Značajke suvremenog kibernetičkog terorizma

Perković, Sara

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Croatian Studies / Sveučilište u Zagrebu, Fakultet hrvatskih studija**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:111:712887

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-08-08**

SVEUČILIŠTE U ZAGREBU
HRVATSKI STUDIJI
UNIVERSITY OF ZAGREB
CENTER FOR CROATIAN STUDIES

Repository / Repozitorij:

Repository of University of Zagreb, Centre for Croatian Studies

zir.nsk.hr

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET HRVATSKIH STUDIJA

Sara Perković

ZNAČAJKE SUVREMENOG KIBERNETIČKOG TERORIZMA

ZAVRŠNI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET HRVATSKIH STUDIJA

ODSJEK ZA SOCIOLOGIJU

SARA PERKOVIĆ

ZNAČAJKE SUVREMENOG KIBERNETIČKOG TERORIZMA

ZAVRŠNI RAD

Mentor: doc. dr. sc. Ivan Perkov

Zagreb, 2022.

Sadržaj

Sažetak

Tema su ovog završnog rada značajke suvremenog kibernetičkog terorizma. Terorizam je uporaba oružanog ili drugog nasilja u svrhu ostvarenja političkog, vjerskog ili ideološkog cilja. Razvojem tehnologije terorizam je poprimio nove pojavne oblike. Teroristički napadi danas se ponajviše odvijaju unutar tehnologijskih i internetskih mreža, a manje na konvencionalnim ratnim bojištima. Cilj ovog rada je objasniti značajke suvremenog kibernetičkog terorizma te analizirati globalni društveni kontekst u kojem se on odvija.

Ključne riječi: kibernetički terorizam, tehnologija, internet, propaganda, radikalizacija

1. Uvod

Terorizam je danas prisutan gotovo u svim dijelovima svijeta. Pojava je koja se ne može zaustaviti, već samo u određenoj mjeri pokušati spriječiti ili kontrolirati. Strategije terorističkih organizacija mijenjaju se s vremenom. Prije razvoja informacijske tehnologije teroristički su se napadi uglavnom realizirali u gusto naseljenim područjima, a žrtve su najčešće bili civili, s ciljem zastrašivanja ciljane skupine. Današnji su teroristički napadi puno sofisticiraniji i u pravilu uključuju korištenje napredne informacijske tehnologije.

Promjene su se dogodile i u strukturi terorističkih organizacija. Terorističke grupe su prije bile zatvorenog tipa i teško se stupalo u komunikaciju s njima. Danas, uz pomoć sveprisutne računalne tehnologije, članovi skupine međusobno brže i jednostavnije komuniciraju, ali su otvoreniji i prema vanjskom svijetu. Svoju ideologiju promiču putem raznih internetskih stranica i društvenih mreža, a slike i video snimke objavljuju na gotovo svim platformama. Uz pomoć određenih sustava uspijevaju prikupljati informacije o svojim metama kao i sve podatke potrebne za izvršenje terorističkog napada.

Motivi za priključivanje terorističkoj organizaciji su brojni i heterogeni. Neki su pripadnici motivirani željom za moći ili im to članstvo predstavlja samoispunjenje, dok su drugi prisiljeni ili pod prijetnjom. Zahvaljujući širokoj dostupnosti propagandnih materijala u današnjem vremenu, pojavljuje se i samo-radikalizacija kandidata koji dobrovoljno i iz vlastitog interesa ili stava žele pristupiti terorističkoj grupi, jer su na internetu vidjeli materijale koji su ih zainteresirali.

Ključni čimbenik koji doprinosi sve većoj sklonosti prema terorističkim akcijama u virtualnom svijetu je anonimnost koju napadači u kibernetičkim ratovima često uspiju i sačuvati. Internet je tako, uz brojne nedvojbene pozitivne društvene učinke donio i mogućnosti jednostavnijeg i učinkovitijeg djelovanja terorističkih organizacija i širenja njihove propagande.

Cilj je ovoga rada objasniti značajke suvremenog kibernetičkog terorizma. U drugom odjeljku prikazat će se ključne karakteristike terorizma. U trećem odjeljku objasnit će se suvremeni terorizam i njegova obilježja u današnjem svijetu te prikazati odnos terorizma i nacionalne i međunarodne sigurnosti. U četvrtom odjeljku pojasnit će se kibernetički

(cyber) terorizam. Spomenut će se propagandi materijali koji pridonose njegovoj raširenosti u svim dijelovima svijeta. Navest će se razni načini na koje teroristička skupine prikupljaju informacije i podatke za buduće napade, a zatim obrazložiti kako funkcionira komunikacija među članovima terorističke grupe, kao i koji su njihovi motivi za terorističkim napadima.

2. Ključne karakteristike terorizma

Riječ terorizam dolazi od latinske riječi terror „što znači namjerno izazivanje straha stalnom prijetnjom nasiljem ili primjenom nasilja radi postizanja određenih političkih ciljeva“ (Hrvatska enciklopedija: 2022). Nataša Šakić tumači kako terorizam nije ideologija već strategija korištena od terorista, motivirana najčešće političkim stajalištima koji se ne slažu s vladajućim. Često se spominje usporedba terorista s gerilcima, ali ključna razlika leži u činjenici da se gerilski ratovi najčešće vode u planinama, daleko od gradova, dok teroristi napadaju nenaoružane protivnike u centrima državne moći. Zastrašivanje populacije je glavna namjera terorista. Podmetanje bombi, atentati i otmice spadaju među najčešće metode koje teroristi prakticiraju (1996: 152).

Teroristom se ne postaje brzo, već je to proces uvjetovan određenim socijalnim ili političkim aspektima. Simpatizeri terorističkih organizacija obično počnu davati podršku teroristima te postupno postaju vjerni članovi. Motivacija potencijalnog terorista i poželjnost od strane organizacije su samo neki od uvjeta koje kandidati moraju zadovoljiti ako žele postati članovi (Bilandžić, 2010: 841). Teroristička organizacija početnim članovima razvija osjećaj prihvaćenosti i samopoštovanja te se nad njima vrši pritisak kako bi u potpunosti pripali zajednici i pratili njene ciljeve. Također grade sustav mišljenja koji bi im omogućio dehumaniziranje žrtava, odnosno kako bi sam čin ubijanja smatrali prihvatljivim. Jednom kada se učlane, članovi ne smiju napustiti organizaciju te je kazna za takvo što brutalna, najčešće smrtna (Bilandžić, 2010: 840).

Mnogi smatraju da je masovni suvremeni terorizam počeo od napada na Sjedinjene Američke Države 11. rujna 2001. godine. Nakon tog napada terorizam dobiva na snazi u društvu u kojem živimo te Amerikanci pozivaju ostatak svijeta na zajedničku borbu protiv terorizma (Marić, 2012: 89). Ipak treba naglasiti da je terorizam masovna pojava od ranije; 60-ih godina prošlog stoljeća u svijetu ukupno je preko 600 aktivnih terorističkih organizacija. Od tada je počinjeno preko 80 tisuća terorističkih zločina (Bilandžić, 2010: 839).

Kanadsko-američki ekonomist John Kenneth Galbraith dijeli moć na tri vrste, kondignu, kompenzacijsku i kondicioniranu. Kondigna moć se veže uz kažnjavanje, dok se kompenzacijskom moći one koji se odluče podčiniti nagrađuje. Kod uvjeravanja ljudi i pripadnika kondicioniranom moći postupno vladari ili ljudi na čelu skupine mijenjaju uvjerenja onih koji se odluče na podčinjavanje. Uporabom kondigne moći, točnije, uz

pomoć represije, država je uspjela uništiti 47% terorističkih organizacija. Kompenzacijsku moć primjenjuju države kada traže od terorističkih organizacija odustajanje od uporabe terora te ih uključuju u demokratske procese da bi mirnim i legalnim putem ostvarili svoje ciljeve. U tom slučaju obje strane dobivaju nagrade. Uzevši u obzir da je organizacija mjesto povezivanja ljudi s istim interesima, kondicionirana moć dakle označava izviranje uvjerenja koje je nužno za ostvarivanje ciljeva (Bilandžić, 2010: 839-841).

Terorizam je danas dio cijelog svijeta i neupitno je da postoji, no ne smijemo i svaki događaj, pljačku ili nasilje nazivati terorizmom (Marić, 2012: 92). Pravnica Katarina Tomaševski tumači da je glavni problem objektivnosti prilikom proučavanja ljudske osobe, u svrhu dolaženja do uzroka terorizma, očitovanje čovječnog u toj osobi. Tvrdi kako se teroristi, kao i vojnici, služe strategijom impersonalnosti, pri čemu im žrtve postaju samo broj i ne razmišljaju o njima kao ljudima. Također tvrdi da se mogućnost ubijanja bez milosti opravdava, ne društvenim ili političkim uzrocima, već psihopatološkim (Tomaševski, 1981: 162-166).

3. Suvremeni terorizam

Teroristički napadi postaju učestali još tijekom 20. stoljeća, ali terorizam na globalnoj razini postaje sve naglašeniji u 21. stoljeću. Skoro pa svi mediji su izvještavali o terorističkim napadima te većina portala na internetu sadrže rubrike pod nazivom „terorizam“ (Marić, 2012: 91). Među najpoznatijim primjerima je medijsko praćenje terorističkog napada na Svjetski trgovački centar u SAD-u 11. rujna 2001. godine. Diljem svijeta prikazivale su se snimke rušenja takozvanih „blizanaca“, a mnogi mediji su izravno pratili slijed događaja (Tomljanović, 2016: 21).

Suvremeni je terorizam izrazito povezan s napretkom tehnologije, osobito informacijske i komunikacijske, a važnu ulogu imaju i sve rasprostranjeniji i dostupniji mediji i virtualne društvene mreže. Još jedan ključan čimbenik u cijeloj priči je činjenica da se povećava industrija naoružanja. Terorizam današnjeg doba kakvog znamo započinje tijekom vrhunca hladnoga rata i razvoja nacionalnih pokreta. Tijekom tog razdoblja stvaraju se mnoge organizacije i grupe koje terorističke poteze uzimaju za glavno političko djelovanje, točnije ostvarivanje vlastitih interesa i ciljeva (Marić, 2012: 93).

Teroristima je u prvom planu nanošenje što veće štete određenoj grupi ljudi i šire, no u zadnje vrijeme se koriste nestandardnim načinom ratovanja. Koriste se informacijom kao oružjem ratovanja jer informacija u sadašnjem svijetu vrijedi i donosi mnogo više posljedica od standardnih načina ratovanja (Marić, 2012: 93).

Korištenje suvremenih tehnologija omogućilo je teroristima bolju i bržu razmjenu informacija, tajno komuniciranje i financiranje. Financijska potpora je ključan element koji osigurava opstanak i djelovanje terorističkih organizacija (Marić, 2012: 93). Terorističke skupine se i financiraju uz pomoć interneta preko dobrovoljnih donacija i fondova koje vlasti teško uspijevaju kontrolirati. Primjer je Hizb-ut-Tahrir, međunarodna panislamistička organizacija, koja za transfer donacija korist PayPal (Babić, 2015: 17). Skupine terorista u današnje vrijeme imaju veće sustave financiranja i njima je puno kompliciranije ući u trag. Razlog tome je što se mnogo sponzoriranja terorista radi pod „krinkom“ pomoći za humanitarne organizacije (Marić, 2012: 94).

Terorizam se u svojoj biti nije mijenjao tijekom povijesti, ali terorizam kakav mi poznajemo je poprilično suptilniji i sofisticiraniji nego što je bio prije te su se tehnike ratovanja promijenile i modernizirale. Terorističke organizacije i napadi nisu slučajni postupci pojedinaca već pomno promišljeni oblici nasilja i napadi s već osmišljenim namjerama usađivanja straha u ljude (Marić, 2012: 93-94).

Što se tiče samoubojica tijekom napada, od osamdesetih godina prošloga stoljeća do 2003. godine samo je 3% oblika napada bilo samoubilačke vrste, međutim, nakon napada na SAD 11. rujna 2001. taj postotak raste na 80%. Danas svakodnevno možemo vidjeti u medijima vijesti o terorizmu i napadima, međutim samoubilački napadi nisu oblik napada ovog doba, jer su u prošlosti japanske kamikaze i židovski zeloti isto bili samoubojice. Danas je samoubilačka metoda najčešće prisutna među pripadnicima džihadista (Marić, 2012: 95). Marić definira samoubilački terorizam kao „spremnost pojedinca da žrtvuju život radi uništavanja ili pokušaja uništavanja nekog cilja, a u svrhu ostvarenja političkog cilja.“ (2012: 95-96).

Filozof Jean Baudrillard tumači suvremeni terorizam kao „teror protiv terora“ te ga uspoređuje s virusom naglašavajući da je on svugdje oko nas te je postao dio kulture koja se bori protiv njega. Također, suvremeni terorizam naziva četvrtim svjetskim ratom te dolazi do zaključka da terorizam ne dozvoljava bilo kakvom svjetskom poretku dominaciju te da se suprotstavlja mondijalizaciji koja je nemoralna kao i sam terorizam. Baudrillard ključni trenutak u obilježavanju suvremenog terorizma vidi u igranju terorista „na vlastitu

smrt ofenzivno i učinkovito“ i služenje intuicijom protiv gotovo savršenog sustava. Time su uspjeli oružjem protiv čitavog sistema učiniti vlastitu smrt (Baudrillard, 2003., prema: Tonković, 2014: 280).

Autori Gayraud i Senat ističu odličnu prilagođenost terorističkih organizacija današnjem, modernom svijetu i uzimaju u obzir neograničen pristup internetu koji dozvoljava teroristima bezbrižnu i neometanu komunikaciju u cijelome svijetu. Dolaze do zaključka da je terorizam staroga svijeta bio predvidljiv, usporen i slab, dok je u današnjem svijetu okrutan i nezaustavljiv (prema: Tonković, 2014: 282).

Sociologinja Anita Tonković postavlja pitanje možemo li na terorizam gledati kao na jednu vrstu antiglobalizacijskoga pokreta. Konstatira činjenicu da terorizam ima političke ciljeve kao jedan od svojih povoda ali i da je uzrokovan nepravdom. Jedna od negativnih strana globalizacije je što razvijenije države pod krinkom globalizacije postižu nadzor, dobivaju povlastice, povećavaju utjecaj i moć te postupno postaju sve superiornije, što postaje nesnošljivo onim zemljama u razvoju, jer dolazi do sve veće razlike između bogatih i siromašnih u cijelome svijetu (2014: 287).

Posljedica medijskih prenošenja terorističkih akcija je iskrivljeno poimanje realnosti. (Gayraud i Senat 2008., prema: Tonković, 2014: 287). Naime, razni mediji prikazuju stvarnost tako što sve pozitivno vežu sa zapadnim državama dok sve negativno asociraju s onim mjestima odakle potječu terorističke organizacije, nasilje, tirani, zločinci i područja bogata naftom (Perešin, 2007., prema: Tonković, 2014: 288).

3.1 Odnos terorizma i nacionalne i međunarodne sigurnosti

Doc. dr. sc. Ivan Perkov navodi kako je nakon napada na SAD 2001.godine osviještenost o opasnosti terorizma povećana. Europski sigurnosni diskurs po pitanju terorizma se javlja 70-ih godina prošloga stoljeća među članicama Europske unije. Na brojnim sastancima raspravljalo se o sigurnosti od terorističkih napada. 1975. godine u Rimu formirana je „TREVI-suradnja“, koja znači „*terrorisme, radicalisme, extremisme et violence international“*. U Finskoj 1999. godine je osmišljen „Tampere program“ u kojem bi se uz suradnju policije i pravosuđa radilo na unutarnjoj sigurnosti Europe. „Haški program“ je osmišljen također kao prevencija terorističkih napada (Perkov, 2013: 22-23). 2010. godine je na razini Europske unije ustanovljena Strategija unutarnje sigurnosti gdje su među prijetnjama Europi navedeni cyber kriminal i terorističke akcije. Tri su poglavlja navedene

Strategije, „Zaštita ljudi u Europi unutar globalnog društva“, „Prema europskom modelu sigurnosti“ i „Budući koraci“. U trećem poglavlju među glavnim zadatcima je sprječavanje funkcioniranja kriminalnih mreža s naglaskom na terorističke skupine. Također, prioritet je i „sprječavanje radikalizacije i novačenja članova terorističkih organizacija“ (Perkov, 2013: 32).

Prof. dr. sc. Mirko Bilandžić navodi kako je prva antiteroristička organizacija osnovana na području Hrvatske Antiteroristička jedinica Lučko. Nakon napada velikosrpske agresije na Hrvatsku jedinica je započela s djelovanjem na području čitave države (2009., prema: Milković, 2006). Zapovjedništvo specijalne policije sastoji se od šest postrojbi od kojih je najznačajnija za antiterorističko djelovanje Specijalna jedinica policije Zagreb, koja je naknadno pripojena Antiterorističkoj jedinici Lučko. Među ciljevima navedene jedinice je „rješavanje otmica ljudi i prijevoznih sredstava, snajperske i helikopterske operacije, pronalaženje, deaktiviranje i uništavanje formacijskih i improviziranih eksplozivnih naprava na zemlji i pod vodom te uhićenje naoružanih osoba“ (Bilandžić, 2009: 44-45). U sklopu Oružanih snaga na našem području u protuterorističkoj obrani također djeluju i Hrvatsko ratno zrakoplovstvo i Protuzračna obrana. Što se tiče obrane morskoga teritorija, Hrvatska ratna mornarica djeluje u obrani luka (Bilandžić, 2009: 47).

4. Kibernetički (cyber) terorizam

Riječ kibernetički dolazi od engleske riječi cyber koja „se odnosi na prividnu stvarnost nastalu s pomoću računala“ (Hrvatska enciklopedija: 2022). Kibernetski terorizam je napad u političku svrhu od strane pojedinaca ili skupina usredotočen na računalne programe, sustave i podatke, dakle bez fizičke borbe (Vuković, 2012: 18).

Autori Gordon i Loeb navode kako su mogućnosti tehnologije beskonačne kada se radi o kibernetičkom terorizmu. Krađa povjerljivih podataka, brisanje podataka, mijenjanje web stranica i napadi virusa najčešći su primjeri napada, a mete su državne računalne i financijske mreže, te elektrane (2005., prema: Janczewski i Colarik, 2007: 2).

Hrvoje Vuković smatra da se među početcima terorističkih napada putem računalne tehnologije podrazumijeva napad na nekoliko veleposlanstava Šri Lanke 1997. godine. Naime, internet Black Tigers, bivša teroristička grupa Šri Lanke, izvršila je napad na e-mail sustave kako bi onesposobila komunikaciju na određeno vrijeme u znak protesta protiv navedene vlade. Poslana poruka glasila je „We are the internet Black Tigers and we’re doing

this to interrupt your communications“, a opisani napad se smatra začetkom svih budućih kibernetskih oblika terorizma (2012: 18-19).

Postoje dva oblika terorističkog napada koje se mogu svrstati pod kibernetički terorizam. Pod prvim oblikom ciljem napada smatra se informacijska tehnologija. Teroristi ciljaju prekid komunikacije ili fizičko uništenje uređaja kao krajnju svrhu. Pod drugi oblik informacijska tehnologija se podrazumijeva kao oružje za određeni napad. Najčešći primjer bio bi mijenjanje funkcije tehnologije u vlastitu korist (Perešin, 2007: 106).

U kibernetskom prostoru informatika se koristi istovremeno kao strategija i kao cilj, a gotovo uvijek kao oružje. Napadači koji ne moraju nužno biti fizički prisutni na mjestu napada te manja količina potrebnih sredstava su također razlozi sve veće učestalosti kibernetičkih terorističkih akcija, kao i opcija sakrivanja vlastitog identiteta napadača (Vuković, 2012: 19).

1998. godine napadnuta je stranica i e-mail sustav Atomskog istraživačkog centra Bhabha u Indiji od strane trojice anonimnih napadača koji su u naknadnom intervjuu preko interneta obrazložili svoj postupak kao znak protesta protiv tadašnjih nuklearnih eksplozija (Briere, 2005., prema: Janczewski i Colarik, 2007: 2).

U novije vrijeme teroristički napadi mogu biti realizirani i uz pomoć dronova, bespilotnih letjelica. Svjetski vođe su izjavili kako postoji strah od zlouporabe dronova od strane terorističkih skupina. Naime, skupine mogu aktivirati eksplozije u nuklearnim elektranama, kao i uz pomoć dronova raspršivati nuklearni materijal u velike gradove, što bi dovelo do širenja panike, a možda i natjeralo određen dio stanovništva na selidbu. Strah postoji i zbog toga što džihadisti kupuju bespilotne letjelice za prijevoz nuklearnog materijala (Sovilj, 2017: 262). Islamska država u svojim napadima na Siriju i Irak koristi dronove, a smatra se da planiraju više letjelica koristiti u većim napadima na više ljudi (Sovilj, 2017: 257).

4.1 Propagandni materijali na internetu

Što se tiče terorizma u vrijeme interneta, zainteresiranim pojedincima, koji su aktivni na internetu, dostupan je mnogo veći broj informacija nego li je to bilo prijašnjim pripadnicima terorističkih skupina. Mnogi na internetu mogu pronaći informacije o izradi bombi, salafističkim publikacijama i džihadistima, „Islamskoj državi“. Također se mogu pronaći brutalne snimke odrubljivanja glave i ubijanja. Ono najbitnije što je dostupno pripadnicima

istih interesa je jednostavnija komunikacija i povezivanje diljem svijeta (Prodan, 2015: 102).

Brojni znanstvenici su se složili da internet služi kao ubrzivač radikalizacije te ju promovira. Jer osim za promidžbu i prenošenje poruka, internet je i od velikog značaja u određenim stadijima radikalizacije. Pod time se misli na kupnju vodiča za edukaciju i priručnika za izrađivanje bombi i dinamita (Precht, 2007., prema: Prodan, 2015: 102). „The Mujahedin poison handbook" priručnik je u kojem su detaljno opisana pravila za izradu bombi (Babić, 2015: 15).

Fotografije i videa koje teroristi postavljaju na internet uvelike pridonose radikalizaciji jer time dokazuju svoje stavove i poglede. Kod videa odrubljivanja glave može se vidjeti visoka kvaliteta i dobra režija, ali puno manje krvavih scena, što također pridonosi interesu tih skupina da takva videa dolaze do što više ljudi. Tih videa na internetu ima sve više i upravo njihova dostupnost je utjecala da se što veći broj ljudi pridruži džihadu. Primjer koji potvrđuje navedeno je što su u domovima većine uhićenih pripadnika tih skupina pronađene snimke dekapitacije (Prodan, 2015: 103). Na stranicama Sahab, Global Islam Media Front, al-Aqsa Martyrs' Brigades i Salafi Media Balkans napadači objavljuju snimke ubojstava i međusobno komuniciraju. YouTube i Google služe kao idealno mjesto za propagandne materijale. Iako se računi na tim stranicama vrlo brzo ugase, a videa obrišu, ipak zbog popularnosti tih stranica i svakodnevne uporabe počinitelji postignu svoj cilj, jer u malo vremena gledanost bude velika. Stranice s pornografijom nisu iznimka za postavljanje terorističkog sadržaja (Babić, 2015: 15).

Što se tiče najmlađih i najnevinijih pripadnika terorističkih skupina, djece, oni takve snimke smatraju potpuno normalnim, svakodnevnim scenama. To možemo vidjeti na primjeru osmogodišnjeg dječaka muslimanske vjeroispovijesti u čijem je stanu policija pronašla brutalne snimke dekapitacije, kojeg je prijavio njegov učitelj nakon što je saznao da je dječak iste snimke slao svojim prijateljima u školi. Ono što je najviše uznemirujuće je činjenica što su njemu te scene samo jedna zanimljiva kombinacija horor filma i igrice, što samo dokazuje koliko je on sa svojih osam godina otupio na nasilje i brutalne snimke. Upravo to dječje nepoznavanje i nerazlikovanje dobrog od zla te laka manipulacija njima, je ono što terorističke skupine kao Al Qa'ida i ISIL znaju i iskorištavaju. Tu djecu od rane dobi pripremaju na edukaciju koju će proći kada budu dovoljno odrasli za pristup skupini. Anonimnost interneta je ključna za umrežavanje i povezivanje svih pa tako i žena i

sramežljivih ljudi. To nije bio slučaj prije, ali danas je internet dostupan gotovo svima i na svim dijelovima svijeta. To također doprinosi radikalizaciji (Prodan, 2015: 103-104).

Termin psihološki rat profesor Vladica Babić koristi prilikom opisivanja služenja tehnologijom od strane terorističkih organizacija. Šireći dezinformacije i paniku putem elektroničke tehnologije teroristi uspijevaju prevariti veliki dio populacije te plasirati vlastitu ideologiju masi. Dok će jedan dio publike zastrašiti i obeshrabriti svojim viđenjima terorističkih napada, druge će privući i prenijeti im iste stavove bez obzira u kojem dijelu svijeta se nalazili. Vođe skupina su poznati i po tome što internetske stranice često gase ili preoblikuju, ali video snimke i poruke ostavljaju na dostupnost gotovo svima. Uzevši u obzir to i anonimnost koju internet omogućuje svima, vrlo je teško ući im u trag ili ih zaustaviti. Prema podatcima iz 2010.godine, oko 900 stranica s terorističkim sadržajem nastane na godišnjoj razini (Hsinchun, 2010., prema: Babić, 2015: 14). Postoji mnogo stranica, foruma, portala ili linkova pomoću kojih bilo tko može doći do informacija o terorističkim skupina, njihovih objava, video snimki ili videa gdje objašnjavaju kako izraditi smrtonosna oružja ili otrovne napitke. Inspire časopis je najpoznatiji primjer online časopisa u kojem teroristička skupina promiče svoje stavove i privlači nove članove, a vodi ga organizacija Al Qa'ida. U istom časopisu je objavljen „The Mujahedin poison handbook“, ranije spomenut u tekstu. Među ostalim propagandnim materijalima koji su djelovali putem interneta su stranice i časopisi poput Sawt al-Jihad, Sada al-Jihad , Al-Mujahid al-Taqni, Mu’askar al-Battar i Al Khansa.

Na našem području to su bile Vijesti Ummeta. Prvo su postojale kao portal, a zatim kao blog. Na tom regionalnom blogu glorificirana je aktivnost terorističkih skupina diljem svijeta, a strah i mržnja su bili dio propagandnog materijala. Zbog panike koju je blog širio je i uklonjen, kao i računi na društvenim mrežama istog imena (Tomljanović, 2016: 20).

David Copeland, osuđeni terorist, je 1999. godine u Londonu izvršio tri napada bombom prilikom kojih je ubio troje ljudi i ranio preko 130. Tijekom suđenja saznalo se da je bombe izradio uz pomoć materijala koje je pronašao na internetu. Radilo se o priručnicima „Terrorist Handbook“ i „How to make bombs“ (Janczewski i Colarik, 2007: 2).

Na području Jugoistočne Europe postoje brojne skupine u znaku podrške velikim terorističkim organizacijama poput Al Qa'ida-e i ISIL-a. Mlađi dio populacije najčešće simpatizira terorističke akcije putem online servisa. S obzirom da teroristi uvijek mogu iznova aktivirati servis ili stranicu, učinkovitije je praćenje njihove komunikacije preko

chat-soba ili foruma. Ali ti servisi nikada nisu pozicionirani na području Europe (Babić, 2015: 16).

4.2 Komunikacija unutar terorističke organizacije

Kod suvremenog terorizma online tehnologija koju koriste teroristi i ekstremisti u svrhu provođenja svojih akcija je poprilično velik broj uređaja koji im omogućuju što skriveniju i lakšu komunikaciju. Među najčešćim oblicima razmjene informacija su SIM kartice za mobilne uređaje koje su poprilično povoljne i legalne, a dostupne i služe jednokratno. Uz pomoć USB vanjskih memorijskih kartica neprimjetno razmjenjuju ogromne količine podataka. Također koriste satelitske telefone pazeći da ostaju u slabo naseljenim mjestima. Među popularnijim metodama je korištenje teklića, koju je koristio i Osama bin Laden, te tako godinama izbjegavao ostavljanje digitalnog traga. Najčešća i vrlo uspješna obrana od otkrivanja budućih napada je komuniciranje pomoću šifriranih poruka i korištenje metafora u razmjenjivanju SMS poruka. Primjer je komunikacija dvojice napadača na SAD 2001. godine, kada su Pentagon nazivali „umjetnošću" a Bijelu kuću „politikom" (Prodan, 2015: 115). Virtualna komunikacija danas se također odvija putem popularnih i svima dostupnih platformi kao što su WhatsApp, Viber i Skype (Babić, 2015: 17).

Komunikacija među teroristima otkriva i mnoge sofisticirane tehnike. Komuniciraju preko raznih komunikacijskih kanala među kojima je najvažniji, naravno, internet. Pretpostavlja se da danas postoji preko 4 tisuće stranica na kojima se odvijaju planovi budućih napada i „virtualni" teroristički rat. Naime, pripadnici tih skupina podatke postavljaju u obliku grafičkih ili zvučnih datoteka ne mijenjajući ni dužinu ni strukturu podataka. Ali ključ takvog komuniciranja je što takvim podatcima pristup imaju isključivo one osobe koje znaju što se nalazi u datotekama, koje informacije, te posjeduju određene „ključeve" ili programe pomoću kojih će pristupiti tim informacijama. Upravo zbog toga dolazi do problema razotkrivanja terorističkih planova obavještajnim službama (Prodan, 2015: 116-117).

Ne samo da tim načinom osmišljavaju planove za napad, već tako i obavještavaju vlade, prijete im te preuzimaju odgovornost za počinjena djela (Tomić, Musa i Primorac, 2012., prema: Prodan, 2015: 117).

Internet je u današnje vrijeme vrlo popularan jer je izuzetno jeftin. Male, tek osnovane, terorističke organizacije mogu imati golemu cyber zastupljenost te su time konkurencija puno većim organizacijama. Nadalje, pomoću interneta, omogućeno je i ne nužno

pripadnicima terorističkih skupina, načini i upute o sastavljanju samoubilačkog pojasa te njegove uporabe. Korisnici postižu anonimnost različitim načinima, većinom besplatnima, kao što je registriranje anonimnim računima iz usluga Yahoo, Hotmail i drugo (Prodan, 2015: 117).

Jedna od negativnih strana komuniciranja preko interneta, za teroriste, jest ta što se i obavještajne službe i sigurnosne snage mogu predstavljati kao dio grupe i stvoriti sumnju među teroristima. Stoga, teroristi više ni ne znaju kome vjerovati, a kome ne. Upravo zbog toga i teroristi trebaju biti na oprezu te se pouzdati na teže dostupnije forume koji im omogućavaju privatne i sigurne razgovore. To znači da će se uvelike povećati broj mjesta koje će sigurnosne službe teže pratiti. Također, koriste se i društvenim mrežama, primjerice Twitterom (Prodan, 2015: 117-118).

Najzanimljiviji način komuniciranja među suvremenim teroristima je kada jedna osoba drugoj pošalje poruku ali nikad ne pritisne tipku „pošalji“. Naime, drugoj osobi budu dostupni podatci za prijavu na račun prve osobe te tako druga osoba može vidjeti poruke prve osobe bez da joj je ova poslala. Upravo te podatke za pristupiti određenom računu dobiju pripadnici skupine (Prodan, 2015: 118-119).

Također, često komuniciraju preko mapa označenih kao „skice“. Određeni pripadnici imaju korisničke podatke koji im omogućuju pristup tim mapama te u njima ostavljaju poruke i međusobno komuniciraju. Tim načinom razmjenjuju informacije, prenose upute i planiraju terorističke napade (Prodan, 2015: 118-119).

4.3 Prikupljanje podataka

Ono što današnjim teroristima omogućava brzo prikupljanje informacija o meti napada, osobama uključenim u napad i slično je upravo internet. Naime, uz pomoć alata kao što su Streetview i Google Maps, počinitelji uspijevaju locirati građevinske oblike koji su im napad i sve puteve te teritorije koji su im potrebni, kao što javna dostupnost o zračnim linijama omogućava jednostavnije napade u zraku. Kada se radi o konkretnim osobama, društvene mreže su mjesto gotovo svih osobnih podataka meta, njihovih navika i svakodnevnih aktivnosti, što teroristima ne zahtjeva ni previše vremena ni financijskih sredstava za pronalaženje ciljne osobe/skupine. Aum Shinrikyo, japanski kult osnovan 1984. godine, je 2000. godine promatrao kretanje 150 prijevoznih sredstava japanske policije, uz pomoć GPS-a. GPS sustav je zapravo bio taj koji je otkrio navedeno

promatranje. Pored GPS metode, postoje i GSM, svjetski standard za mobilnu telefoniju, te GPRS, bežična podatkovna komunikacijska usluga, koje koriste i terorističke grupe kao i one antiterorističke (Babić, 2015: 16).

Kada govorimo o prikupljanju podataka, napadači do zaštićenih podataka meta dolaze na mnogo načina. Među najčešćim metodama je ilegalni sustav za pretraživanje lozinki te krađa identiteta. Inteligencija otvorenog koda, OSINT, tehnika je kojom se služe pripadnici Al-Qaid-e, kao i OSJ, Open Source Jihad, pomoću koje prikupljaju informacije i tu metodu javno objavljuju u svom časopisu Inspire (Babić, 2015: 16-17). U današnjem svijetu je pristupačnost internetu i elektroničkoj tehnologiji omogućena gotovo svakom čovjeku, isto tako i dostupnost jednostavnih i besplatnih lekcija o hakiranju (Nelson et al., 1999: 24-30).

4.4 Motivacija za kibernetički terorizam

Motivacije za kibernetskim terorizmom su različite. S jedne strane postoji unutarnja motivacija, pod kojom se podrazumijeva potreba za moći i samoispunjenjem pojedinca, dok s druge strane na potrebu za napadom utječu novac i odgovornost. Profil tipičnog terorističkog napadača je mlada osoba narcisoidnog ponašanja, otuđena od društva i interakcije. Terorističke grupe se u početku formiraju zbog zajedničkog interesa svih pripadnika, a tek kasnije se krenu usmjeravati na interese pojedinaca unutar te iste grupe. Među interesima skupine su rušenje države i uspostavljanje novog društvenog poretka te promicanje određene ideologije, dok je najčešći interes pojedinca moć ili osveta. Takve skupine ne financiraju svoje pripadnike i nemaju u cilju ostvariti njihove potrebe i želje koje se ne tiču skupine kojoj pripadaju (Nelson et al., 1999: 63-64).

Privlačeći nove kandidate, grupe putem interneta kontaktiraju i biraju nove članove. Kandidati prilikom predstavljanja trebaju imati osnovno znanje o vjeri i ubijanju, te određene psihičke i fizičke karakteristike. Drugi način pridobivanja novih članova je uz primjenu nasilja, ili prijetnji, a ponekad i novčanim podmićivanjem. Fenomen današnjeg priključivanja terorističkim skupinama je pojam samo-radikalizacije do koje dolazi jer pojedinac kontinuirano gledajući teroristički sadržaj i propagandni materijal sam osjeti potrebu za učlanjivanjem. Među članovima jedne grupe često se mogu pronaći visoko obrazovani ljudi s područja informatičke tehnologije ili hakerskih stručnjaka. Kibernetički terorizam je dosegnuo moć koju je nemoguće kontrolirati zbog njenog svjetskog razmjera. Mnogobrojne zakonske regulative također nisu uspjele zaustaviti problem, možda tek

kontrolirati ga do određene mjere. Ne postoje globalna ili općeprihvaćena pravila koja bi se mogla provoditi u svakom dijelu svijeta u kojem je terorizam postojan (Antoliš, 2015: 127). Razlozi za bavljenje specifično kibernetskim terorizmom su brojni. Među prvima je globalna povezanost. Naime, broj potencijalnih meta je puno veći nego kod standardnog terorizma a i samim time je publika veća. Financijski i vremenski troškovi su puno manji, a mogućnost kontrole i širenja ideologije puno raširenija. Drugo, sve je veća ovisnost o računalnoj tehnologiji. Teroristi svoje financijske potpore mogu pronaći ili nabaviti u većoj mjeri nego ikada prije, a posljedice napada su rasprostranjenije. Iako postoje konvencije o kibernetskom terorizmu, nedostatak pravnih konsenzusa omogućava napadačima sigurno utočište. Također, komplikacije se rađaju kada treba utvrditi identitet napadača u kibernetskom prostoru, što doprinosi okretanju kibernetičkom terorizmu (Nelson et al., 1999: 24-30).

5. Zaključak

Cilj ovog rada bio je temeljito raščlaniti suvremeni terorizam s naglaskom na kibernetički terorizam. Pod početkom masovnog terorizma smatra se napad na SAD 2001. godine. Teroristički napadi masovnost dobivaju i zahvaljujući medijima koji u suvremenom svijetu uživo prate terorističke napade. Nekoć su terorističke skupine bile zatvorenog tipa i malo se znalo o njihovim akcijama i budućim pothvatima. Današnje terorističke organizacije imaju puno više prednosti po pitanju komunikacije s ljudima i pripadnicima svojih skupina te brže i lakše nabavljaju sredstva za izvršavanje svojih terorističkih napada. Preko donacija i humanitarnih akcija terorističke grupe osiguravaju sebi financijsku potporu. Živimo u vremenu kada se većina stvari odvija i dogovara putem interneta, a terorizam nije iznimka. Krađe povjerljivih podataka i identiteta, brisanje podataka i napadi virusima su među najčešćim primjerima suvremenog terorizma. Informacijska tehnologija danas služi i kao cilj napada i kao strategija za izvršenje napada. Najznačajniji utjecaj terorističkih grupa se vidi u njihovim propagandnim materijalima koji su dostupni gotovo svima u bilo kojem dijelu svijeta. Zainteresiranim građanima je omogućeno uz pomoć računalne tehnologije pristupiti sadržaju terorističkih napada, dostupna je obuka uz pomoć brojnih priručnika, pa čak i stupanje u kontakt s članovima. Uz pomoć priručnika i vodiča za edukaciju ubrzano se širi radikalizacija diljem svijeta. Iako postoje mnogi načini upadanja u mreže terorističkih

ćelija, oni su također spremni i podržavaju stranice do kojih je teško doći, te forume i adrese na koje je još teže pristupiti. Jednom kada im se stranice uklone, a računi na društvenim mrežama blokiraju, oni uspijevaju iznova podignuti nove platforme na kojima će nastaviti svoju komunikaciju s građanima. Većina terorista ne moraju uopće biti u fizičkom kontaktu sa svojim kolegama a mogu dobiti upute i informacije isključivo putem interneta i komunikacijskih kanala. Kako napreduje razvoj tehnologije uz koju je moguće pratiti njihove akcije i buduće planove, tako i oni sami među sobom iznova otkrivaju nove metode za međusobnu komunikaciju. Motivi za pristupanje terorističkim organizacijama su brojni i raznoliki. Od čovjekove potrebe za samoispunjenjem, preko želje za moći, do onih koji su prisiljeni od strane vođa skupine. Danas postoje mnoge protuterorističke organizacije na nacionalnoj ili međunarodnoj razini koje se bave održavanjem sigurnosti i borbom protiv terorizma. Čimbenik koji je uvelike utjecao na popularnost terorističkih napada u kibernetskom prostoru je anonimnost koja je omogućena svima na internetu. Ta anonimnost je najveći problem procesa globalizacije u svijetu na svim razinama. Težili smo umrežavanju cijelog svijeta, što smo i dobili, ali nismo bili svjesni da nam upravo to može donijeti najveći problem po pitanju suvremenih terorističkih napada. S tim problemom se institucije, države i pojedine službe još uvijek bore i nastoje biti korak ispred njih, ali su svjesni činjenice da i teroristi također svakodnevno idu korak naprijed.

6. Bibliografske jedinice

1. Antoliš, K. (2010). Internetska forenzika i cyber terorizam. *Policija i sigurnost, 19* (1), 121-128.
2. Babić, V. (2015). Novi oblici djelovanja terorista (Cyber terorizam). In *4th International Scientific and Professional Conference 'Police College Research Days In Zagreb* (pp. 23-24).
3. Baudrillard, J. (2003.) *Duh terorizma,* Dubrovnik: Biblioteka Karantena, str. 10-11
4. Bilandžić, M. (2010.) „Terorizam u teorijama i teorijskim perspektivama", *Društvena istraživanja Zagreb,* sv. 20 (3): 837- 859
5. Bilandžić, M. i Milković, S. (2009). SPECIJALNE VOJNO-POLICIJSKE PROTUTERORISTIČKE POSTROJBE: HRVATSKA I SVIJET. *Polemos, XII* (24), 33-60.
6. Briere, D. (2005). Wireless network hacks and mods for dummies (for Dummies S.). Hungry Minds, Inc.
7. Bušljeta Tonković, A. (2014). SUVREMENI TERORIZAM – GLOBALNA SIGURNOSNA PRIJETNJA I/ILI OBLIK ANTIGLOBALIZACIJSKOGA DJELOVANJA. *Mostariensia, 18* (1-2), 277-292
8. Gordon, L., & Loeb, M. (2005). Managing aging cybersecurity resources: a cost-benefit analysis (1st ed.). McGraw-Hill.
9. Hsinchun C.,Thoms, S.,Tianjun F. (2008). Cyber extremism in Web 2.0: An exploratory study of international Jihadist groups, Tucson: Artificial Intell. Lab., Arizona Univ.
10. Janczewski, L., & Colarik, A. (Eds.). (2007). *Cyber warfare and cyber terrorism*. IGI Global.
11. „Kibernetički", *Hrvatska enciklopedija,* https://www.enciklopedija.hr/natuknica.aspx?id=68081 (datum posjećenja: 1.8.2022.)
12. Marić, S. (2012.) „Terorizam kao globalni problem"
13. Milković, S. (2006.) Uloga specijalne policije u borbi protiv terorizma. Magistarski rad. Zagreb: Visoka škola za sigurnost na radu, s pravom javnosti.
14. Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). Cyberterror Prospects and Implications.
15. Perešin, A., „Paradigma 'novog' terorizma informacijskog doba", Politička misao, 44 (2007.) 2, str. 93-112.

16. Perkov, I. (2013). *Europeizacija hrvatskog sigurnosnog diskursa* (Diplomski rad). Filozofski fakultet, Sveučilište u Zagrebu.
17. Precht, T. (2007.) *Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism. An Assessment of the Factors Influencing Violent Islamist Extremism and Suggestions for Counter Radicalisation Measures. Copenhagen: Danish Ministry of Justice*
18. Prodan, T. (2015). „Internet, terorizam, protuterorizam“, *National security and the future*, 16 (1), str. 93-143
19. Sovilj, D. i Poje Sovilj, M. (2017). Terorizam dronovima – novi način ratovanja?. *Policija i sigurnost, 26* (3/2017.), 255-266.
20. Šakić, N. (1998). „Terorizam“, *Polemos, I* (1), 151-158
21. „Terorizam“, *Hrvatska enciklopedija,*

    https://enciklopedija.hr/Natuknica.aspx?ID=60997 (datum posjećenja: 28. srpnja 2022.)

22. Tomaševski, K. (1980). Uzroci terorizma. *Revija za sociologiju, 10* (3-4), 161-172
23. Tomić, Z.; Musa, I.; Primorac, M. „Terorističke organizacije kao akteri političke komunikacije“ . Medianali - znanstveni časopis za medije, novinarstvo, masovno komuniciranje, odnose s javnostima i kulturu društva, Vol.6 No.11. lipanj 2012.
24. Tomljanović, M. (2016). *Dva fenomena suvremenog terorizma: uključenost žena u terorističke akcije i medijsko praćenje terorističkog djelovanja* (Završni rad).
25. Vuković, H. (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. *National security and the future, 13* (3), 12-31.