FBIM Transactions
DOI 10.12709/fbim.07.07.02.12

# RADIKALIZACIJA VISOKOTEHNOLOŠKOG TERORIZMA

## THE RADICALIZATION OF HIGH-TECH TERRORISM

**Ivica Petrović**
Akademija za nacionalnu bezbednost, Beograd, Srbija

**Dragana Trnavac**
Poslovni i pravni fakultet, Univerzitet UNION-Nikola Tesla, Beograd, Srbija


JEL kategorija rada: **L86**

***Apstrakt***

*Visokotehnološki terorizam je rizik još od pojave Interneta. Tehnologija se razvijala brzim tempom samim tim i rizik i uticaj visokotehnološkog terorizma. Važno je da postoje sigurni i ažurirani mehanizmi za ublažavanje rizika visokotehnološkog terorizma, uz međunarodnu saradnju radi daljeg unapređenja istrage i informacija. Ovaj rad govori o mehanizmima kao što su bezbednost aplikacije, bezbednosne politike, razumevanje obrazovanja programi, međunarodna saradnja, nadgledanje i veštačka inteligencija (VI), praćenje, korišćenje i ometanje pristupa. Implementacija svih mehanizama omogućava računarske mreže i sisteme koji su manje ranjivi zato što svaki mehanizam poseduje odvojene funkcije za borbu protiv visokotehnološkog terorizma. Kao rezultat toga, ovo istraživanje dokazuje pozitivnu povezanost između prepoznatih mehanizama i percipiranog rizika od visokotehnološkog terorizma. Bilo je različitih inicijativa, koje su pokrenuli nadležni organi iz celog sveta, kako bi se osiguralo da je pretnja od visokotehnološkog terorizma pod kontrolom. Međutim, pretnja od visokotehnološkog terorizma neprestano raste zbog stalnog razvoja platformi zasnovanih na Internetu. Tako, sprovođenje zakona, politike, prakse i neophodnih mera trebalo bi da se nastavi sa savremenim razvojem kompjuterskih tehnologija.*

***Ključne reči:*** *visokotehnološki terorizam, veštačka inteligencija (VI), nadgledanje, korišćenje i ometanje*

***Abstract***

*High-tech terrorism has been a risk since the advent of the Internet. Technology has evolved at a rapid pace, thus the risk and impact of high-tech terrorism. Importantly, there are secure and up-to-date mechanisms to mitigate the risks of high-tech terrorism, with international cooperation to further advance investigations and information. This paper discusses mechanisms such as application security, security policies, education understanding of programs, international collaboration, monitoring and artificial intelligence (VI), monitoring, use and disruption of access. The implementation of all mechanisms is facilitated by computer networks and systems that are less vulnerable because each mechanism has separate functions to*

*Adresa autora zaduženog za korespodenciju:*
***Dragana Trnavac***
*draganatrnavac@gmail.com*

*counter high-tech terrorism. As a result, the goals for this research prove a positive correlation between the mechanisms identified and the perceived risk of high-tech terrorism. There have been various initiatives, introduced by authorities around the world, to ensure that the threat of high-tech terrorism is under control. However, the threat of high-tech terrorism is steadily rising due to the constant development of Internet-based platforms. Thus, the implementation of the law, policies, practices and necessary measures should continue with the modern development of computer technologies.*

***Keywords**: high-tech terrorism, artificial intelligence, surveillance, utilization, interference.*

## 1 UVOD

Visokotehnološki terorizam je postao popularan poslednjih godina, posebno sa brzo razvijajućom tehnologijom i povećanje zavisnosti ljudskog roda od Interneta i društvenih medija. Iako je visokotehnološki terorizma bilo kog oblika, međunarodno priznat kao glavni rizik, ne postoji glavna definicija, ipak čini se da je opšteprihvaćena ili univerzalna definicija visokotehnološkog terorizma (Dogrul, M., Aslan, A., & Celik, E., 2011) ovu koju navodimo u nastavku. Mnogi istraživači su citirali definiciju Deninga (2000); koji visokotehnološki terorizam opisuje kao "*konvergenciju sajber prostora i terorizma gde su nezakoniti napadi i pretnje napadima protiv računara, mreža i informacija sačuvanih u njima; vrše se zastrašivanjem ili prisiljavanjem vlade ili njenih građana na unapređenje političkih ili društvenih ciljeva koje bi trebalo da rezultira nasiljem nad osobama ili imovini ili bar da nanese dovoljno štete generišući strah*". Iako ovo čini razumnu definiciju visokotehnološkog terorizma u tom trenutku, presudni su međunarodni napori koji preispituju opseg i razvoj mehanizama koji stoje iza visokotehnološkog terorizma da se to osigura zakonima tako da sami po sebi ne stvaraju rupe tj. prostor za visokotehnološkim terorizmom (Denning, & Dorothy E., 2000).

Gore navedena definicija implicira da je visokotehnološki terorizam važi samo ako ošteti poverljivost, integritet i dostupnost (CIA) računara, mreža i informacije koje su sačuvane; kao i radnje koje izazovu nasilje ili neku vrstu šteta. Međutim, u savremenom okruženju i teroristi koristite sajber-prostor i elektronske uređaje za komunikaciju, planiranje, vršenje napade, pribavljanje finansiranja, nabavku oružja, obaveštajno okupljanje i pristalice terorista. 2000. godine pojedinac je hakovao i preuzeo odgovornost za australijski otpad sistem upravljanja, Maroochy Shire i na daljinu ispraznio milione galona sirove kanalizacije (Prasad, 2012). Sve veći broj terorističkih grupa poput islamske Država Irak i Sirije (ISIS ) i Al-Kaida, iskoristili su to, Internet kao medij za promociju njihovog uzroka i ponašanja terorističke operacije (Prasad, 2012).. Ove grupe su uspešno privukle veliki broj sledbenika, donatore i pristalice zbog snažne propagande; posebno posezanje za mladima koji žude za avanturama i dokazivanjem. Grupe koriste mnogo različitih frontova da sakriju svoj pravi identitet i aktivnosti, uključujući korišćenje anonimnih zaštita dubokog i mračnog spleta, koja se krije iza verskih i drugih neprofitnih tela itd. Takođe je isprepleteno sa drugim nezakonitim aktivnostima uključujući pranje novca, korupciju i organizovani kriminal. Ovo izaziva dalje dileme odakle se zločin može počiniti odnosno bilo koji deo sveta, skriven ispod mnogih slojeva aktivnosti i pojedinaca. Dakle, neophodno je da svi načini na koji se vrši ovaj zločin nadgleda se i ublažava. Iako su vlade pojačale mere bezbednosti uključujući praćenje putem Interneta, bilo je mnogo prepreka u njihovim nastojanjima. Ali i ostali priznaju da je visokotehnološki terorizam, obično pogrešno tumačen sa drugima slične visokotehnološke pretnje zbog ograničene grane znanja, a ismevanje opasnosti koju predstavlja povećava rizik od visokotehnoloških napada. Sukobni ili suženi zakoni и propisi mogu da poremete istrage i parnice. Odredbe o zaštiti privatnosti i zaštite podataka kompanije kao što su WhatsApp, Apple i druge koje koriste, prouzrokovalo je šifriranje radi zaštite privatnosti njihovih korisnika što mnogo ometa istrage i sudske sporove i proces. Zabrinutosti zbog strogog zakonodavstva takođe mogu izazvati nelagodnost među javnošću. 2017. godine Amber Rudd, državna sekretarka Velike Britanije izrazila je nameru da promeni zakon tako da se poveća kazna od 10 godina na 15 godina zatvora za osobe koje više puta gledaju teroristički sadržaj na mreži, iako sa dovoljnim merama za zaštitu članova javnost uz odbranu razumnog

izgovora (Prasad, 2012). U vestima se navodi i slučaj u kojem osumnjičeni nije mogao biti optužen za terorizam, samo zato što mu je bio potreban materijal da se preuzme i sačuva, dok je kod osumnjičenog pronađen samo striming video snimaka bombi. Isto tako, vesti o povećanom broju korisnika Onion-a Ruter (TOR) u poređenju s drugim pregledačima zbog privatnosti, zabrinutosti i sklonosti anonimnosti, takođe povećavaju rizik visokotehnološkog terorizma. TOR je takođe kapija Mraka i Dubinski web, uključujući aspekte servisa kriminala kao usluge (CaaS) i drugi organizovani zločini. Povećana upotreba kripto valute takođe pomažu kretanje i pranje fondovi. Obrazovanje i izlaganje su neophodni da bi se ublažio rizik. Sve veći broj globalnih prodora interneta, nedostatak bezbednosne svesti kod korisnika i porast broja zavisnost od internet komunikacija smanjuje mogućnosti borbe protiv visokotehnološkog terorizma (Jalil, 2003). Odgovorni organi neprestano su težila tome osigurati, da je pretnja pod kontrolom i da ne utiče na građane ili državu (Prasad, 2012). Vladini sektori iz celog sveta inicirali su nove sisteme, programe, politike, stroge zakone i razne druge akcije u cilju borbe protiv pretnje od visokotehnološkog terorizma. Međutim, to je izazovna bitka koju stalno treba ažurirati nadgledati, kao i same pretnje koje se neprestano razvijaju i rastu. Vlade, kompanije i pojedinci trebaju biti oprezni jer pretnje mogu uticati na njih same, odnosno preduzeća, informacije, privatnost i na kraju njihova sigurnost, koju uzrokuju njihove ranjive računarske mreže i sisteme, kao i zaposleni ili prikriveni prodavci. Stoga ovaj rad procenjuje percepciju dobro upućenih članova javnosti o riziku od visokotehnološkog terorizam u skladu sa raznim naporima i mehanizmima na raspolaganju za borbu protiv ovog zločina. Da bismo pružili više, diskusija je zasnovana na nalazima ovog istraživanja. Ovaj rad je organizovan na sledeći način: Odeljak 2 govori o relevantnoj literaturi, odeljak 3 govori o merama za ublažavanje rizika od visokotehnološkog terorizma, a zatim sledi Odeljak 4 koji govori o akcionom planu Republike Srbije u borbi protiv visokotehnološkog kriminala, odeljak 5 sadrži statističke trendove u oblasti visokotehnološkog kriminala Republike Srbije, odeljak 6 celokupnu perspektivu ovog rada.

## 2 PREGLED LITERATURE

Percipirani rizik od visokotehnološkog terorizma: Visokotehnološki terorizam leži između tanke linije postajanja virtualne bombe, ali nije tako opasna po život kao stvarna bomba . Rizik od visokotehnološkog terorizma možda neće izgledati ozbiljno, ali u stvari je stvar zaštita nacionalne sigurnosti. Biti više politički motivisan, visokotehnološki terorizam je usmeren ka nanošenju štete kritičnoj infrastrukturi države na koju se indirektno odnosi uticaj na širu javnost u smislu ometanja finansijske pomoći i komercijalnu infrastrukturu, preuzimajući kontrolu odbrane, pa čak i pristup medicinskoj dokumentaciji Zbog političke koordinacije, narod je suočen efektima visokotehnološkog terorizma u stvarnosti. Ovi poremećaji su dovoljni da stvore strah prema javnosti i time omogućava visokotehnološkim terorističkim grupama da daljinski upravljaju operacijama države (Alqahtani, n.d.). Na primer, napadi mogu uzrokovati prekide u snabdevanju vodom ako visokotehnološki teroristi imaju kontrolu nad branama, prouzrokujući nestašicu vode sami tim i patnju građana. Iako možda ne zvuči kao ozbiljno pitanje i prilično je daleko dostignut, ali rizik treba stalno pratiti. Iako je javnost upoznata sa visokotehnološkim terorizmom putem izveštaja u medijima, još uvek nisu toliko obavešteni o poznavanje tehničkih karakteristika i štetu zbog nedostatka informacija i svesti. Studije su pokazale da je percipirani rizik od visokotehnološkog terorizma relativno nizak tokom perioda povišenog visokotehnološkog terorističkog napada. Građani možda nisu svesni (Sjöberg, 2004). upozoravajućih znakova (crvenih zastava) visokotehnološkog terorizma zbog složenosti i brzi razvoj korišćenih metoda. Teško je predvideti gde i kada će se dogoditi napad. Međutim, moguće je smanjiti rizik ispitivanjem područja koja mogu privući visokotehnološke terorističke napade. Zbog toga cilj ove pojave je dobijanje pristupa bez postojanja otkrivanja i izazivanje intenzivnog straha i štete bilo kome namenjeno. Strah je glavni pokretač visokotehnološkog terorizma, on izaziva promene u ponašanju koje destabilizuju političke zemlje i ekonomski sistem, utičući na berze, potrošačke navike i dugoročne finansijske odluke kao što su promene cena nekretnina usled povećanja terorističkih incidenata u određenom području. Dakle, politička nestabilnost može da utiče i na

lokalnu ekonomiju kao globalna investiciona ekonomija, tako da bi stabilnost ekonomskog i političkog sistema neke zemlje trebalo bi da bude manje ranjivija (Murrill, 2011). Rizik visokotehnoloških terorističkih napada prema kritičnoj infrastrukturi države je izuzetno visoka. Zbog svoje ranjivost i složenost, štete nanesene u nacionalnoj infrastrukturi mogla bi uništiti razvoj te zemlje. Vlade su shvatile potrebu da se zaštiti njihov informacioni sistem i kritični infrastrukturni sistemi zbog sve većih pretnji od visokotehnološkog terorizma. Međutim, mnoga ograničenja ne omogućavaju potpuno spuštanje Interneta jer postoje različita pravna pitanja koja su povezana. Anonimnost napadača otežava čak i to identifikovati i procesuirati uljeza kao brojne geografska i zakonska ograničenja koja se dovode u pitanje (Dombe, & Golandsky, 2016).

## 3 MERE ZA UBLAŽAVANJE RIZIKA OD VISOKOTEHNOLOŠKOG TERORIZMA

Iako je Internet najveća pojedinačna komponenta “cyberspace”-a povezan u gotovo više od 200 zemalja sa više od milijarde korisnika širom sveta, verovatnoća za visokotehnološki terorizam koji se javlja putem interneta raste drastično jer je internet zasnovan na nacionalnim i međunarodnim telekomunikacionim infrastrukturama koje uključuje fiksne, bežične i satelitske komunikacije. Mogli bi ciljne mete visokotehnoloških terorista, biti kritična infrastruktura zemlje kao što su telekomunikacioni sistemi, sistem saobraćaja, elektroenergetski sistem, komunalni sistem i drugi značajni sistemi koji su potrebni za vođenje neke zemlje .Dakle, ako su ovi sistemi uništeni, tada a cela nacija može biti uništena u smislu ekonomskog i socijalno blagostanje. Složenost infrastrukture neke zemlje povećava rizik od visokotehnološkog terorizma ako nije prisutan odbrambeni mehanizam za zaštitu od ovakvih terorističkih napada. Vlade bi trebalo da poboljšaju i usaglase relevantne zakonodavstva u svojim zemljama sa međunarodnim standardima i striktno se pridržavajte politike nulte tolerancije prema visokotehnološkom terorizmu, priznajući potrebu za privatnošću i ljudska prava. Edukacija članova javnosti o visokotehnološkom terorizmu je obavezan, uključujući omogućavanje pristupačnosti i tačne informacije o ranjivosti, pretnjama i incidentima kao i očekivano ponašanje i pružanje pristupa službenicima da se obrate o zabrinutosti ili prijave sumnjiva ponašanja. Ovo nije samo za članove javnost kao pojedinci, nego i za organizacije koje igraju ključnu ulogu u nadgledanju zaposlenih, obavljajući pozadinski pristup i druge politike ljudskih resursa, osim pravovremeno improvizujućih mera zaštite informacijskih manir. Na raspolaganju su i razni mrežni materijali tj. razumevanje pretnje visokotehnološkog terorizma i takođe o tome kako zaštititi računar od napada. Otuda je ključ za borbu protiv visokotehnološkog terorizma obrazovanje i javno-privatna partnerstva (Goodman, 2007).

Bezbednosne politike i sveobuhvatno planiranje za dejstvo mehanizam odbrane od napada visokotehnološkog terorizma trebao bi biti osnovana u organizacijama . Razvijene sigurnosne prakse treba da obuhvate sve aspekte uključene u informacioni sistem koji bi mogao da uradi usvajanje međunarodnih standardnih smernica o informacionoj sigurnosti. Pridržavanjem računarske sigurnosti politike, visokotehnološkog teroriste bilo bi teško probiti u kompjuterski sistem, čime se smanjuje rizik od visokotehnološkog terorizma koji nastaje (Goodman, 2007).

Implementacija sigurnosnih aplikacija u računare otežava da napadi visokotehnološkog terorizma prodiru unutar sistema. Te sigurnosne aplikacije bi trebale ažurirati često, pomoću odbora i uprava razumevanja i priznavanja hitne potrebe i racionaliziranje troškova nastalih na duži rok održivost firme. Međutim, nažalost, mnoge firme to izbegavaju, "vatre za vatru" koje uključuju njihove računarske sisteme za provere rupe u petlji koje mogu privući visokotehnološke terorističke napade jer je skupo i to mora biti urađeno na samostalno rizik.

Ključna karakteristika visokotehnološkog terorizma koja treba biti naglašena je njegovo bezgranično izlaganje, anonimnost i redukovani rizik, koji motiviše terorista. Terorista bi mogao isplanirati napad kilometrima dalje, a da ne napušta dom i smanjiti šanse da bude uhvaćen. Trenutno ograničenje zakonodavstvo unutar nadležnosti je presudni ugao koji treba da se poboljša. Postoji hitna potreba za harmonizacijom zakonodavstva na međunarodnom nivou, a sarađuje više zemalja sporazumima o uzajamnoj pravnoj pomoći i izručivanju. Potrebno je razviti

međunarodnu saradnju u domenu kontrole visokotehnološkog terorizma jer visokotehnološki terorizam je globalno pitanje u koje je uključena vlada zemlje i svetske organizacije koje usvajaju mrežu informacionih sistema. Saradnja sa drugim državama bi mogle biti inicirane ekonomskim alatima od strane formiranje i promovisanje zajedničkih standarda za međunarodne odnose trgovina koja će privući međusobno razumevanje između zemalja, kao i kontrolu rizika od visokotehnološkog terorizma. Vlade, posebno one za koje se zna da su luka ili pružaju sigurno utočište za visokotehnološke teroriste moraju međusobno razvijati jaku međunarodnu saradnju, razmenu informacija i pokrenuti zajedničke obuke za kontrolu rizika od visokotehnološkog terorizma Ovo može biti dodatno omogućeno aktivnijim učešćem iz globalne zajednice institucije. Konvencija Saveta Evrope (SE) od visokotehnološkog kriminala je inicirala prvu međunarodnu izjavu o zločinu počinjenim putem interneta i drugog računara mreže. Evropska unija je takođe preduzela određene korake protiv kontrole ilegalnih sadržaja na Internetu od strane zaštita intelektualne svojine i ličnih podataka, promocija elektronska trgovina i pooštravanje bezbednosti transakcije. Prisustvo aktivnog sistema odbrane kao što je transnacionalni sistem nadzora važan je element ublažavajućeg sistema. To bi moglo pružiti ključne informacije o identitet terorizma, pokretanje mehanizma za suzbijanje i drugi proaktivni koraci za borbu protiv rizika. Međutim, kontroverzno, mada bi to narušilo privatnost prava javnosti, mnogi to i dalje koriste u zemljama i za to je potrebna međunarodna saradnja da u potpunosti funkcionišu. Jedan takav sistem je ECHELON koji koristi zemlje poput Australije, Ujedinjenog Kraljevstva i Novog Zelanda koji ima sposobnost hvatanja inteligencije informacije širom sveta koristeći sistem nadzora dizajniran za filtriranje poruka i telefonskih razgovora putem računarskog sistema koji je u stanju da prepozna ključne reči i fraze. Odbrana Australije, Direkcija za signale (DSD) koristi ovaj sistem nadzora za nadgledanje Indokine, Južne Kine i Indonezije. Komunikacije vlade Ujedinjenog Kraljevstva je Štab (GCHK) koristi ovaj nadzor za nadgledanje Evrope, Rusije i Afrike. Vlada Novog Zelanda Biro za sigurnost komunikacija (GCSB) koristi ovaj sistem za praćenje regiona zapadnog Pacifika. Još jedan pristup koji zahteva međunarodnu saradnju je M.U.D pristup, koji stoji za Monitoring, Korišćenje i Ometanje. Koraci za nadgledanje i korišćenje mogu biti od koristi za analizu procesa radikalizacije terorizma organizacijom da bi se pronašla rešenja za deradikalizaciju situacije. Postupke ometanja mogu koristiti inficiranje terorističkih web lokacija kako bi ih uništili ili promenili sadržaj web stranice. To je više obrnuta radnja kako bi se smanjio rizik od visokotehnoških terorističkih napada. Međutim, pitanja nastaju kada postoje sukobljeni ciljevi zbog kojih neki još uvek žele da nadgledaju blogove, grupe za ćaskanje itd. Ova metoda takođe pomaže u identifikaciji zemalja koje pomažu i podržavaju život teroristi. Zbog pojačanog nadzora i zakonskih propisa, mnogi pojedinci traže mogućnosti da zaštite svoje privatnost iako nije u zločinačkoj nameri. Alati poput tehnika šifrovanja, upotreba pregledača i softver koji štiti njihovu anonimnost samo otežava da zvaničnici nadgledaju stvarne pretnje, posebno sa povećanjem prometa pomoću ovih alata. (Sundaram, 2008).

Isto tako, sa lakim pristupom informacijama visokotehnološki terorizam kao terorističke grupe koriste mrežu i društveni mediji kako bi proširili svoju mrežu, od presudne je važnosti ova istraživanja da se ažuriraju. Preduzeća i pojedinci koji pružaju i dalje Kriminalni softver kao usluge (CaaS) komplikuje postupak otkrivanja. Moguće rešenje bi koristiti veštačku inteligenciju (VI). VI je inovativan i logički pristup koji simulira ljudsku inteligenciju u mašinama, koristeći konvencionalne fiksne algoritme, što im omogućava da donose odluke i prilagođavaju se svom okruženju. VI je u stanju da se samopodešava, samokonfiguriše, samoupravlja, dijagnostifikuje i samoisceljuje. Čini se da metode VI pružaju više obećavajući ishod u smanjenju rizika od visokotehnoloških napada povećavajući sigurnost sajber-prostora. Funkcije VI koje su implementirane u softver koji se bori protiv cyber napada uključuju kompjutersku inteligenciju, prepoznavanje uzoraka, inteligentne agente i neuronske mreže i mogu se primeniti za otkrivanje i sprečavanje upada, odbijanja usluge, neželjene pošte, zloupotrebe i pomoći u forenzičkim ispitivanjima. (Tereshchenko, 2013).

## 4 AKCIONI PLAN REPUBLIKE SRBIJE U BORBI PROTIV VISOKO-TEHNOLOŠKOG KRIMINALA

Republika Srbija je u obavezi da donese i sprovodi strategiju i akcioni plan za efektivno rešavanje visokotehnološkog kriminala u skladu sa strateškim i operativnim pristupom Evropskoj uniji (EU) u pogledu visokotehnološkog kriminala. Navedena obaveza prevashodno proizilazi iz Pregovaračkih merila za Poglavlje 24 – Pravda, sloboda, bezbednost. Evropska Unija je konstatovala da je Republika Srbija ratifikovala Konvenciju o visokotehnološkom kriminalu (sačinjena u Budimpešti, engl. Budapest Convention) 2009. godine i pozvala Republiku Srbiju da dodatno uskladi svoje zakonodavstvo sa Direktivom 2013/40/EU o napadima na informacione sisteme. Ministarstvo unutrašnjih poslova je, u skladu sa Zakonom o ministarstvima („Službeni glasnik RS", br. 44/14, 14/15, 96/15 – dr. zakon i 62/17) nosilac izrade navedenog strateškog dokumenta u saradnji sa ostalim državnim institucijama, tj. zainteresovanim stranama. U planu za podršku transformacije Zapadnog Balkana u okviru Strategije za verodostojnu perspektivu proširenja i pojačanu saradnju sa državama sa područja Zapadnog Balkana istaknuta je potreba za povećanom podrškom u izgradnji kapaciteta u oblasti visokotehnološkog kriminala, uključujući saradnju sa Evropskom grupom za trening i edukaciju o visokotehnološkom kriminalu i buduće učešće u okviru Agencije za evropsku mrežu i informacionu bezbednost. U okviru Akcionog plana za Poglavlje 24 – Pravda, sloboda i bezbednost, gde je nosilac aktivnosti Ministarstvo unutrašnjih poslova, nalaze se tri preporuke sa osam definisanih aktivnosti, koje Republika Srbija treba da ispuni u okviru pristupnog procesa u EU, sa fokusom na unapređenje organizacionih, kadrovskih i tehničkih kapaciteta, analiziranja trenutnog normativnog i organizacionog okvira i preduzimanja radnji u cilju usaglašavanja sa pravnim tekovinama EU u oblasti visokotehnološkog kriminala i ojačavanje saradnje između državnih organa i institucija. Imajući u vidu da je jedna od glavnih karakteristika dela visokotehnološkog kriminala njihova transnacionalna priroda, od procesa evropskih integracija se očekuje povećanje ekspeditivnosti rada u predmetima visokotehnološkog kriminala, u smislu bržeg protoka informacija potrebnih za otkrivanje i gonjenje učinilaca krivičnih dela, te bržeg odgovaranja po međusobnim zahtevima za pružanje međunarodne pravne pomoći, a sve kroz jačanje kapaciteta državnih organa Republike Srbije, a naročito Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. Pored navedenih preporuka, Republika Srbija je nakon otvaranja Poglavlja 24 – Pravda, sloboda i bezbednost dobila prelazno merilo koje ima za cilj izradu Strategije za borbu protiv visokotehnološkog kriminala i koje glasi: „Srbija priprema, donosi i sprovodi strategiju i akcioni plan za efektivnu borbu protiv visokotehnološkog kriminala u skladu sa strateškim i operativnim pristupom EU u pogledu visokotehnološkog kriminala. Srbija ojačava svoje operativne kapacitete (u pogledu osoblja i opreme u Jedinici za visokotehnološki kriminal) kako bi rešila problem visokotehnološkog kriminala i usklađuje 2 svoje zakonodavstvo sa relevantnim pravnim tekovinama EU, uključujući u pogledu seksualnog zlostavljanja dece na internetu, obezbeđuje specijalizovane obuke i podiže nivo svesti javnosti i među državnim službenicima po pitanju visokotehnološkog kriminala". Na osnovu navedenih međunarodnih i nacionalnih dokumenata iz ove oblasti Republika Srbija je donela prvu Strategiju za borbu protiv visokotehnološkog kriminala sa pratećim Akcionim planom za njeno sprovođenje. Strategija predstavlja nastavak i proširenje aktivnosti kojima je cilj jačanje efikasnosti svih subjekata u oblasti suzbijanja visokotehnološkog kriminala u Republici Srbiji. Posebno je usmerena na nastavak usklađivanja zakonodavstva s međunarodnim standardima, dalje unapređenje kapaciteta nosilaca borbe protiv visokotehnološkog kriminala, unapređenje preventivnog i proaktivnog pristupa društva u suzbijanju svih oblika kriminala u toj oblasti, unapređenje inter-resorne saradnje u društvu, kao i saradnje Republike Srbije na regionalnom i međunarodnom nivou u oblasti visokotehnološkog kriminala. Ispunjenjem strateških ciljeva i daljim razvojem međunarodne i regionalne saradnje u ovoj oblasti, Republika Srbija će doprineti ne samo sigurnosti u zemlji nego i u regionu. Strategija za borbu protiv visokotehnološkog kriminala predstavlja dokument kojim Vlada utvrđuje institucionalni odgovor na pojavne oblike visokotehnološkog kriminala, definiše uloge i

nadležnosti državnih organa, identifikuje ciljeve i utvrđuje osnovne pravce delovanja na suzbijanju svih vidova visokotehnološkog kriminala. U ovoj strategiji određene imenice navedene su u muškom rodu, a koriste se kao neutralne za muški i ženski rod. Strategija se donosi na period od 2019. do 2023. godine. Akcioni plan 2019-2020. za sprovođenje Strategije za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine čini njen sastavni deo.

## 5 STATISTIČKI TRENDOVI U OBLASTI VISOKOTEHNOLOŠKOG KRIMINALA

Prema podacima Posebnog odeljenja za borbu protiv visokotehnološkog kriminala u proteklih pet godina na teritoriji Republike Srbije (period 2013-2017. godina) stopa kriminala je u porastu. Pregled broja predmeta Posebnog tužilaštva za visokotehnološki kriminal zaključno sa 31.12.2017. godine. 2019-2023 . godine čini njen sastavni deo.

U periodu od 1. januara 2013. godine do 31. decembra 2017. godine, Posebnom tužilaštvu za visokotehnološki kriminal podnete su krivične prijave protiv ukupno 1.318 poznatih punoletnih lica, dok je optužni akt podnet protiv ukupno 280 poznatih punoletnih lica. Ministarstvo unutrašnjih poslova je u periodu od 2013. do 2017. godine, podneo krivične prijave zbog izvršenja ukupno 3.824 krivičnih dela visokotehnološkog kriminala.

Krivična dela protiv bezbednosti računarskih podataka – ukupno 91 krivično delo i to: oštećenje računarskih podataka i programa iz člana 298. Krivičnog zakonika (5 krivičnih dela ili 5,5 % od ukupnog broja), računarska sabotaža iz člana 299. Krivičnog zakonika (7 ili 7,7%), pravljenje i unošenje računarskih virusa iz člana 300. Krivičnog zakonika (4 ili 4,4%), računarska prevara iz člana 301. Krivičnog zakonika (40 ili 43,9%), neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302. Krivičnog zakonika (34 ili 37,4%) i Krivična dela protiv intelektualne svojine - ukupno 328 krivičnih dela i to: povreda-sprečavanje i ograničavanje pristupa javnoj računarskoj mreži iz člana 303. Krivičnog zakonika (1 ili 1,1%). moralnih prava autora i interpretatora iz člana 198. Krivičnog zakonika (1 ili 0,3%), Ostala krivična dela – ukupno 3.405 krivičnih dela i to: prikazivanje, pribavljanje i neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199. Krivičnog zakonika (316 ili 96,3%), povreda pronalazačevog prava iz člana 201. Krivičnog zakonika (1 ili 0,3%) i neovlašćeno korišćenje tuđeg dizajna iz člana 202. Krivičnog zakonika (10 ili 3,1%). posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185. stav 4. Krivičnog zakonika (128 ili 3,8%), iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu iz člana 185 b Krivičnog zakonika (14 ili 0,4%), falsifikovanje i zloupotreba platnih kartica iz člana 225. Krivičnog zakonika (2.412 ili 70,8%), pravljenje, nabavljanje i davanje drugom sredstava za falsifikovanje iz člana 227. stav 2. Krivičnog zakonika (18 ili 0,5), neovlašćena upotreba tuđeg poslovnog imena i druge posebne oznake robe ili usluga iz člana 233. Krivičnog zakonika (827 ili 24,3%), odavanje poslovne tajne iz člana 240. Krivičnog zakonika (6 ili 0,2%).

## 6 ZAKLJUČAK

Može se zaključiti da je pretnja od visokotehnološkog terorizma napadi koji će se stalno povećavati kako ljudi postaju zavisni od interneta i zato povećavaju mogućnosti visokotehnoloških terorističkih napada. Teroristi poput ISIS uspešno stvaraju snažnu sliku prema percepciji javnosti na globalnom nivou. Pretnja napadima kontinuirano raste kako je rasprostranjenost korisnika na mreži neprestano u porastu. Rizik da dođe do visokotehnološkog terorističkog napada raste zajedno sa brzim rastom računarskih tehnologija. Dakle, sprovođenje zakona, politike, prakse i potrebne mere bi trebalo da se i dalje razvijaju kao što se i računarska tehnologija kontinuirano razvija. To je odgovornost službenika za razvoj sigurne tehnologije koji je sposoban da utvrdi sumnjive aktivnosti analizom javnih i privatnih podataka. Implementacija svih ovih mehanizama omogućava računar, da su mreža i sistemi manje ugroženi i upravljajući njima smanjuje rizik od visokotehnološkog terorizma zato što svaki mehanizam poseduje odvojene funkcije za borbu protiv visokotehnološkog terorizma, čak iako su već postojali različiti odbrambeni mehanizmi. Zbog stalnog razvoja Internet platforme pretnja od visokotehnološkog terorizma je i dalje u stalnom porastu.

## CITIRANA DELA

Alqahtani, A. (n.d.). The Potential Threat of Cyber-terrorism on National Security of Saudi Arabia. 1st ed. [ebook] Department of Politics and International Studies the University of Hull - UK. Available at: http://www.academia.edu/8951385/The_Potential_Threat_of_Cyberterrorism_on_National_Security [Accessed 19 Sep. 2016].

Aly, A., Macdonald, S., Jarvis, L. and Chen, T. (2016). Violent Extremism Online: New Perspectives on Terrorism and the Internet. 1st ed. [ebook] New York: Routledge, pp.18-21. Available at: https://www.book2look.com/embed/9781317431879 [Accessed 5 Sep. 2016].

Balkhi, S. (2013). 25 Biggest Cyber Attacks In History. [online] Available at: http://list25.com/25-biggest-cyber-attacks-in-history/ [Accessed 24 Dec. 2016].

Bogdanoski, M. and Petreski, D. (2013). CYBER TERRORISM– GLOBAL SECURITY THREAT. 1st ed. [ebook] Research Gate. Available at: http://file:///C:/Users/Win%208.1/Downloads/CYBER%20TERRORI SM-%20GLOBAL%20SECURITY%20THREAT%20- %20Mitko%20Bogdanoski.pdf [Accessed 24 Dec. 2016].

Casciani, Dominic (2017), Longer Jail Terms for Viewing Terror Content Online. BBC Available at https://www.bbc.com/news/uk41479620 [ Accessed on 27th Sept 2018)

Che, E. (2007). Securing a Network Society Cyber-Terrorism, International Cooperation, and Transnational Surveillance. [online] Available at: http://rieas.gr/images/RIEAS113ELIOTCHE.pdf [Accessed 10 Sep. 2016].

Cyber terrorism Defense Initiative. (2016 ). [online] Cyberterrorismcenter.org. Available at: http://www.cyberterrorismcenter.org/ [Accessed 23 Nov. 2016].

Dawson, M., Omar, M. and Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. Research Gate, [online] 3, pp.1539-1549. Available at: http://www.saintleo.edu/media/972036/understanding_the_methods_ behind_cyber_terrorism.pdf [Accessed 5 Sep. 2016].

Dilek, S., Cakır, H. and Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, [online] 6(1), pp.21-39. Available at: http://aircconline.com/ijaia/V6N1/6115ijaia02.pdf [Accessed 17 Dec. 2016].

Denning, Dorothy E. (2000). Cyberterrorism: Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism

Dogrul, M., Aslan, A. and Celik, E. (2011). Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. 3rd ed. [ebook] Istambul: CCD COE Publications. Available at: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pd f [Accessed 5 Sep. 2016].

Dombe, A. and Golandsky, Y. (2016). A Review and Analysis of the World of Cyber Terrorism. 1st ed. [ebook] Available at: http://www.cyberisk.biz/cyber-terrorism-review-and-analysis/ [Accessed 23 Nov. 2016].

Goodman, S. (2007). Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop. Chapter 5. Cyberterrorism and Security Measures. [online] Available at: https://www.nap.edu/read/11848/chapter/6 [Accessed 5 Sep. 2016].

Hoffman, A. and Schweitzer, Y. (2015). Cyber Jihad in the Service of the Islamic State (ISIS). [online ] www.inss.org.il. Available at:

http://www.inss.org.il/uploadImages/systemFiles/adkan18_1ENG%2 0 (5) _Hoffman-Schweitzer.pdf [Accessed 5 Sep. 2016].

Hyde, O. (2011). Machine Learning for Cybersecurity at Network Speed & Scale. 1st ed. [ebook] AIOne Inc. Available at: http://www.academia.edu/1026724/Machine_Learning_for_Cyber_Security_at_Network_Speed_and_Scale [Accessed 14 Dec. 2016].

Jalil, S. (2003). Countering Cyber Terrorism Effectively: Are We Ready to Rumble? 1st ed. [ebook] SANS Institute. Available at: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorismeffectively-ready-rumble/105154 [Accessed 4 Sep. 2016].

Janczewski, L. and Colarik, A. (2008). Cyber Warfare and Cyber Terrorism. 1st ed. [ebook] New York and Hershey: Information Science Reference. Available at: https://books.google.com.my/books?hl=en&lr=&id=XWK9AQAAQ BAJ&oi = fnd&pg = PA1&dq = cyber + terrorism + cases&ots = 27XIC8yu mj&sig = 4r2Npu9JU4yVd8U70t8cYkVQaE&redir_esc = y#v = onepage&q&f = false [Accessed 14 Aug. 2016].

Murrill, R. (2011). The Question of Cyber Terrorism. [online] Forensic Focus - Articles. Available at: https://articles.forensicfocus.com/2011/07/23/the-question-of-cyberterrorism/ [Accessed 5 Sep. 2016].

Prasad, K. (2012). Cyber terrorism: Addressing the Challenges for Establishing an International Legal Framework. 1st ed. [ebook] Perth: Edith Cowan University. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act [Accessed 5 Sep. 2016].

Santiago, J. (2015). Top countries best prepared against cyber-attacks. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2015/07/top-countries-bestprepared-against-cyberattacks/ [Accessed 24 Dec. 2016].

Sjöberg, L. (2004). THE PERCEIVED RISK OF TERRORISM. [online] Available at: http://swoba.hhs.se/hastba/papers/hastba2002_011.pdf [Accessed 19 Dec. 2016].

Službeni glasnik RS, br. 44/14, 14/15, 96/15 – dr. zakoni 62/17

Sundaram, S. (2008). Cyber Terrorism: Problems, Perspectives, and Prescription. [online] Academia.edu . Available at: http://www.academia.edu/812094/Cyber_Terrorism_Problems_Perspectives_and_Prescription [Accessed 5 Sep. 2016].

Tereshchenko, N. (2013). US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure. [online] E -International Relations. Available at: http://www.e-ir.info/2013/06/12/us-foreignpolicy-challenges-of-non-state-actors-cyber-terrorism-against-criticalinfrastructure/ [Accessed 9 Sep. 2016].

Vlada R.S. (2018). Strategija za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine http://www.mup.rs/wps/wcm/connect/7b8500bb-171c-4ba3-b61a-b3772d5feaf8/PDF_LAT_Strategija+za+borbu+protiv+VTK+2019-2023.pdf?MOD=AJPERES&CVID=mtm2sqy 2019.

Datum prve prijave: 23.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

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

***Style – APA Sixth Edition:***

Petrović, I., & Trnavac, D. (2019, 10 15). Radikalizacija visokotehnološkog terorizma. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 108-117. doi:10.12709/fbim.07.07.02.12

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

Petrović, Ivica, and Dragana Trnavac. 2019. "Radikalizacija visokotehnološkog terorizma." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 108-117. doi:10.12709/fbim.07.07.02.12.

***Style – GOST Name Sort:***

**Petrović Ivica and Trnavac Dragana** Radikalizacija visokotehnološkog terorizma [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 108-117.

***Style – Harvard Anglia:***

Petrović, I. & Trnavac, D., 2019. Radikalizacija visokotehnološkog terorizma. *FBIM Transactions,* 15 10, 7(2), pp. 108-117.

***Style – ISO 690 Numerical Reference:***

*Radikalizacija visokotehnološkog terorizma.* **Petrović, Ivica and Trnavac, Dragana.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 108-117.