Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

CYBER TERORIZAM
CYBER TERRORISM

Pregledni naučni rad

Enes Bezdrob, MA[171]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U prvom dijelu radu se problematizira način kreiranja teoretskog okvira za analiziranje fenomena „cyber terorizma". U drugom dijelu rada se analizira fenomen „virtualnog genija". Ova pojava je specifičan produkt posredne komunikacije dostupne na društvenim mrežama. U trećem dijelu rada autor raspravlja o otpornosti društvenih grupa na indoktrinaciju koja se odvija u cyber prostoru.

Ciljevi rada (naučni i/ili društveni): Upravo je cyber prostor, svojom specifičnošću dozvolio izranjanje genijalaca koji na izgled imaju puno veće znanje od osoba sa kojima dolazimo u dodir u direktnoj svakodnevnoj komunikaciji. U ovom radu se raspravlja i o vrstama poruka koje se nastoje odaslati i steći naklonost ili, kao forma specijalnog rata, izazvati strah u određenoj društvenoj zajednici.

Metodologija/Dizajn: U radu je korištena analiza sadržaja relevantne literature.

Ograničenja istraživanja/rada: Rad je pregledni naučni.

Rezultati/Nalazi: Gotovo da ne postoji strukturirana društvena zajednica koja nije na neki način upoznata sa materijalnim i intelektualnim resursima i potencijalima njenih članova, sa prednostima i nedostacima socijalizacije unutar grupe. Upravo ovdje je šansa za preventivno djelovanje i sprečavanje eventualnih cyber podstrekača da pronađu stvarne izvršioce terorističkih akata.

Generalni zaključak: Ključno je naglasiti da postoji potreba razumijevanja onih koji regrutiraju izvršioce terorističkih akata, njihovih motiva, metoda djelovanja i prepoznavanja potencijalnih istomišljenika. Poseban naglasak se stavlja na profil podstrekača koji iskorištava slabosti eventualnog izvršioca predstavljajući se kao njegov istomišljenik i ohrabruje odnosnog na poduzimanje nasilnih aktivnosti na osnovu činjenica i pojava koje sam izvršilac smatra da treba ispraviti u njegovom okruženju.

Opravdanost istraživanja/rada: Poseban problem nastaje pri pokušaju da se ovaj fenomen promatra izdvojeno od ostalih negativnih oblika društvenosti. Naravno, autor prepoznaje specifičan, tehnološki, uvjet koji bi, na prvu, ukazivao da se radi o posebnom obliku terorizma. Međutim, evolucija društvene dinamike ne mijenja posljedicu djelovanja onih koji se bave terorizmom. Važan aspekt zamjene teza je i u činjenici da su u propagiranje ove nove „naučne discipline" snažno uključeni i mediji ne praveći razliku između nauke i naučne fantastike koju „učenjaci" željni slave namjerno izostavljaju.

[171] Vijeće ministara BiH, Odjel za sigurnost

Ključne riječi
Terorizam, Internet, sigurnost, cyber prostor, specijalni rat

Abstract
Reason for writing and research problem (s): In the first part of the paper, the way theoretical frame for the analysis of the "cyber terrorism" phenomenon was created, is problematized. The second part of the paper analyses the "virtual genius" phenomenon. This appearance is a specific product of indirect communication available on social networks. In the third part of the paper the author discuss the resilience of social groups to indoctrination that occurs in cyber space.
Aims of the paper (scientific and/or social): It is cyber space, with its specificity, that allows the emerging of geniuses who, at first glance, have a larger knowledge then people; we come in contact in everyday communications. This part also deals with the types of messages that are conveyed in order to gain favor or, as a form of special war, cause fear in a specific social community.
Methodology/Design: Paper is a review paper.
Research/Paper limitation: This paper employed content analysis of relevant literature.
Results/Findings: A structured social community, not familiar with the material and intellectual resources and potential of its members, together with the advantages and disadvantages of socialization inside of the group, almost does not exist. Right here is the chance for prevention and the stopping of potential cyber persuaders to find actual executors of terrorist acts.
General Conclusion: It is crucial to emphasize that a need exists to understand those who recruit the executors of terrorist acts, their motives, methods, and the way they recognize potential supporters. A special emphasis is put to the profile of the persuader who uses the weaknesses of potential executors appearing as a like-minded individual and encouraging him to conduct violent activities based on the facts and appearances that the executor himself believes need fixing in his surroundings.
Research/Paper Validity: A particular problem occurs when trying to view this phenomenon separately from other negative social forms. Of course, the author recognizes a specific, technological, environment that would, at first, point out that it is a special form of terrorism. However, the evolution of social dynamics does not change the consequence of the activities those who engaged in terrorism. An important aspect of this scientific error is in the fact that media are strongly involved in the propagation of this new "scientific discipline" without making a difference between science and science fiction which is deliberately left out by fame craving "scholars".

Keywords
Terrorism, internet, security, cyber space, special war

Uvod

Na samom početku je potrebno uspostaviti određeni logički okvir analize razmatrane teme. Da li je nužno pri raspravi o cyber terorizmu „izmišljati" kompleksne teorije i metodološke zahvate ili je moguć jednostavniji pristup kako sa aspekta teorije tako i metodologije? Prema mom shvatanju ne radi se o novom fenomenu niti o novoj nauci. Specifična tehnološka dimenzija, na prvu, ostavlja dojam da se radi o novom fenomenu ali i o

potrebi stvaranja nove nauke koja će moći ponuditi rješenja problema kojim cyber terorizam opterećuje društva širom svijeta (Weimann, G., 2004: 4). Mnogi od nesporazuma nastaju iz želje naučnika da zasnuju novu nauku, da budu pioniri u nekoj novoj oblasti, ili su u pitanju neki drugi egoistični razlozi. Bez obzira na manipuliranje pojmovnim određenjima cyber terorizam ne izlazi izvan, već uspostavljenog teoretskog okvira (Babić, V., 2009: 171). Rasprava o terorizmu je daleko od zaokružene, niz je neslaganja među naučnicima o uzročno-posljedičnim vezama terorizma i društvene dinamike, ali ni u kom slučaju to ne znači da postojeći teoretsko-metodološki okvir nije dostatan u analiziranju cyber terorizma (Beggs, C., 2010: 14).

Važno je istaći da definicije terorizma, koje je moguće naći u literaturi, dolaze iz različitih teoretskih krugova, što je u neku ruku dovelo do definicijske zamagljenosti i otežalo ogoljenje fenomena. Ovdje se nećemo baviti definicijama, već ćemo se fokusirati na jedan aksiom i to da je terorizam uvijek politički motiviran. Bez obzira na ideološku obojenost grupa ili pojedinaca koji izvode terorističke napade, uvijek je prisutan politički motiv (Kovačević, G. 2015: 110). O svim ostalim elementima terorizma, na koje se ukazuje u različitim definicijama, moguće je raspravljati osim o političkom motivu. Dakle, o kojem god obliku terorizma da se radi, kada ogolimo politički motiv možemo se efikasno boriti protiv njega. Mnogi autori se neće složiti sa ovom konstatacijom, jer su navodili druge motive kao razloge za terorizam. Međutim, svi motivi koliko god izgledali udaljeni od politike, podvrgnuti su, u svakom konkretnom slučaju, procesu politizacije i tek tada su postali motivi terorizma. Kao primjer možemo uzeti religijski fundamentalizam, koji je prema velikom broju naučnika ideološka matrica, u mnogo slučajeva, terorističkih organizacija i grupa. Posebno se ovdje ističe islamski fundamentalizam. Problem je u činjenici da se ovdje zanemaruje proces politizacije a u prvi plan se stavlja religija. Međutim, religijski fundamentalizam je politička ideologija i religija mu je samo u imenu i ako bismo ga ogolili vidjeli bismo da se radi o klasičnom obliku fašizma (Kovačević, G. 2013: 238).

Terorizam se uvijek javlja u uvjetima gdje određena grupa ili pojedinac ne mogu legitimnim i legalnim političkim mehanizmima postići željene političke promjene. Izvori nemogućnosti postizanja željenih političkih promjena mogu biti različiti: od toga da je percipirani neprijatelj nasilan u nastojanju da zadrži stečene pozicije društvene moći, do toga da grupa koja želi te promjene nema podršku većinske zajednice (Held, D. 1999: 200).

Da bih bio što precizniji potrebno je objasniti suštinu političkog u terorizmu. Svako društvo, uokvireno u nacionalnoj državi, profilira se i bivstvuje posredstvom niza političkih institucija i mehanizama koji, u većoj ili manjoj mjeri, su odraz volje tog društva. Što je veća usklađenost volje i postojećih institucija i mehanizama to je manje prostora za nezadovoljstvo. Obrnuto, postoji prostor za oživljavanje političkih aspiracija usmjerenih na drugačije usklađivanje. Naravno, i ovdje postoji granica. Ako je neusklađenost velikog obima onda će doći do pokušaja usklađivanja drugim političkim sredstvima, a ne terorizmom (Abazović, M. 2012: 52 - 54). Važno je istaći da terorizam je nasilno političko sredstvo ali samo u mirnodopskim uvjetima. U uvjetima rata, napad na bilo koju neprijateljsku metu je legitiman, posebno ako će to rezultirati strahom u neprijateljskim redovima. Iz

prethodne konstatacije je jasno da je niz aktivnosti u historiji čovječanstva pogrešno okarakteriziran kao terorizam. Neko djelovanje nazvati terorizmom može samo akter koji u datom momentu raspolaže mogućnošću da određuje šta jeste a šta nije istina. Dakle, onaj ko je u poziciji moći raspolaže mogućnošću da imenuje neku aktivnost kako mu u tom trenutku odgovara i da protiv nosilaca te aktivnosti primjenjuje različite mehanizme represije iz arsenala koji mu je na raspolaganju, ovisno od njegove sposobnosti da društvenoj zajednici legitimira primjenu tim mjera (Ibid.). Poseban problem u razumijevanju terorizma nastaje iz konvergencije neznanja predstavnika vlasti i medija, gdje „povika na vuka" može otići u nedogled dok se ne utvrdi činjenično stanje. Ovo se posebno lako dešava kada je u pitanju dobro reklamirana pojava kao što je terorizam. Medijski momentum koji postoji u slučaju terorizma nastoji se iskoristiti i za „reklamiranje" cyber terorizma, posebno ukazujući na fantastične mogućnosti koje su na raspolaganju cyber teroristima. Mi, kao naučnici, moramo razlikovati naučnu fantastiku od nauke. Moramo društvu objasniti šta jeste moguće a šta nije. Na kraju mnogo je teoretski mogućih aktivnosti koje nisu praktično sprovodive.

Cyber prostor i terorizam

Cyber prostor ili okruženje je, također, jedan od onih fenomena koji se atribuira mogućnostima i sposobnostima preko mjere. Naravno, to jeste prostor, u pravom smislu, materijalizirane globalizacije. Po našem mišljenju mjesto dijaloga različitih kulturoloških krugova; mjesto postavljanja informacija, podataka, obavještenja u različitim formama i za različitu publiku; mjesto pružanja raznih usluga; mjesto obrazovanja; mjesto dijaloga, polemike, reklamiranja, propagande, vrbovanja, prevara i tako dalje (Chu, S. C., Lien, C. H., Cao, Y. 2018.). Međutim, potrebno je istaći da je niz sistema različite namjene dostupno u cyber prostoru kojima upravljaju direktno ljudi ili neki oblik vještačke inteligencije. Iako izgleda da su mogućnosti bezgranične ovaj prostor je upravljan određenim zakonitostima, čije zaobilaženje ili zloupotreba privlače pažnju i aktiviraju mehanizme zaštite (Bara, D. 2015: 130). Ovdje ću se fokusirati na jednu specifičnost komunikacije unutar cyber prostora koja pojedincima ili grupama otvara mogućnost da šire svoje „ideje", poruke, prijetnje, da vrbuju istomišljenike, da traže podršku za svoje „projekte" i sl. Vrlo je važno razumjeti u kojem su obimu pojedinci pa i čitave zajednice opterećeni svakodnevnim rutinama čijim izvršavanjem obezbjeđuju vlastitu egzistenciju i funkcioniranje društvene grupe u kojoj psihički i fizički egzistiraju (Weimann, G. 2019: 115). Radi se o uhodanim bihevioralnim obrascima koji konzumiraju vrijeme pojedincima ili grupama, ostavljajući im malo prostora za bilo kakvo kritičko promišljanje o nekim predočenim problemima (Guegan, J. 2019: 192). Kritičko promišljanje podrazumijeva upoznavanje sa historijom „problema", argumentima svih zainteresiranih strana i donošenje suda u na osnovu stavljanja sebe u odnosnu situaciju. Pregršt novih informacija uvijek otežava historijski uklon, pa mnogi od njega i odustaju zarad svježih informacija. Upravo zbog poteškoća koje su povezane sa prethodnim postupkom pojedinci ili grupe su, u većoj ili manjoj mjeri, skloni da prihvate tuđu „analizu" problema koja im ima više logike u odnosu na njihove životne uvjete i provedu određene aktivnosti iz preporuka „analize" (Lehti, L., Kallio, J. 2017: 60). Ovdje je potencijalno prostor za cyber terorizam gdje ne postoje fizičke barijere, poput granica, za okupljanje simpatizera i istomišljenika, pa i aktivnih članova koji

su spremni poduzimati aktivnosti na planu realizacije određenih ideja ili djelatnosti za koje drže da će riješiti specifičan problem (Karapanos, E., Teixeira, P., Gouveia, R. 2016: 889). Iako se radi o virtualnoj zajednici uvijek moramo imati na umu da su stvarni ljudi iza tih virtualnih osoba, koji mogu svojim djelovanjem proizvesti željene efekte (Sudweeks, F. 2001: 71). Potrebno je napomenuti još jednu ljudsku osobinu, kada govorimo o virtualnim identitetima, kojima se pojedinci predstavljaju u cyber okruženju moramo skrenuti pažnju na jedan posebno, za analiziranje terorizma, važan aspekt. Dakle, većina ljudi koji su prisutni u cyber prostoru susreli su se sa virtualnim genijem. Radi se o osobama koje u komunikaciji raspolažu znanjima i informacijama, mnogo većeg obima, od onoga koje bismo susreli u realnom životu kod bilo koje osobe. Obzirom da je komuniciranje u cyber okruženju modelirano na način da oponaša ono koje se dešava i u realnom svijetu, često se previdi činjenica da ljudi koji se pojavljuju u ulozi virtualnog genija (Jang-Jaccard, J. 2014: 981) mogu biti profesionalci čija je dnevna rutina upravo iskorištavanje identificirane nekritičnosti šire publike. Znanja i informacije kojima ovi ljudi raspolažu ne moraju, i u većini slučajeva nisu, njihova, već ona koja su dostupna u samom cyber prostoru a odnosne osobe znaju kako u što kraćem vremenu pristupiti takvim znanjima i plasirati ih (Chen, J. 2014: 902). Upravo brzina iznošenja informacija je ona koja stvara privid direktne komunikacije i stvara privid da se radi o stvarnom autoritetu u nekoj oblasti (Gordon, S. 2002: 640). Jednom kada se identificira publika koja će prihvatiti poruke i identificirati se sa sadržajem, otvara se prostor za djelovanje bilo da se radi o pozitivnih ili negativnim aktivnostima. U tom trenutku publika, koja je sve do tada bila relativno pasivna, postaje protagonista dobro kreiranog scenarija (Marwick, A. E., Boyd, D. 2011: 129). Važno je naglasiti da su teroristi samo jedni od negativaca koji koriste ovakav model stjecanja resursa za ostvarivanje svojih ciljeva (Choo, K-K. R. 2011: 722). Nedoumice postoje oko toga koliko je ovaj pristup funkcionalan, ali je u svakom slučaju mnogo jeftiniji od istog ovog pristupa koji bi se provodio u realnom životu (Huang, L. 2011: 732). Međutim, zadnji pokazatelji, posebno vezano za napade u EU, dovode do zaključka da je efikasnost neupitna.

Kao što sam već ranije napomenuo cyber prostor je i zamišljen kao virtualna replika stvarnosti i da bi se to postiglo niz je mehanizama kojima se prikupljaju podaci o subjektima koji operiraju u odnosnom prostoru (Stanfield, D., Beddoe, L., Ballantyne, N., Lowe, S., Renata, N. 2017: 45). Veoma sofisticirane naučne metode su primijenjene da bi stvarna osoba prihvatila i svoj virtualni identitet kao nedjeljiv od njegove ličnosti. Različite statističke, bihevioralne, psihološke, sociološke analize osiguravaju „istinitost" virtualne stvarnosti . Dakle, postojanje mehanizama koji u realnom vremenu prikupljaju podatke o svakom korisniku i stvaraju procjene o njegovim budućim obrascima ponašanja su sastavni dio sistema na kojima je uspostavljen cyber prostor. Podaci koji se dobiju na ovaj način mogu biti zloupotrebljeni od strane, u našem slučaju, terorista za „nagovaranje" osoba da urade nešto što bez sistematskog i ciljanog uvjeravanja ne bi uradili (Wise, J. B., O'Byrne, W. I. 2015: 404). Ne radi se o prostom nagovaranju, jer većina ljudi instinktivno prepoznaje takvu vrstu komuniciranja kao negativnu i stvara otpor prema njoj. Nagovaranje u ovom smislu postoji kao zagovaranje određenog ponašanja i projiciranje vlastitog motiva kao zajedničkog cilja, što rijetko nailazi na bilo kakav otpor od strane onih koji su meta ovakvih indoktrinacija (Huang-Horowitz, N. C., Freberg, K. 2016: 200). Zagovaranje podrazumijeva i poseban identitet zagovaratelja. U jednom slučaju zagovaratelj ne krije

svoj politički motiv i poziciju zbog kojih traži „pomoć" jer slušaoci mogu da se identificiraju sa njegovim statusom i razlozima za djelovanje posebno ako se poziva na organske ideje kao što su religija, rasa, etnička pripadnost itd. (Gunduz, U. 2017: 87). Sa druge strane kada je u pitanju publika koju nije moguće pridobiti na osnovu organskih ideja, zagovaratelj će se identificirati sa tom publikom oponašanjem njih samih i izražavajući zabrinutost za probleme u njihovom društvu pozivajući ih na akciju za promjene (Davis, J. L., Jurgenson, N. 2014: 479). U zadnjem slučaju pravi politički motiv je maskiran drugim političkim motivom koji se nalazi kod ciljane grupe. Grupa ili pojedinac može poduzimati terorističke aktivnosti iz razloga koji nemaju veze sa razlozima onoga koji ih potiče na djelovanje. U ovom slučaju je bitna posljedica, bez obzira što politički motiv ostaje skriven.

Cyber prostor je samo sredstvo i mjesto dogovora za izvođenje terorističkih napada, tako da se opet vraćamo na početak i tvrdnju da cyber terorizam nije poseban oblik terorizma. Važnost ovog pojma je medijski kreirana a sve ono što se pripisuje kao mogućnost cyber prostora se zasniva na identificiranim nezadovoljstvima pojedinaca i grupa koje egzistiraju u realnom društvu (Leeds-Hurwitz, W. 2009: 892).

Djelovanje u cyber prostoru je moguće nadzirati i identificirati nosioce negativnih aktivnosti. Specijalizirani sistemi i obučeni kadrovi itekako su prisutni u cyber prostoru i aktivno rade na otkrivanju nezakonitih aktivnosti i onesposobljavanju njihovih nosioca terorizma (Beggs, C. 2010: 57).

Dodatno, svaka država vodi određene baze podataka o svojim građanima i raspolaže nizom podataka o njihovim sposobnostima. Pored toga, svaka država, identificira i analizira sigurnosne probleme i rizike koji su prisutni unutar njenih granica (Abazović, M. 2012: 15). Naučnim pristupom je svakako moguće provoditi društvene projekte koji će kreirati svijest u društvu o mogućim načinima vrbovanja i iskorištavanja pripadnika društvene zajednice. Država treba da ima jasnu predstavu o zadovoljstvu građana načinom alociranja društvenih resursa i radi aktivno na povećanju tog zadovoljstva što će svakako imati pozitivan efekt u smanjenju mogućnosti vrbovanja pripadnika vlastitog društva od strane terorista u postizanju nekih njihovih političkih ciljeva, ali će doprinijeti općoj otpornosti zajednice na bilo koju vrstu negativne indoktrinacije koja bi za posljedicu mogla imati ljudske žrtve i materijalnu štetu (Christensen, T. 2019: 19). Ovakvo stanje je ideal, ne postoji društvo u kojem su svi njegovi članovi zadovoljni, pa se mora aktivno raditi kako na otkrivanju, kako, onih koji potiču na terorizam, tako i onih koji bi mogli biti izvođači terorističkih aktivnosti. Kontinuirane naučne analize i istraživanja u oblasti terorizma su jedan od ključnih mehanizama ove borbe, ali pored toga i izgradnja institucija koje će voditi računa o subjektima koji su identificirani kao potencijalni izvršioci terorističkih aktivnosti. Svako društvo ima dovoljno kapaciteta da se zaštiti od terorizma samo je pitanje da li postoji svijest i volja kod nosioca političkih funkcija da se aktivno posvete izgradnji sigurnog društva i zajednice uspostavljene na povjerenju, poštovanju ljudskih prava, neosporivim kolektivnim identitetima i jakom i efikasnom socijalnom modelu.

Mogućnosti vs nemogućnosti

Nauka, ni u kom slučaju, ne smije biti pod utjecajem bilo kakvih argumenata koji nisu produkt primjene naučne metodologije. Ovo je posebno važno kada govorimo o političkim utjecajima pod koje često potpadaju naučnici. Drugo, naučnici svojim radom moraju ponuditi odgovore kojima se objašnjava problem i nude konkretna rješenja. Nije nauka samo u identificiranju prijetnji i rizika nego u iznalaženju efikasnog odgovora, tek tu dolazi do izražaja stvarna priroda nauke. Novo doba, ovo temeljeno na tehnologiji dalo je zamaha mašti ljudi koji nauku poznaju posredno, a ustvari se ne bave naukom direktno. To su oni ljudi koji logiciraju određene scenarije a da ih naučno ne potvrđuju. Svjedoci smo niza takvih zahvata, posebno u filmskoj industriji gdje je urađeno mnogo na stvaranju kulta ličnosti hakera koji su svemoćni i raspolažu znanjima koja se mogu zloupotrijebiti i svijet dovesti do propasti. Kao što smo već ranije rekli, važno je da naučnici prave razliku između naučne fantastike i nauke. Ne zaboravimo da je i cyber okruženje produkt nauke i zakonitosti koje je vrlo teško zaobići, bez obzira na uvriježeno mišljenje.

Sistemi koji su esencijalni za funkcioniranje društava ili sistemi čije uništenje ili zaustavljanje bi izazvalo teške posljedice su zaštićeni od bilo koje vrste cyber napada. Tehnologija koja je potrebna da bi ugrozila ovakve sisteme je preskupa i pod striktnim nadzorom vlada država koje bi mogle biti meta takvog napada. Sa druge strane stručnjaci koji posjeduju znanja za izvođenje ovakvih napada su također poznati. Specifična znanja o načinu funkcioniranja ovih sistema poznata su ograničenom broju ljudi, a sami ti ljudi su također, poznati agencijama za provedbu zakona ili agencijama za drugu namjenu. Dakle, mit je haker koji sa laptopom upada u obrambeni sistem npr. SAD. U slučaju da se desi neka situacija sličnog obima, izvršioci se vrlo brzo mogu otkriti i to sa aspekta potrebne tehnologije za takvu aktivnost ili fizičkog pristupa sistemu. U odnosnom slučaju vrbovana je osoba koja ima pristup i znanje, a nije u pitanju poseban fenomen terorizma. Zašto bi osoba pristala da sabotira sistem koji osigurava funkcioniranje nekog društva, iako joj je društvo dalo povjerenje da upravlja tim sistemom, je pitanje za drugu vrstu analize. Društva kroz svoje mehanizme socijalizacije i usvajanja pozitivnih normi od strane pojedinaca i grupa trebaju stvarati svijest o društvenim vrijednostima koje svi pripadnici tog društva percipiraju kao pozitivne. Bez ovakvog pristupa uvijek postoji prostor za nezadovoljstvo, pa čak i kod pojedinaca koji upravljaju veoma osjetljivim sistemima. Dakle, postoji prostor za manipulaciju od treće osobe kojoj u danom trenutku odgovara da je određeno društvo pogođeno posljedicama krize.

Zaključak

Fenomen cyber terorizma je više propaganda nego je stvarna pojava u pitanju. Postoje specifičnosti koje ostavljaju prostora da se govori o posebnom pojavnom obliku, ali stvaranje nove nauke je bespotrebno. Sa aspekta nauke, jasno je da, treba uvažiti interdisciplinarnost u borbi protiv zloupotrebe tehnoloških dostignuća ali isto tako neizostavan je i zahvat društvenih nauka u zaokruživanju strategije suprotstavljanja ovom načinu pripremanja terorističkih napada. Mnogo je informacija u cyber okruženju koje na neki

način mogu biti iskorištene u planiranju napada, identificiranju izvršioca, potrebnih resursa za određene aktivnosti itd. Međutim, nadzorom takvih informacija i identificiranjem osoba koje se interesiraju za specifične resurse i tehnologije iskoristive za izazivanje štete u nekom društvu aktivno se mogu spriječiti nedozvoljene aktivnosti. Ne smije se zaboraviti da terorizam ima političku pozadinu, koja ne mora biti u interakciji između lokalnih aktera, već zainteresirana strana dolazi iz druge države i terorizam koristi za postizanje svojih vanjsko-političkih ciljeva.

I na kraju opet se vraćam na tvrdnju da kada otkrijemo politički motiv u određenoj terorističkoj aktivnosti u mogućnosti smo da formuliramo adekvatan odgovor i aktiviramo efikasne mehanizme zaštite određene zajednice koja je meta takvih aktivnosti.

Literatura

1. Ashforth, B. E., Schinoff, B. S., Rogers, K. M. (2016). "I identify with her," "I identify with him": Unpacking the dynamics of personal identification in organizations. Academy of Management Review, 41.
2. Babić, Vladica (2009). Kompjuterski kriminal, Sarajevo: Rabic.
3. Bara, Danijel (2015). Uloga cyber-osiguranja u upravljanju i prijenosu rizika cyber- sigurnosti, Opatija: ZBORNIK RADOVA S MEĐUNARODNE ZNANSTVENO-STRUČNE KONFERENCIJE Dani hrvatskog osiguranja.
4. Beggs, Charles (2010). Safeguarding Infrastructure Assets from Cyber-terrorism, London: Lambert Academic Publishing.
5. Chen, Jinjun (2014). Special Issue: Dependable and Secure Computing, Journal of Computer and System Sciences vol. 80, London: Elsevier.
6. Choo, Kim-Kwang Raymond (2011). The cyber threat landscape: Challenges and future research directions, Computers & Security, Volume 30, Issue 8, London: Elsevier
7. Christensen, Tom (2019). Organizing for Societal Security and Crisis Management: Governance Capacity and Legitimacy, London: Springer.
8. Chu, S. C., Lien, C. H., Cao, Y. (2018). Electronic word-of-mouth (eWOM) on WeChat: Examining the influence of sense of belonging, need for self-enhancement, and consumer engagement on Chinese travellers' eWOM. International Journal of Advertising.
9. Davis, J. L., Jurgenson, N. (2014). Context collapse: Theorizing context collusions and collisions. Information, Communication & Society, 17.
10. Gordon, Sarah (2002). Cyberterrorism?, Computers & Security, Volume 21, Issue 7, London: Elsevier.
11. Guegan, Jerome (2019). (Social) Identity and Creativity in Virtual Settings: Review of Processes and Research Agenda, The Palgrave Handbook of Social Creativity Research. London: Pelgrave.
12. Gunduz, U. (2017). The effect of social media on identity construction. Mediterranean Journal of Social Sciences, 8 (5).
13. Held, David (1999). Global Transformations: Politics, Economics and Culture: Cambridge: Polity Press.
14. Huang, Lin (2011). Masquerade detection using profile hidden Markov models, Computers & Security, Volume 30, Issue 8, London: Elsevier.
15. Huang-Horowitz, N. C., Freberg, K. (2016). Bridging organizational identity and reputation messages online: A conceptual model. Corporate Communications: An International Journal, 21.
16. Jang-Jaccard, Julian (2014). A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences vol. 80, London: Elsevier.
17. Jin, Y., Liu, B. F., Austin, L. L. (2014). Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on publics' crisis responses. Communication Research, 41.

18. Karapanos, E., Teixeira, P., Gouveia, R. (2016). Need fulfillment and experiences on social media: A case on Facebook and WhatsApp. Computers in Human Behavior, 55, 888-897.
19. Kovačević, G., Smajić, M., Ahić, J., Korajlić, N. (2013). Novi koncept razumijevanja odnosa sigurnosti i politike, Policija i sigurnost, godina 22. broj 2/2013. MUP HR, Hrvatska, str. 236 – 248.
20. Kovačević, G., Alispahić, B., Korajlić, N. (2015). Nastanak i razvoj krize u 21. solјeću, Veleučilište Velika Gorica – Zbornik radova, Hrvatska, str. 103 – 113.
21. Leeds-Hurwitz, W. (2009). Social construction of reality. In Littlejohn, S., Foss, K. (Eds.), Encyclopedia of communication theory. Thousand Oaks, CA: SAGE.
22. Lehti, L., Kallio, J. (2017). Participation in an online social policy discussion: Arguments in focus. Discourse, Context & Media, 19.
23. Marwick, A. E., Boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. New Media & Society, 13.
24. Stanfield, D., Beddoe, L., Ballantyne, N., Lowe, S., Renata, N. (2017). Critical conversations: Social workers' perceptions of the use of a closed Facebook group as a participatory professional space. Aotearoa New Zealand Social Work, 29 (3).
25. Sudweeks, Fay (2001). Culture, Technology, Communication - Towards an Intercultural Global Village, New York: Sunny Press.
26. Weimann, Gabriel (2004). Cyberterrorism: How Real is the Threat?, Special Report, United States Institute of Peace.
27. Weimann, Gabriel (2019). The Influentials: People Who Influence People, New York: Sunny Press.
28. Wise, J. B., O'Byrne, W. I. (2015). Social scholars: Educators' digital identity construction in open, online learning environments. Literacy Research: Theory, Method, and Practice, 64.