprječavanja kriminalne aktivnosti koje mogu biti izravno i neizravno povezane s terorizmom prvenstveno zbog zlouporabe cyber prostora;
- onemogućavanja prijenosa i nabavke oružja, eksploziva, te tehničkih i drugih sredstava namijenjenih potencijalnim terorističkim aktivnostima;
- sprječavanja korištenja sredstava za masovno uništavanje, te roba vojne i druge namjene u terorističke svrhe;
- onemogućavanja financiranja, prikupljanja sredstava i pomaganja na bilo koji način terorističkim organizacijama ili pojedincima koji se dovode u vezu s terorizmom;
- zaštitite od terorističkih djelovanja svih materijalnih i nematerijalnih dobra države: građana, imovine, pravnih subjekata, državnih institucija, svojih i stranih diplomatskih predstavništava, prometne i informacijske komunikacije, te državne granice i pravnog poretka;
- definiranja i provođenja programa osposobljavanja, obuke i treninga stanovništva, zaposlenika državne uprave za protuterorističko djelovanje u području prevencije i pojedinih elemenata zaštite;
- definiranja i provođenja obrazovnih i studijskih programa na temu upravljanja krizama, profesionalnog usavršavanja, te stvaranja organizacijskih i funkcionalnih preduvjeta za znanstvena istraživanja, znanstveni i stručni rad u području cyber terorizma.

6 ZAKLJUČAK

Navedenim, generalno se može reći kako su kaznena djela terorizma u bosanskohercegovačkom zakonodavstvu detaljno propisana sukladno međunarodnim preporukama, te da se većinom inkriminacija grupiranih u vezi s terorizmom može izreći sankcija za djela počinjena kao djela cyber terorizma, iako za isto nema posebno propisane norme. Preporuka je uvođenje već do sad više puta navedene univerzalne nadležnosti za progon počinitelja djela cyber terorizma. Također dopunu KZ BiH bi trebalo opisati kroz odrednicu koja se veže za *javno mjesto*, što bi se odnosilo i na internet prostor i društvene mreže, jer bi se time u značajnoj mjeri omogućilo djelovanje u ranoj fazi pojave cyber terorizma čime bi se preventivno djelovalo na širenje ove pojave u BiH i svijetu.

CITIRANA DELA

Babić, V. (2009). *Kompjuterski kriminal*, Sarajevo, Rabic.

Babić, V. (2016). *Cyber terorizam - suvremena sigurnosna prijetnja.* Vitez.

Kazneni zakon Bosne i Hercegovine (Sl. gl. BiH br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14)

Datum prve prijave: 18.09.2019.
Datum prijema korigovanog članka: 07.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Babić, V. (2019, 10 15). Mjere prevencije i sigurnosne politike protiv cyber terorizma. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 1-6. doi:10.12709/fbim.07.07.02.01

*Style – **Chicago** Sixteenth Edition:*

Babić, Vladica. 2019. "Mjere prevencije i sigurnosne politike protiv cyber terorizma." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 1-6. doi:10.12709/fbim.07.07.02.01.

*Style – **GOST** Name Sort:*

Babić Vladica Mjere prevencije i sigurnosne politike protiv cyber terorizma [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 1-6.

*Style – **Harvard** Anglia:*

Babić, V., 2019. Mjere prevencije i sigurnosne politike protiv cyber terorizma. *FBIM Transactions,* 15 10, 7(2), pp. 1-6.

Style – **ISO 690** Numerical Reference:

Mjere prevencije i sigurnosne politike protiv cyber terorizma. **Babić, Vladica.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 1-6.