Internet, terorizam, protuterorizam

Tonći Prodan[1]

SAŽETAK: U današnjem globaliziranom društvu internet igra veliku ulogu za potrebe: novačenja, edukacije, radikalizacije, planiranja, pripreme, potpore i izvođenja terorističkih aktivnosti. Cilj ovog rada je rasvijetliti dio tih procesa te analizirati postojeće načine suprotstavljanja ovom složenom fenomenu. Pokrenute su brojne inicjative usmjerene ka suprotstavljanju korištenja interneta u terorističke svrhe, međutim, teroristi ga i dalje vrlo intenzivno i efikasno koriste za svoje potrebe, dok broj njegovih korisnika svakim danom raste sve većom brzinom. S obzirom na takvo stanje, potrebne su dodatne inicijative i suradnja na rješavanju ovog problema u koju moraju biti uključeni stručnjaci iz prakse, akademski stručnjaci, tvorci politika, uz povezivanje javnog i privatnog sektora te poticanje međunarodne suradnje i razmjenu najboljih praksi.

KLJUČNE RIJEČI: internet, terorizam, protuterorizam, radikalizacija, novačenje.

ABSTRACT: In today's globalized society, the Internet plays an important role in recruitment, education, radicalization, planning, preparing, supporting and carrying out terrorist acts. The objective of this paper is to shed light on some of these processes and analyse the existing ways of countering this complex phenomenon. Many initiatives have been launched to counter the use of the Internet for terrorist purposes, but terrorists are still

1 Dr. sc. Tonći Prodan je zaposlenik Ureda Vijeća za nacionalnu sigurnost RH u Zagrebu. Stavovi izneseni u ovom članku osobni su stavovi autora i ne mogu se ni pod kojim uvjetima smatrati službenim stavovima institucije u kojoj je autor članka zaposlen, niti izdavača publikacije u kojoj je članak objavljen.

using it very intensively and efficiently for their needs, while the number of its users keeps growing at an ever increasing rate. It is therefore necessary to introduce additional initiatives and cooperation on solving this problem, which must include experts with practical experience, academic experts and policy makers, in addition to connecting public and private sectors and encouraging international cooperation and the exchange of best practices.

***KEY WORDS**: Internet, terrorism, counterterrorism, radicalization, recruitment.*

Uvod

Suvremenim sigurnosnim strategijama međunarodnih sigurnosnih organizacija te nacionalnim sigurnosnim strategijama država diljem svijeta dominira problem terorizma. Terorizam je jedan od najopasnijih problema s kojim je suočen suvremeni svijet, a to su potvrdili teroristički napadi na Ameriku 2001., Španjolsku 2004., Ujedinjeno Kraljevstvo 2005., ponovno na SAD 2013., slučaj francuskog Charlie Hebdo-a s početka 2015. te brojni drugi teroristički akti. Očigledno je da ISIL iz dana u dan predstavlja sve veću terorističku prijetnju brojnim državama svijeta i sigurnosti uopće. Stoga, terorizam predstavlja interes mnogih znanstvenika, teoretičara, političara, novinara, profesionalnih pripadnika obavještajnih, sigurnosnih, vojnih i policijskih institucija.

Tehnološki razvoj nigdje nije bio tako dinamičan i sveobuhvatan kao u području komunikacijske i informacijske tehnologije, a taj se razvoj, dakako, odrazio i na terorizam. Nerijetko u medijima piše da teroristi koriste internet kako bi širili svoje ideje, a neki istraživači terorizma pretpostavljaju da se mladi muškarci na taj način mogu radikalizirati u samo nekoliko mjeseci.

Vijeće sigurnosti Ujedinjenih naroda je u svojoj Rezoluciji 1963[2] iz 2010. godine prepoznalo problem korištenja

[2] Rezolucija 1963 (2010) usvojena od strane Vijeća sigurnosti na njihovoj 6459. sjednici dana 20.12.2010. godine S/RES/1963 (2010). URL:http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1963(2010).Učitano 1.04.2015.

interneta u terorističke svrhe, izražavajući zabrinutost zbog povećane uporabe novih informacijskih i komunikacijskih tehnologija (osobito interneta) u globaliziranom društvu od strane terorista za potrebe novačenja i poticanja, kao i za financiranje, planiranje i pripremu njihovih aktivnosti. Također je prepoznalo važnost suradnje među državama članicama kako bi se spriječilo teroriste u iskorištavanju tehnologija, komunikacija i resursa za poticanje podrške za izvođenje terorističkih akata.[3]

Cilj ovog rada je rasvijetliti proces radikalizacije terorista putem interneta i uopće korištenja interneta u terorističke svrhe te analizirati moguće načine suprotstavljanja ovom fenomenu. Istraživanjem ćemo najprije utvrditi koliki problem doista predstavlja radikalizacija terorista putem interneta, koliko i kako ga teroristi koriste, te u skladu s rezultatima istraživanja razmotriti razvoj programa i politika kojima bi se djelotvorno moglo odgovoriti na ovaj problem, uz potpuno poštivanje temeljnih prava i sloboda, posebice slobode izražavanja.

Uvažavajući složenost istraživanog fenomena, rad je koncipiran tako da predstavlja pregled trenutnog pogleda na:

- Ulogu interneta u radikalizaciji i procesu novačenja terorista
- Načine na koji se internet koristi kao operativni alat terorista
- Raspon odgovora politika na korištenje interneta u terorističke svrhe

1. Uloga interneta u radikalizacijskom i procesu novačenja terorista

Posljednjih godina europski donositelji politika (*policymakers*), praktičari i akademska zajednica su počeli istraživati kako internet utječe na proces radikalizacije i oblike ekstremizama povezanih s terorizmom te kako pojedinci podržavaju terorizam. Mnogi se slažu da internet igra važnu ulogu kao radikalizacijski alat.[4] Awan ističe da je internet u posljednjih 15-20 godina postao glavna platforma za širenje i posredovanje kulture i ideologije džihadizma. U

[3] Isto. str.3.

[4] Akil N. Awan. *Virtual Jihadist Media. Function, Legitimacy and Radicalizing Efficacy*. / European Journal of Cultural Studies, 10(3), 389-408., 2007.; Anne Aly. '*The Internet as Ideological Battleground*'. / Edith Cowan University Research Online, 2010. str.4. URL:http://ro.ecu.edu.au/act/9. Učitano 5.4.2015.

svojoj analizi Awan istražuje funkcije novih džihadističkih medija, načine na koje oni zaslužuju legitimitet i uvjerljivost te učinkovitost u radikalizaciji i novačenju.

Osim što predstavlja središnji dio medijske strategije terorističkih skupina i mreža, korisnost interneta za teroriste proširila se i obuhvaća taktičke funkcije. U suvremenom terorističkom okruženju u kojem je psihološko ratovanje njegov sastavni dio, prisutnost na internetu je kritična za uspjeh terorista, kao financijska, taktička ili organizacijska sposobnost. Internet nudi komunikacijski prostor u kojem teroristi mogu identificirati, novačiti, indoktrinirati i utjecati na potencijalne članove pomoću različitih usluga dostupnih na internetu. Objašnjavajući novačenje, radikalizaciju i obuku, O' Rourke[5] navodi da teroristički entiteti pojačavaju svoje sposobnosti putem interneta kako bi se predstavili kao veća taktička prijetnja, nego što to fizički mogu postići. Internet se između ostalog koristi i za olakšavanje aktivnog novačenja pojedinaca koji su odrasli u zapadnim društvima te upoznavanju novih ljudi i raspravljanju pitanja u *Cyber* području.

Konstatacije koje na ovu temu susrećemo u medijima te znanstvenoj i stručnoj literatiuri izgledaju vrlo uvjerljivo, međutim, u rijetkim slučajevima su potkrijepljeni podacima koji su prikupljeni iz „prve ruke“ i koji su povezani s konkretnim slučajevima. Zbog toga ćemo u ovom radu analizirati konkretne primjere uhićenih pojedinaca koji su optuženi i/ili osuđeni za djela terorizma te za koje je dokazana (ili se dokazivala, istraživala) veza njihovih aktivnosti na internetu s terorističkim djelima za koje ih se teretilo, optužilo i/ili osudilo.

U ovom ćemo radu navoditi teze znanstvenika, kreatora protuterorističkih politika, stručnjaka iz područja terorizma te opservacije o povezanosti interneta s terorizmom, koje su općeprihvaćene u masovnim medijima, te ih uspoređivati i dovoditi u vezu s dokazima iz „prve ruke“. Radi se o dokazima do kojih su došli policijski istražitelji te suci u konkretnim sudskim postupcima. Također ćemo navoditi i analizirati izjave nekoliko osoba uhićenih i suđenih za djela povezana s terorizmom te njihovo viđenje uloge interneta u radikalizacijskom procesu. Dolaženje u posjed ovakvih dokaza izuzetno je težak proces i povezan je s teškoćama sigurnosne, proceduralne i logističke naravi, ali prikupljanje empirijskih dokaza od izuzetno je velike važnosti za

[5] Simon O'Rourke. *Virtual Radicalisation: Challenges for Police.* / Edith Cowan University Research Online, 2007. str. 30. URL: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1041&context=isw

istraživanje tako kompleksnog fenomena kao što je radikalizacija putem interneta.

Ono što bismo na samom početku mogli s velikom sigurnošću tvrditi jest to da je internet zbog svoje uloge u današnjem informacijskom dobu nedvojbeno jedan od važnih aspekata radikalizacije i da ga je nužno detaljnije istražiti kako bi se mogao shvatiti cjelokupni proces radikalizacije. O tome vrlo zorno svjedoči Tablica 1 iz koje je vidljivo koliko veliki broj građana Europske unije koristi internet, te koliki je godišnji rast korisnika interneta u osmogodišnjem razdoblju.

Tablica 1: RAST BROJA KORISNIKA INTERNETA U EU PO GODINAMA (%)

Godina	Broj korisnika interneta u EU po godinama (%)
2007.	55
2008.	60
2009.	66
2010.	70
2011.	73
2012.	76
2013.	79
2014.	81

Izvor: Eurostat 2015.

Kako je to vidljivo iz gornje tablice, broj korisnika interneta u Europskoj uniji je sa 55% u 2007. godini porastao na 81% u 2014. godini. Koliki je stvarni potencijal interneta kao alata za bilo koju namjenu, uz pomoć kojeg je moguće doprijeti do 81% stanovnika najmoćnije ekonomske integracije svijeta, suvišno je dodatno pojašnjavati.

U Tablici 2 je prikazan broj korisnika i učestalost korištenja interneta tijekom jedne godine (2014.), pojedinačno u svih današnjih 28 članica Europske unije.

Tablica 2: KORIŠTENJE INTERNETA I UČESTALOST KORIŠTENJA 2014. GODINE (% POJEDINACA)

Internet korisnici i nekorisnici **Frekvencija upotrebe (prosjek)**

	Korišten jednom u posljednja 3 mj.	Korišten ne s posla ni od kuće	Nikad korišten	Svaki dan ili skoro svaki dan	Najmanje jednom tjedno uključujući dnevnu upotrebu
EU - 28	**78**	**51**	**18**	**65**	**75**
Belgija	85	59	13	71	83
Bugarska	55	27	37	46	54
Češka Repub.	80	37	16	60	76
Danska	96	75	3	85	92
Njemačka	86	56	11	72	82
Estonia	84	58	12	73	82
Irska	80	65	16	65	76
Grčka	63	37	33	49	59
Španjolska	76	62	21	60	71
Francuska	84	58	12	68	80
Hrvatska	69	41	28	56	65
Italija	62	24	32	58	59
Cipar	69	43	28	56	65
Latvija	76	35	21	61	72
Litva	72	32	25	57	69
Luksemburg	95	70	4	87	93
Mađarska	76	44	22	66	75
Malta	73	51	25	63	70
Nizozemska	93	70	5	84	91
Austrija	81	57	15	64	77
Poljska	67	36	28	51	63
Portugal	65	37	30	51	61

Rumunjska	54	25	39	32	48
Slovenija	72	42	24	58	68
Slovačka	80	50	15	62	76
Finska	92	69	6	81	90
Švedska	93	76	6	83	91
Uj. Kraljevstvo	92	73	6	81	89

Napomena: Rumunjska, prekid u nizu u 2014. zbog rezultata popisa stanovništva 2011.

Izvor: Eurostat 2015.

Kako je to vidljivo iz gornje tablice, internet je u vrlo širokoj upotrebi u članicama Europske unije. Najmanje jednom tjedno koristi ga 75% stanovnika Unije.

Slijedom dosad prezentiranog, možemo se složiti s tezama znanstvenika i istraživača korištenja interneta u terorističke svrhe i istaknuti da internet olakšava proces radikalizacije, zato što je na raspolaganju mnogim ljudima diljem svijeta 24 sata dnevno, zbog čega predstavlja stalno dostupan: izvor informacija, medij za komunikaciju te prostor za širenje terorističke propagande i ekstremističkih vjerovanja.

Zbog svega toga se možemo složiti i s tezom da internet predstavlja svojevrsnu „eho komoru“, zato što komunikacijom ostvarenom s istomišljenicima putem interneta mišljenja i vjerovanja pojedinaca brzo pronalaze istomišljenike diljem svijeta i stvaraju odjek, zbog čega ti ekstremni pojedinci vrlo brzo dolaze do potvrde i odobravanja svojih ekstremnih stavova. U realnom životu („*offline*“) ovakav proces zasigurno nije moguć: niti može biti tako brz, niti može imati tako širok obuhvat (cijeli svijet).

Uspoređujući *online* i *offline* (klasičnu dosadašnju) radikalizaciju u nekim zemljama, navodimo podatak da nasilna radikalizacija u džamijama i drugim religijskim ustanovama ne obuhvaća više od 1% ili 2% od ukupnog broja radikalizacija,[6] što znači da radikalizacija ide drugim putevima te da je vjerojatno jedan od najplodonosnijih modela onaj koji se odvija uz pomoć *online* alata. Koja su to još okruženja podobna za provođenje radikalizacije te

[6] Roots of violent radicalisation, 2012. House of Commons Home Affairs Committee.. Str. 15. URL: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/1446.pdf, učitano 11. svibnja 2015,

njihovu usporedbu s internetom prikazat ćemo u narednom poglavlju.

Želimo podsjetiti da su se prije pojave interneta koristila neka druga okruženja, i još danas se koriste, za proces radikalizacije i novačenja terorista.

Tu se ubrajaju: obrazovne institucije, vjerske institucije i organizacije, zdravstvene ustanove, kazneno pravni sustavi (zatvori), dobrotvorni sektori i inozemstvo.7 Ilustracije radi, kada spominjemo obrazovne institucije, zanimljiv je podataka po kojem je 30% osoba koje su bile uključene u terorističke napade, pod vodstvom ili u suradnji s Al Qa'idom u razdoblju od 1999-2009, polazilo sveučilišta ili visokoškolske ustanove. Dodatnih 15% je polazilo ili steklo dodatnu stručnu kvalifikaciju.

Većina radikalizacija se danas odvija u privatnim prostorima, jednostavno zato što su teroristične organizacije i pojedinci koji provode radikalizaciju sada puno više svjesni aktivnosti koje se provode s druge strane kako bi se njihove aktivnosti spriječile, puno više nego je to bio slučaj prije nekoliko godina. U prijašnjem razdoblju je bilo puno više mogućnosti za provođenje radikalizacije na marginama vjerskih institucija: džamijama, medresama i drugim sličnim ustanovama.8

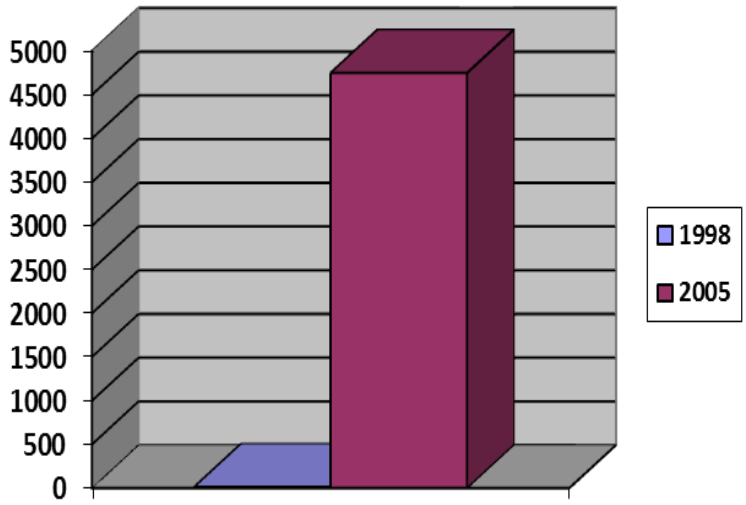
Slijedom svega dosad prezentiranog, radikalizacija se sve manje provodi u javnim institucijama kao što su to obrazovne i vjerske ustanove te specifičnim ustanovama kao što su zatvori, zbog čega nam je istraživanje uloge interneta u radikalizacijskom procesu osobito interesantno.

Kad je u pitanju korištenje interneta u terorističke svrhe, onda je u svakom slučaju najprije potrebno analizirati terorističke i ekstremističke mrežne stranice te utvrditi razloge – zašto i u koje svrhe teroristične organizacije uopće koriste internet. U tom smislu je nadalje važno analizirati kakve sve sadržaje teroristične organizacije postavljaju na internet, kako promoviraju ekstremističke ideje i opravdavaju nasilje te druge nelegalne aktivnosti, na koje *online* načine provode operativna istraživanja i pripreme za svoje terorističke ciljeve.

Kako bismo uvidjeli o kolikom rastu terorističkih mrežnih stranica se radi, dajemo grafički prikaz broja terorističkih mrežnih stranica 1998. i 2005. godine.

7 Isto. Str.13.
8 Isto. Str.18.

Grafički prikaz 1: USPOREDBA BROJA DŽIHADISTIČKIH MREŽNIH STRANICA 1998. I 2005. GODINE



Izvor: : http://www.arifyildirim.com/ilt510/vinay.lal.pdf, učitano 5. travnja 2015.

Na internetu postoji veliki broj pojmova koji se odnose na radikalizaciju putem interneta i tzv. *online* radikalizaciju te veliki broj pojmova koji potkrepljuju ranije iznesenu tezu kako se internet koristi u operativne svrhe. Tablica 3 potvrđuje ove navode. Pojmove smo pretraživali na engleskom jeziku kako bismo stekli širu sliku istraživanog fenomena. Hrvatski prijevod navedenih pojmova naveden je u točci 1. odmah ispod tablice.

Tablica 3: GOOGLE PRETRAŽIVANJE ZA PRIMJERE KRITIČNIH KLJUČNIH RIJEČI

Pretraživana riječ	**Broj rezultata**
„how to make a bomb“	388.000
„Salafi publications“	30.300
„jihadists“	7.080.000
„Islamic State“	48.000.000
„beheading video“	367.000

Izvor: Pretraživanje interneta korištenjem pretraživača Google hr. dana 1. srpnja 2015.

Kao što smo to vidjeli na primjerima prezentiranim u gornjim tablicama, internet umreženim i zainteresiranim pojedincima omogućava sljedeće:

1. Informacije o izradi bombi, džihadistima, salafističkim publikacijama, „Islamskoj državi“, video uratke odrubljivanja glava i slično, omogućavajući im tako bržu i lakšu radikalizaciju, ali i pripremu za provođenje terorističkih napada, bez uobičajene infrastrukture terorističke grupe.
2. Puno lakšu komunikaciju među ciljanim pojedincima i pronalazak istomišljenika diljem svijeta.

Znanstvenici su suglasni u tomu kako internetu u većini slučajeva pripada važna uloga u radikalizacijskom procesu, i to na način da promovira radikalizaciju. Osim što se koristi za propagandu, mjesto susreta i sredstvo za širenje poruka radikalnog islama u fazi pred-radikalizacije, internet se također koristi i za potrebe koje su od posebne važnosti u kasnijim fazama radikalizacije. To uključuje mogućnost nabave priručnika za obuku i priručnika za eksplozive.[9] Pojedine studije navode da je internet pojačivač ili ubrzavač radikalizacije te da ruši tradicionalne barijere pred pojedincima koji žele biti radikalizirani.

Sageman je sasvim izričit u navodima da internet može potaknuti još jedan poseban slučaj, a to je pitanje uloge interneta kao inkubatora ili akceleratora fenomena usamljenih vukova. Čini se da je internet vrlo učinkovit alat: on pruža prostor u kojem oni mogu dobiti radikalizacijski materijal, priručnike za obuku i adekvatne video uratke. To im pruža izravan pristup zajednici istomišljenika širom svijeta s kojima se povezuju, a u nekim slučajevima im može pružiti daljnji poticaj i smjer za obavljanje njihovih aktivnosti. Mnogi od pojedinaca uključenih u ove procese pokazuju neku razinu društvenog otuđenja pa, u tom kontekstu, zajednica stvorena na internetu može djelovati kao zamjena društvenom okruženju kojeg nisu u mogućnosti locirati i u njega se uključiti u stvarnom svijetu oko njih.[10]

Nadalje, internet korisnicima osigurava informacije koje su im potrebne kako bi potvrdili svoja vjerovanja (stavove). U tom su smislu osobito važne fotografije i video uratci koji

[9] Tomas Precht. *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 , December 2007.

[10] Raffaello Pantucci. *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists*. *Developments in Radicalisation and Political Violence*. International Centre for the Study of Radicalisation and Political Violence, 2011. str. 34.

pojačavaju konkretne poglede i mogu predstavljati snažne iskre za radikalizacijski proces.

Jedan od primjera korištenja interneta u ove svrhe je prikazivanje krvavih filmova, glavosjeka od strane pripadnika ISIL-a. Kao što smo to prikazali u Tablici 3 takvih je pojmova na internetu jako veliki broj. Snimke su kvalitetne, režirane i ne prikazuju cijelo pogubljenje, a čin se izvršava na otvorenom. Sve je jako dramatično, s manje krvi nego je to bio slučaj ranije, a sve kako bi te snimke mogle doći do što šire publike. Osim upozorenja nevjernicima, pogubljenja služe i kao način vrbovanja novog kadra. Naime, u zadnjih desetak i više godina značajan broj ljudi pridružio se džihadu upravo zbog ovakvih snimki pogubljenja, konkretno dekapitacije. Zadnji primjer koji potkrepljuje navedene teze da se radi o dobroj propagandi dolazi s uhićenjima pripadnika raznih terorističkih ćelija u Europi i u SAD-u. Snimke odrubljivanja glava nađene su u domovima gotovo svih uhićenih.

Posebno uznemirujući događaj zbio se 2008., kad je policija kod osmogodišnjeg dječaka muslimanske vjeroispovijesti pronašla zbirku videosnimki pogubljenja odsijecanjem glave. Ovaj je slučaj prijavio učitelj koji je primijetio da dječak šalje snimke svojim kolegama u razredu. Dječaku je dekapitacija gotovo savršena kombinacija horor filma i videoigrice. Opasno je što djecu takvi prizori otupe na nasilje, a Al Qa'ida i ISIL to savršeno dobro znaju, te žele iskoristiti tako što im džihadističku ideologiju čine dostupnijom, omogućujući im obuku kada dovoljno odrastu. Kako to ističe stručnjakinja za simbole Dawn Permutter, **s**avršen primjer indoktriniranog i obučenog džihadista jest „Jihadi John", krvnik koji je odsjekao glavu Jamesu Foleyu.[11]

Nadalje, internet pojedincima omogućava pronalazak istomišljenika i formiranje *online* zajednice", što ne bi bilo moguće *offline* tj. u običnom životu. U tom procesu koji se provodi unutar „*online* zajednice" provodi se normalizacija inače „nenormalnih" životnih pogleda i ponašanja, kao što su to ekstremistički pogledi o upotrebi nasilja za rješavanje određenih problema. Osim već navedenog, putem interneta je moguće dosegnuti do pojedinaca do kojih provoditelji radikalizacije, zbog raznih razloga, drugačije ne bi ni mogli doći. Nadalje, istim putem provoditelji radikalizacije dolaze i do žena12 za koje je često neprihvatljivo, u mnogim

[11] Vlado Ozretić. Slobodna Dalmacija, 26.02.2015. Str.10.

[12] Rachel Briggs i Alex Strugnell. *Radicalisation: The Role of the Internet. Policy Planners*' Network Working Paper, London: Institute for Strategic Dialogue, 2011.

kulturama, javno iznositi svoje stavove te se osobno susretati s muškarcima ili se priključiti njihovim grupama.

Sve je više dokaza koji ukazuju da anonimnost interneta nudi veću mogućnost za žene da postanu aktivne u ekstremističkim i džihadističkim krugovima na način kakav nije uobičajen u „offline“ svijetu.[13] Internet im u svakom slučaju pruža veću anonimnost, uz istovremeno ispunjenje njima zacrtanih ciljeva. Slična je situacija i sa sramežljivim osobama, kojima je puno lakše komunicirati putem interneta, nego osobno. Dakle, zahvaljujući internetu moguće je provesti proces radikalizacije, dijelom ili eventualno u cijelosti, bez fizičkog kontakta osoba.

Provedene studije o učincima interneta na radikalizaciju među 242 europska džihadista od 2001-2006. su ustvrdile da postoji korelacija između džihadističkih mrežnih stranica i propagande na internetu te brze radikalizacije zainteresiranih pojedinaca.[14]

Dajući jednostavan pristup radikalnom islamu i priliku za stvaranje domaćih i međunarodnih kontakata, internet igra veliku ulogu u svim fazama procesa radikalizacije, od pred-radikalizacije do izvođenja operacija. Internet je uklonio praktičnu prepreku za ulazak u terorizam čineći ga lakšim. Al Qa'ida je, primjerice, postigla veliki uspjeh za svoje ciljeve lansirajući visokokvalitetni mrežni magazin Inspire, koji je dostupan na internetu, a koji zagovara „džihad od kuće“. Inspire je vrlo široko distribuiran diljem Zapada šireći privlačnost nasilnog ekstremizma.

Tako primjerice lokalna Al Qa'idina franšiza iz Jemena AQAP širi *online* časopis Inspire, koji ponosno pronosi članak usmjeren na novačenje u Americi pod nazivom "Kako napraviti bombu u kuhinji tvoje mame". Inspire je naveden kao inspiracija nizu džihadističkih napada u SAD-u i Velikoj Britaniji. Suprotstavljajući se radikalizacijskim učincima Inspire-a, britanska policija upozorava da će biti uhićen i procesuiran svatko tko s interneta bude preuzimao navedeni list.

Slijedom svega prezentiranog, u javnosti postoji velika zabrinutost da bi korištenje interneta u terorističke svrhe moglo povećati terorističke aktivnosti, radikalizaciju ekstremnih pojedinaca i novačenje u terorističke

[13] *Radicalisation: The role of the Internet*. A working paper of the PPN. Institute for Strategic Dialogue Str.6. URL: http://www.strategicdialogue.org/allnewmats/idandsc2011/StockholmPPN2011_BackgroundPaper_FINAL.pdf

[14] Tomas Precht. *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.

organizacije. Ovi su strahovi dodatno pojačani pretpostavkama da internet pojedincima omogućava samoradikalizaciju.

Samoradikalizacija

Dosad nismo ulazili u detaljniju analizu pojma samoradikalizacije. Postoje ponešto različita gledanja na ovaj fenomen. Naime, za neke autore samoradikalizacija i radikalizacija preko interneta ista su stvar. Jedni, naime, misle na proces koji je lišen fizičkog kontakta i koji se u cijelosti provodi *online,* te može uključivati kontakt s ostalima, dok god se provodi na daljinu.[15] Bjelopera navodi da je aktivnost na internetu centralna u razvoju samopokretačkog (*self-starter*) fenomena[16] i da nudi željeno nasilno džihadističko deformalizirano radikalizacijsko iskustvo.

Utjecaj mrežnih aktivnosti na pojedince varira. U nekim slučajevima pristupanje i uključenje u online džihadističku retoriku pojedince potiče prema nasilju. Studija 18.130 unosa u 2112 online diskusija sa više od 15 džihadističkih foruma arapaskog jezika otkrila je da jedna petina svih razgovora uključuje eksplicitni poziv za više terorističkih napada.[17] Al-Lami pojašnjava da se ova samoradikalizacija u biti sastoji od pojedinaca koji se ovim putem upoznavaju i pod utjecajem su radikalnih ideologija, čak bez druženja s radikalnim skupinama. Gledajući biografije pojedinaca koji su uključeni u "džihad", čini se da radikalizacija nije rezultat jednog čimbenika, nego kombinacija nekoliko njih međusobno povezanih. Često se kao temeljno objašnjenje za radikalne aktivnosti navodi osjećaj poniženja, u ime veće zamišljene zajednice muslimana, te ljutnje prema percipiranoj zapadnoj hegemoniji i njihovom uplitanju.[18]

Drugi pak autori na samoradikalizaciju gledaju iz drugog kuta. Ono što po njima razlikuje samoradikalizaciju od radikalizacije putem interneta je da se samoradikalizacija odvija u izolaciji i podrazumijeva proces u kojem nije

[15] *The Internet as a Terrorist Tool for Recruitment and Radicalisation of Youth'*. Homeland Security Institute, 2009.

[16] Jerome P. Bjelopera. '*American Jihadist Terrorism: Combating a Complex Threat'*. Congressional Research Service Report for Congress, Washington, DC: Congress Research Service, 2011. Str. 104.

[17] Jerome P. Bjelopera. '*American Jihadist Terrorism: Combating a Complex Threat*'. Congressional Research Service Report for Congress, Washington, DC: Congress Research Service, January 23, 2013. Str. 21.

[18] Mina Al-Lami. *'Studies of Radicalisation: State of the Field Report'*. Politics and International Relations Working Paper Series, No. 11, London: University of London, 2009.

ostvaren kontakt s drugim teroristima ili ekstremistima, bilo osobno ili virtualno.

Prema mišljenju pojedinih znanstvenika, u većini slučajeva radikalizacije terorista do danas, aktivnosti na internetu su bile dopunjavane *offline* kontaktima i utjecajima. Društveno mrežni teoretičari, kao što je to primjerice Marc Sageman, zastupaju tezu da su odnosi iz stvarnog svijeta nužan dio radikalizacijskog procesa.[19] Nadalje, da uključenost u nasilje zahtijeva prethodni produženi proces „socijalizacije" u kojem percepcija osobnih interesa slabi, a vrijednost grupne lojalnosti i osobnih veza jača.

Dakle, veliki broj radikalizacijskih aktivnosti se odvija na internetu, u svojevrsnoj izolaciji i privatnosti. S tim u svezi, uočen je rastući trend Al Qa'ide u pronalaženju pojedinaca zainteresiranih za terorizam, prvenstveno zbog nedostatka njihovih prethodnih veza s džihadističkim mrežama, što ustvari predstavlja odgovor na pojačani obavještajni i policijski protuteroristički odgovor.[20] Utjecajni ideolozi, kao što su to Abu Musabal-Suri i Anwar al Awlaki, veliki akcent su stavljali na pojedinačni džihad i male ćelije koje poduzimaju akcije kad god su u mogućnosti, a sve kako bi unaprijedili strateške ciljeve Al Qa'ide i njihove globalne ambicije.

Produkcijske kuće

Kada je riječ o širenju informacija što je moguće šire, internet je odličan izbor.

Gledajući unatrag, neposredno nakon terorističkog napada na SAD 11. rujna 2001., vodstvo Al-Qa' ide je objavilo niz video uradaka iz svojih skrovišta u Pakistanu na TV postaji Al-Jazeera smještenoj u Kataru. Frustrirani odlukom kanala da će emitirati samo mali dio njihovih videa, Al-Qa'ida ih je zatim odlučila postaviti na internet. Od tada su Al-Qa'ida, Talibani i somalski al-Shabab razvili medijske produkcijske kuće kako bi „uzburkali" svoje *online* poruke, od kojih su neke proizvedene prema visokim standardima proizvodnje.

Online medijske organizacije počinju se preobražavati iz informacijskih centara u novinske agencije koje funkcioniraju na vrlo sličan način kao i velike novinske kuće poput Reutersa, Bloomberga ili Associated Pressa. U smislu njihove organizacije, postoji mali broj „stranica-majki" koje

[19] Marc Sageman. *Leaderless Jihad: Terrorist networks in the twenty-first century.* University of Pennsylvania Press, 2008. Str. 121.

[20] Jytte Klausen. *Al Qaeda-Affiliated and 'Homegrown' Jihadism in the UK: 1999-2010*. Institute for Strategic Dialogue, 2010.

predstavljaju izvor informacija i sadržaja za druge stranice takozvanog drugog ili trećeg reda. Ovakve medijske organizacije teroristima znače puno i od velike su im pomoći

Tri glavne terorističke medijske organizacije su: As-Sahab (The Clouds); Global Islamic Media Front (GIMF) i Al-Fajr („The Daybreak“).

Jedan od najinteresantnijih trendova u korištenju novih tehnologija u terorističke svrhe je rastuća upotreba novih društvenih medija od strane ekstremista i terorističkih mreža. Postoje dokazi o tome da džihadisti sada prihvaćaju ovaj pristup kao dio formalne i identificirajuće strategije, a postoje i primjeri mrežnih stranica koje pružaju detaljna uputstva teroristima i njihovim pristalicama o tome kako koristiti Facebook i YouTube za ove namjene.

Istraživanja obavljena na Dublin City University o maloj grupi pojedinaca koji su na internetu postavili i komentirali materijale koji se odnose na sukob u Iraku su pokazala kako pojedinci pretražujući generičke mrežne stranice mogu biti integrirani u specifičnu mrežu.

Cilj terorista je imati što brojnije članstvo i što veći krug podupiratelja. U posljednje je vrijeme registriran trend pokušaja prodora terorističkih organizacija prema široj zapadnoj publici na sljedeće načine:

1. Govori vođa Al Qa'ide i video produkcije terorističkih aktivnosti prevedeni su na zapadne jezike, osobito na engleski.
2. Uočena su značajna poboljšanja u kvaliteti prijevoda i upotrebi jezika
3. Utjecajne džihadističke stranice su proširene kako bi sadržavale engleske, francuske i njemačke odjeljke koji sadržavaju vijesti, razgovore, izvješća i video uratke o džihadističkom konfliktu.

S ciljem prenošenja terorističkih poruka, terorističke organizacije i mreže konstituirale su organizacije virutalnih medija koje igraju važnu ulogu u kreiranju džihadističkih publikacija i audiovizualnih materijala koji se onda mogu „pokupiti“ i proslijediti preko širokih društvenih mreža i foruma.

Neke od najpopularnijih islamističkih militantnih mrežnih foruma je lako usporediti po popularnosti sa stranicama bijelih „supremacista“ kao što je to primjerice Stromfront. Konstituiran je 1995.g. od strane pripadnika Klu Klux Klana, Don-a Black-a. Od 2009. ovaj forum je imao 150.000 članova, od kojih je 31.000 označeno kao „aktivno“.

Prema riječima bivšeg generalnog tajnika Interpola Ronalda K. Noble-a, registriran je ogroman porast broja

džihadističkih mrežnih stranica kojih je 1998. godine bilo 12, a 2006. godine ovaj se broj popeo na 4,500.[21]

Prema drugom izvoru,[22] dok je studija provedena 1998. godine otkrila 12 terorističkih stranica, analiza mreže provedena 2005. godine pronašla je 4.750 mrežnih stranica koje služe teroristima i nihovim podupirateljima.

Tablica 4: USPOREDNI PRIKAZ BROJA DŽIHADISTIČKIH MREŽNIH STRANICA 1998/2005.

Godina	*1998.*	*2005.*
Broj džihadističkih mrežnih stranica	*12*	*4750*

Izvor: Vinay Lal. Virtual Terrorism: How Modern Terrorist Use the Internet

Iako su od velikog značaja, *online* terorističke aktivnosti nije dobro promatrati isključivo i izolirano samo za sebe, već ih treba shvaćati i proučavati u sprezi s *offline* događajima i aktivnostima. Ne postoje ozbiljnije studije utemeljene na empirijskim podacima o tome u kakvoj su interakciji u konkretnim slučajevima bile *online* i *offline* aktivnosti pojedinih terorista te kakav je bio njihov međusobni utjecaj. Upravo zbog toga, makar i na malom uzorku, želimo prikazati dostupne konkretne podatke i dati odgovore na pitanja - kako su određeni nasilni ekstremisti koristili internet tijekom procesa njihove osobne radikalizacije, što je to bilo ključno u svakom pojedinačnom procesu radikalizacije te kakav je bio međuodnos *online* i *offline* ponašanja tih konkretnih pojedinaca. Ovi su podaci utemeljeni na osobnim kazivanjima osuđenika te analizi dokumenata do kojih je došla policija odnosno sud u postupcima suđenja za kaznena djela terorizma. Radi se o 15 slučajeva, od kojih je 9 počinitelja osuđenih temeljem *Terrorism Act* iz 2000. godine ili *Terrorism Act* iz 2006.godine.[23] Ovi se slučajevi odnose na islamistički i ekstremni desni terorizam. Jedan je

[21] URL: http://www.cbsnews.com/news/interpol-head-extremist-websites-skyrocketing/, učitano 18. travnja 2015.

[22] Vinay Lal. *Virtual Terrorism: How Modern Terrorist Use the Internet*, str. 8. URL: http://www.arifyildirim.com/ilt510/vinay.lal.pdf, učitano 1.svibnja 2015.

[23] Ines von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon. *Radicalisation in the digital era - The use of the internet in 15 cases of terrorism and extremism*. Rand Corporation, 2013.

slučaj bivšeg pripadnika Al Qa'ide koji je bio aktivan u Bosni, Afganistanu i Jugoistočnoj Aziji prije nego je prestao s terorističkim aktivnostima. Pet slučajeva se odnosi na program preventivne intervencije (*PREVENT intervention programme*) koji dotiče ranjivost (*The Channel Programme*). Kao što smo naveli, do nekih se podataka o upotrebi interneta u terorističke svrhe došlo kroz razgovore sa samim osuđenicima, međutim, valja imati na umu da, iako je intervjuiranje terorista važan alat, ipak sadrži samo dio podataka koji doprinose našem cjelokupnom razumijevanju njih i može nas, u nekim okolnostima, obmanuti.[24]

Analizom svih navedenih slučajeva je utvrđeno da internet nedvojbeno stvara više mogućnosti za proces radikalizacije. Također, svi analizirani slučajevi su pokazali da im je internet služio kao „eho komora", o čemu smo govorili u prethodnom dijelu rada. Suprotno uvriježenom mišljenju, analizom navedenih 15 slučajeva nije nedvojbeno utvrđeno da je internet ubrzao proces radikalizacije ovih pojedinaca. On je nedvojbeno omogućio proces njihove radikaliazcije, ali se ne može tvrditi da ga je i ubrzao. Nadalje, u većini ovih 15 istraživanih slučajeva se pokazalo da se radikalizacija nije odvijala bez fizičkog kontakta, već suprotno, da je kod većine ovih pojedinaca to bio slučaj. Konačno, analiza ovih 15 slučajeva nije potvrdila tezu da internet povećava mogućnosti za samoradikalizaciju, u onom smislu da se cijeli proces odvijao u izolaciji. Mnogi od slučajeva tzv. o*nline* samoradikalizacije su uključivali virtualnu komunikaciju i interakciju s drugima.

Analiza 15 konkretnih slučajeva[25] je pokazala sljedeće:

1. U svih 15 slučajeva internet je bio ključni izvor informacija, medij za komunikaciju i/ili platforma za ekstremističku propagandu.

T1 i T2 su koristili internet da bi naučili kako se izrađuju bombe. T4 je tražio uputstava kako se izrađuju samoubilački prsluci. PT2 je na internetu provjeravao gdje i kada će se održavati prosvjedi. Njemu je, primjerice, bio jako privlačan kapacitet distribucije poruka internetom (brzina, doseg...). T7, koji je rastao u konzervativnoj sredini, u kojoj nije bilo dopušteno gledanje TV-a, internet je koristio kao medij za stjecanje znanja i kontakt s ljudima, te je pozitivno hranio njegovu radikalizaciju. T5 je internet doživljavao kao

[24] Marc Sageman. Leaderless Jihad. Str. 19.

[25] Pojedince koji su osuđeni za kaznena djela terorizma označit ćemo slovom T, a pojedince koji su osuđeni temeljem *Prevent Intervention Programme*-a označit ćemo s PT.

područje anonimnosti i to je bio ključni faktor za njegovo korištenje interneta.

T10 je na internetu raspravljao o vojnoj obuci, dok su T7, T8 i T9 internetom širili poruke Al Qa'idine ćelije u Ujedinjenom Kraljevstvu.

T3 koji je odrastao kada su bile u upotrebi VHS kasete, uvidjevši kako internet omogućava puno veći doseg i publiku, uspješno je ovim putem širio radikalizacijske poruke. T3 je internet shvaćao kao širenje bazena za unovačitelje: "Internet je poput ribarske mreže, lovi površinsku ribu, a ne ribu s dna. Nekad smo hvatali jednu po jednu, sad hvatamo 100-200 u godini".[26] Kao bivši radikalizator, T3 je u svom intervjuu istaknuo prednosti interneta nad drugim instrumentima, navodeći kako je prije puno vremena morao provoditi po kafićima i zalogajnicama kako bi širio terorističke ideje.[27]

Neki teroristi obuhvaćeni ovom analizom (T1 i T2) su bili skeptični prema sigurnosti upotrebe interneta pa su, radije nego da se odluče da ne koriste internet, investirali u opremu za kriptiranje poruka i programe za brisanje kompromitirajućih sadržaja.

2. U većini slučajeva internet je predstavljao „eho komoru".

Internet može dati iluziju o brojčanoj snazi konsenzusa i kao takav može služiti kao normalizirajući posrednik.[28]

Bez obzira da li džihadističke *online* aktivnosti vode pojedince prema nasilju, internet služi za poticanje radikalizacije na tri načina. Prvo, omogućava džihadistima pojačavanje njihovih poruka sa sugestivnim audio i video uratcima. Drugo, potencijalnim džihadistima čini lakšim pronaći istomišljenike širom svijeta i s njima stupiti u interakciju. Konačno, internet "normalna ponašanja smatra neprihvatljivim i neprimjerenim u stvarnim uvjetima." Teroristi objavljuju *online* retoriku koja istiskuje krivnju za njihove nasilne radnje, koje oni obično opisuju kao nezaobilazne reakcije kada su suočeni s nadmoćnim neprijateljima, kao što je to Zapad.

Analizirajući 15 konkretnih pojedinaca suđenih za kaznena djela terorizma, a vezano za njihovu aktivnost na internetu, ističemo da su T1, T3, T5, T6, T10 i PT2 dali svoj doprinos na mrežnim forumima koji su promovirali diskusije

[26] Ines von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon. *Radicalisation in the digital era - The use of the internet in 15 cases of terrorism and extremism*. Str. 26.

[27] Isto. Str. 27.

[28] Jerome P. Bjelopera. 'American Jihadist Terrorism: Combating a Complex Threat'. Congressional Research Service Report for Congress, Washington, DC: Congress Research Service, 2011.

o ekstremističkim temama. T4 je istomišljenike tražio od džamije do džamije, kako bi s nekim podijelio razmišljanja, i nakon što nikog ne bi našao odlazio bi u *online* potragu. T4 se držao podalje od internet prostora za razgovor (*chat room*) i nije želio debatirati. Na internet bi odlazio prvenstveno kako bi prikupio informacije, a ne da bi se uključivao u debate i razgovore. T6 je s druge strane želio svoje poglede testirati i rado se uključivao u *online* debate. Kad nije bio zadovoljan debatom, ili je bio ignoriran, otišao bi u *offline* svijet, naučio više o raspravljanim temama, te se ponovno vraćao u debate. Kako je utvrđeno analizom njegovih aktivnosti, *online* prisustvo T6 na internetu bi opadalo poslije takvih situacija, ali bi se on ponovno vraćao u *online* debate nakon nekog vremena.[29] Za PT3 snaga interneta je bila u traženju istomišljenika, zahvaljujući čemu se mijenja osobno mišljenje da samo ti imaš takve osjećaje o nečemu.

Većina informacija do kojih je došla policija govori da osuđeni teroristi, koji su obrađeni u ovoj studiji, generalno nisu tražili informacije koje bi mogle dovesti u pitanje njihova ekstremistička uvjerenja. Važno je uzeti u obzir da tomu može biti tako zbog činjenice da se te informacije odnose na kasni stadij pojedinčeve radikalizacije, ili pak da su do takvih informacija dolazili s različitih profila ili kompjutera. Prema mišljenju policije, nepouzdano je uzeti kao reprezentativne informacije o upotrebi interneta do kojih se došlo pretragom računala svakog od optuženih ili osuđenih pojedinaca. Naime, to je zbog toga što tehnički dobro educirani pojedinci mogu koristiti odvojena računala sa različitih lokacija, mogu imati više korisničkih imena te mogu upadati u druge profile ili izbrisati informacije s kompjutera kojeg su koristili.[30]

3. Internet omogućava (radije nego ubrzava) proces radikalizacije

Analizom 15 prethodno navedenih slučajeva teško je zaključiti je li internet ubrzao ili nije njihovu radikalizaciju, jer se radi o malom uzorku, ali takav je zaključak teško donijeti i zbog toga jer nedostaju podaci o tome što su istraživani pojedinci još radili dok su koristili internet (unutar i izvan toga vremena). Trebalo bi analizirati više faktora prije sagledavanja kompletne slike o svim činiteljima koji su pridonijeli radikalizaciji. Kako je to istaknuo T3, *online* iskustvo svakog pojedinca je svojstveno njemu samom: dok

[29] Ines von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon. *Radicalisation in the digital era - The use of the internet in 15 cases of terrorism and extremism*. Annex A Figure 6.

[30] Isto. Str. 27.

internet može učiniti informacije lakše dostupnima, njihov utjecaj na daljnji proces razlikuje se od pojedinca do pojedinca.[31] U većini slučajeva internet je olakšao proces i on ga, sa svoje strane, može i ne mora ubrzati.

T1 i T2 su proces radikalizacije gradili tijekom više godina. T5 je konačno odbio internet kao put ka radikalizaciji. T4 i njegovo iskustvo također pokazuju da internet nije nužno ubrzao njegov radikalizacijski proces. (Razdoblja njegove *online* neaktivnosti prije uhićenja ukazuju da su vanjski faktori mogli ubrzati njegovu radikalizaciju isto koliko *online* aktivnosti, ili više od njih.)[32]

4. Većina slučajeva uključuje *offline* aktivnosti koje su mogle igrati ulogu u radikalizaciji pojedinca

Dokazi studija slučaja pokazuju da i *online* i *offline* faktori igraju važnu i međupovezanu ulogu u radikalizacijskom procesu. Događaji iz stvarnog (fizičkog) života se prožimaju s onima *online* i obrnuto. Dobiveni dokazi govore da internet ne predstavlja zamjenu, nego dodatak osobnoj komunikaciji.

Prije osude T1 i T2 u tisku je objavljeno da se njihova radikalizacija odvijala isključivo *online*. Iako je pregled njihovih *online* aktivnosti pokazao da su T1 i T2 s interneta preuzimali ekstremističke materijale, ipak je više utjecaja na radikalizaciju imao njihov međusobni odnos.[33] Kako je to utvrđeno analizom konkretnih slučajeva, na radikalizaciju T2 je utjecao T1, koji je bio aktivan *offline. Naime,* T1 je sudjelovao na konferenciji i tamo dobio disk s ekstremističkim materijalima. Osobni kontakti su prevladali i u slučaju T5 koji je potvrdio da je ključno za njegovo okretanje prema *online* radikalizaciji bilo njegovo odrastanje uz oca, koji je bio aktivan na ekstremističkim mrežnim stranicama.

Istraživanje je pokazalo da *offline* faktori mogu ponekad igrati veći utjecaj nego *online* faktori. T10 je primjerice pristupio teroristički vođa iz Pakistana u centralnoj džamiji u Dewsbury-u. Nakon tog susreta, T10 i teroristički vođa su počeli redovito komunicirati *online*. Ovaj slučaj pokazuje da je internet za T10 primarno predstavljao izvor informacija, a ne fokus njegove radikalizacije. Slično slučaju T10, model za radikalizaciju T6 i njegovo pridruživanje teroristima je počelo s osobnim kontaktima ispred američkog veleposlanstva. T3 je radikaliziran u Bosni 1990-ih prije pojave Interneta.

[31] Isto. Str. 28.
[32] Isto. Str. 28.
[33] Isto. Str. 29.

5. Većina slučajeva tzv „*online* samoradikalizacije“ uključuje virtualnu komunikaciju i interakciju s drugima

U istraživanim slučajevima uočen je vrlo mali broj dokaza koji bi podržavao postojanje samookidača (*selfstarters*). Većina obrađenih slučajeva u ovom istraživanju je uključivala virtualne i/ili fizičke kontakte među pojedincima.

Za studije slučaja T kategorije, kako se pokazalo tijekom suđenja, *offline* i *online* interakcije su prilično jasne. T1 je, primjerice, koristio 5 Facebook računa kako bi *online* komunicirao s drugim ekstremistima. T3 je bio okružen ekstremistima od rane dobi, T5 je *slijedio svog oca* u ekstremizmu, T6 i T10 su bili uočeni od strane terorističkih vođa, dok su T7, T8 i T9 imali radikalizacijske efekte jedan na drugoga.[34]

Poseban problem predstavlja upotreba interneta kao terorističkog alata za novačenje i radikalizaciju mladih. Terorističke grupe sistematično, u različitim kontekstima, vrebaju ranjivosti mladih ljudi nudeći im razne poticaje – od financijske podrške do nečeg poput obiteljskih obveznica, obećanja nečeg uzbudljivog, kako bi pripadnost grupi učinili privlačnom.[35]

Kao primjere novačenja djece u terorističke svrhe navodimo primjer Palestinskog islamskog džihada i Hamasa koji su regrutirali djecu u dobi od 13 godina da budu bombaši-samoubojice i djecu u dobi od 11 godina za krijumčarenje eksploziva i oružja.[36] Tijekom 2003. godine 13-godišnje blizanke koje su bile unovačene od strane terorističke grupe povezane s Al Qa'idom uhvaćene su u pokušaju samoubilačkog bombaškog napada na zapadne poslovne zgrade i lokalne vlade u Maroku.[37]

Mjera do koje se djeca - vojnici (mlađi od 18 godina) trenutno koriste za sudjelovanje u sukobima dosad nikada nije viđeno. Više od 300.000 djece, dječaka i djevojčica danas služe kao borci i bore se u gotovo 75% svjetskih sukoba. U oko 80% sukoba uključuju se djeca mlađa od 15 godina, u prosječnoj dobi od 12 godina.[38]

---

[34] Isto. Str. 30.

[35] *The Internet as a Terrorist Tool For Recruitment&Radicalization of Youth.* Homeland Security Institute, 2009. URL: http://www.homelandsecurity.org/docs/reports/Internet_Radicalization.pdf, učitano 15. svibnja 2014.

[36] Peter W. Singer “The New Children of Terror.” *The Making of a Terrorist: Recruitment, Training and Root Causes,* vol. 1. James J.F. Frost (ed.) Praeger, November 2005.

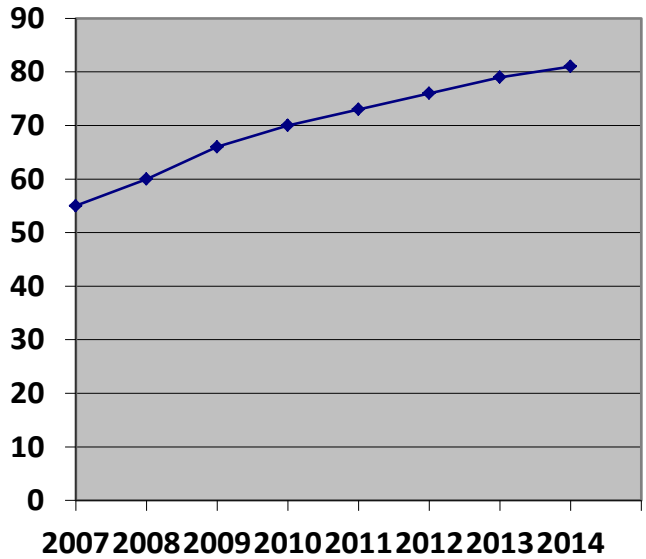
[37] Isto.

[38] *Recruitment and Radicalization of School Aged Youth by International Terrorist Groups, Final Report*, April 23, 2009. USA Department of

Neke su terorističke grupe dizajnirale specijalne mrežne stranice za mlađu publiku putem kojih prenose propagandne poruke preko crtanih filmova i kompjuterskih igara, te nije čudno da se posljednjih godina izvješćuje o povećanom trendu potencijalnog samoradikaliziranja mladih putem interneta.

Godine 1998. bilo je ukupno 12 mrežnih stranica povezanih s terorizmom, da bi taj broj 2003. godine narastao na oko 2630 stranica i da bi u siječnju 2009. došao do broja od 6940 aktivnih terorističkih stranica.

Grafički prikaz 2: RAST BROJA DŽIHADISTIČKIH MREŽNIH STRANICA U EU PO GODINAMA %



Izvor: Eurostat 2015.

Analizirajući aktualne trendove, po kojima broj korisnika interneta iz godine u godinu znatno raste, a što je jasno vidljivo iz Tablice 1, za ustvrditi je da Internet već više godina igra i da će ubuduće igrati sve veću ulogu u radikalizaciji i novačenju terorista, koordinaciji njihovih aktivnosti odnosno za ostale operativno teroristička svrhe o kojima ćemo detaljnije govoriti u sljedećem poglavlju.

Education. HSI. Str. 65. URL: http://www.cleanitproject.eu/wp-content/uploads/2012/07/2009-recruitment-and-radicalization.pdf, učitano 15. svibnja 2014.

2. Upotreba novih *online* tehnologija od strane terorista i ekstremista za operativne svrhe

Kao uvod u ovo poglavlje navest ćemo nekoliko dosad najčešće korištenih načina komunikacije među pripadnicima terorističkih organizacija.

- Sim kartice za mobilne telefone - jeftine su i zakonito dostupne. Mogu se kupiti anonimno, upotrijebiti jednom i baciti.
- **USB vanjske memorije - malih su dimenzija i diskretan način za prijenos velike količine podataka, koji su visoko ranjivi na zlonamjerne sadržaje i viruse.**
- Satelitski telefon - unatoč tehnologiji šifriranja, oni ii dalje ostaju osjetljivi na presretanje. Terorističke vođe su odavno oprezni kod njihovog korištenja, osobito iz udaljenih, slabo naseljenih područja.
- Teklić (dostavljač) - Bin Ladenova metoda koju je godinama koristio. Sofisticirani teroristi su svjesni rizika ostavljanja „digitalnog traga“, koji se može pratiti i identificirati. Ovako se izbjegava ostavljanje digitalnog traga, ali, naravno, još uvijek je potreban dostavljač, čovjek koji se može pratiti. Zato je, između ostalog, američkim obavještajnim službama trebalo toliko dugo vremena da otkriju i uhite vođu Al Qa'ide Osamu bin Ladena,[39] koji se oslanjao upravo na ovakvo prenošenje poruka i podataka.
- Komunikacija šifriranim porukama elektronske pošte i SMS tekstualnim porukama – oprezni teroristički planeri ističu potrebu šifriranog komuniciranja ili upotrebu metafora kad razgovaraju o svojim metama, zato što imaju u vidu da njihova komunikacija može biti presretnuta. Primjerice, dvojica planera terorističkog napada na SAD, Mohammed Atta i Ramzi Binalshibh, Svjetski trgovački centar nazivali su „arhitetkturom“, Pentagon su nazivali „umjetnošću“, a Bijelu kuću „politikom“.[40]

[39] Ubijen je od strane US Navy Seals u Pakistanu 2011. godine.

[40] Prema drugom izvoru, stručnjaku za terorizam John-u Thompson-u, Al-Qaida je poznata po korištenju vjerskih pojmova zajedno s kodnim riječima - obično nazivanim velom govora. U svojim razmjenama pokušavaju nasamariti vlasti. Na primjer, koristili su pojmove kao što su "Želimo paket bijelog sljeza", ili "Što se dogodilo s tim paketom bijelog sljeza," kako bi opisali eksploziv.
Navedeno u: *Terrorist Use of the Internet The Real Story*. URL:http://www.au.af.mil/au/awc/awcgate/jfq/terr_internet_2q07.pdf

Svaki dan se pojavljuju novi dokazi o načinima na koji teroristi koriste internet kao operativni alat uključujući: novačenje, obuku, prikupljanje novčanih sredstava, koordinaciju i komunikaciju. Također, uočen je trend intenziviranja i širenja propagandnih napora kojima podupiru sve naprijed navedeno.

Na internet stranicama pojedinih terorističkih organizacija, primjerice Al Qa'ide, mogu se naći upute za otmice, upute za izradu svih vrsta eksploziva, upute za izradu improviziranih auto-bombi, otrova, pogubljenja i drugo.

Za potrebe ovog rada, a kao potvrdu ranije iznesenih teza, pretražili smo nekoliko pojmova koji su povezani s terorističkim operacijama.

Tablica 5: GOOGLE PRETRAŽIVANJE ZA PRIMJERE KRITIČNIH KLJUČNIH RIJEČI

Pretraživana riječ	**Broj rezultata**
„how to make a bomb“	388.000
„beheading video“	367.000
„how to make suicide vests“	8.390

Izvor: Pretraživanje interneta korištenjem pretraživača Google hr. dana 1. srpnja 2015.

Kao što je iz tablice vidljivo, jako je veliki broj pojmova povezanih s terorističkim operacijama koji se mogu pronaći na internetu, a odnose se na upute za izradu bombi, samoubilačkih pojaseva, video uradaka odsijecanja glava te brojnih drugih, teroristima vrlo korisnih informacija.

Postoje dvije temeljne kategorije poruka: tajne i javne. Obje nose rizik otkrivanja pošiljatelja. Komunikacija unutar organizacija i pojedinaca najčešće nije otvorena, već najčešće kodirana. U djelovanju terorista mogu se otkriti i razne sofisticirane tehnike komuniciranja. Naime, njihova tajnost djelovanja primorava ih na izradu sofisticiranih tehnika komuniciranja preko nekoliko komunikacijskih kanala.

Najvažniji kanal komuniciranja za teroriste je internet. Stručnjaci procjenjuju da danas ima oko 4.000 stranica na internetu preko kojih se odvija «virtualni» teroristički rat i planiraju stvarni napadi. Teroristi kodiraju podatke u okviru grafičkih ili zvučnih *file*-ova ne narušavajući njihovu strukturu, pa čak ne mijenjajući njihovu dužinu. Tako kodirane informacije može pročitati samo onaj tko zna da

takav *file* nosi informaciju i posjeduje odgovarajući ključ. Kodirane poruke značajno otežavaju rad obavještajnim službama na otkrivanju terorističkih planova.

Internet ne samo da služi za internu komunikaciju između terorističkih skupina i pojedinaca, već on služi i za komunikaciju sa suprotstavljenim stranama. Mnoštvo je primjera u kojima teroristi putem svojih mrežnih stranica upozoravaju strane (neprijateljske) vlade, informiraju o svojim (zlo)djelima, preuzimaju odgovornost, prijete im, predlažu itd.[41]

Zašto baš internet?

Internet ima pet karakteristika koje ga čine idelanim alatom za terorističke organizacije. Prvo, teroristima omogućava brzu međusobnu komunikaciju u realnom vremenu, ali jednako tako omogućava kreiranje mrežne stranice koja je dostupna milijunima ljudi diljem svijeta. Instrukcije, obavještajne informacije pa čak i sredstva (fondovi) mogu biti odaslani i primljeni elektronskom poštom u sekundama. Drugo, upotreba interneta je jeftina. Treće, svepristunost interneta znači da male terorističke grupe mogu imati globalnu *cyber* pristunost, čime su konkurentni puno većim organizacijama. Četvrto, razvojem novih tehnologija i softvera omogućava čak i priprostim korisnicima razvoj i širenje složenih infomracija (npr. videoisječak s uputama o tome kako sastaviti samoubilački bombaški pojas, uz demonstraciju njegove uporabe na modelu autobusa punog putnika). Peto, moderne tehnologije enkripcije omogućavaju korisnicima surfanje internetom, prijenos novčanih sredstava i anonimno komuniciranje. Kako bi postigli anonimnost, teroristi mogu preuzeti različite vrste, za korištenje jednostavnih, računalnih sigurnosnih softvera od kojih su neki komercijalni, a neki od njih su i besplatno dostupni. Također, mogu se registrirati na anonimnim računima e-pošte iz usluga kao što su Yahoo ili Hotmail.

Korištenje novih tehnologija i društvenih mreža u teroristične svrhe ima svoje brojne prednosti, ali i neke nedostatke. Jedno od najvećih ograničenja ove vrste društvenih medija je njihova otvorenost i transparentnost. Naime, terorističko oslanjanje na mrežne stranice i forume omogućava praćenje njihovih metoda i trendova izvana. Oslanjanje na internet također otvara mogućnost policijskim i sigurnosnim snagama da se predstave kao dio grupe s ciljem dezinformiranja, ili jednostavno kako bi stvorili sumnju

[41] Zoran Tomić, Ilija Musa, Marijan Primorac. *Teroristička 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.

među teroristima koji tada više ne znaju kome mogu vjerovati.[42]

Zbog svih navedenih razloga teroristi su prisiljeni osloniti se na više zatvorene forume za komunikaciju i koordinaciju naprednije prirode. Dakle, unatoč upotrebi polujavnih foruma, teroristi i dalje trebaju sigurna i privatna mjesta za sastajanje, komunikaciju i koordinaciju njihovih aktivnosti. U tom smislu, njihova upotreba takozvanih „dubokih" ili „tamnih" mreža vjerojatno će se znatno povećati i to je jedno od najtežih područja za nadziranje od strane policijskih i sigurnosnih snaga.

Postoje primjeri upotrebe društvenih medija od strane terorističkih mreža kao pomoć pri izvođenju terorističkih operacija (praćenje kretanja policije i sigurnosnih snaga preko „eyewitness Twitter updates").

Drugi način korištenja interneta je kao sredstva komunikacije među pripadnicima terorističkih skupina. To je, primjerice, slučaj sa Al Qa'idom i Osamom bin Ladenom, koji je u određenim razdobljima sa pripadnicima Al Qa'ide komunicirao preko prenosivih računala (laptop) i posredstvom bežične mreže putem kriptiranih poruka. Pripadnici terorističkih organizacija i operativnih grupa i danas se, više nego ikad, u svojoj međusobnoj komunikaciji aktivno koriste internetom i raznim drugim servisima dostupnim na internetu. Njihovi teroristički, operativni, odnosno zapovjedni centri komuniciraju sa operativnim grupama, koje čine uglavnom po trojica ili više terorista, preko elektronske pošte koja se provjerava preko internet računa *(webmail)* koje otvaraju na raznim besplatnim, anonimnim servisima za poštu (yahoo, gmail itd). „Mrtve javke"[43] u današnjem digitalnom vremenu predstavljaju način na koji jedna osoba šalje poruku drugoj osobi preko interneta, ali, što je najinteresatnije, ne pritiskajući tipku pošalji *(send).* Primatelju poruke su dostupni podaci za logiranje na internet račun pošiljatelja tako da može vidjeti poruku i odgovoriti ako je potrebno.

Naime, korisničke podatke, dakle korisničko ime i lozinku, nakon otvaranja takve internet pošte dobijaju

[42] Teroristi brzo uče iz svojih pogrešaka i međusobno šire najbolju praksu o tome kako pobijediti taktiku koju koriste obavještajne, sigurnosne i policijske službe. U tome su vrlo vješti, premještaju svoje mrežne stranice kad su ugrožene, zbog čega ih je teško pratiti i "skinuti" ih s Interneta.

[43] Nicole Bogart. Terrorist organizations use variety of techniques to communicate with overseas cohorts, Global News, 23.4.2013. URL: http://globalnews.ca/news/504972/terrorist-organizations-use-variety-of-techniques-to-communicate-with-overseas-cohorts/). Učitano 2. travnja 2015.

pripadnici određene terorističke operativne grupe, te preko pošte koja se čita isključivo u samom internet prostoru *(webmail)* komuniciraju na način da se ta adresa ne koristi za slanje poruka trećim osobama, ili na druge adrese, nego trojica ili više korisnika međusobno razmjenjuju poruke na način da poruke ostavljaju u *folderu* označenom kao „skice" *("drafts")*. Kako sva trojica imaju korisničko ime i lozinku iste elektronske pošte koja se provjerava preko mreže, oni koriste tu adresu i u tom *folderu* mogu pročitati poruku koja im je ostavljena, a koja ustvari predstavlja operativna uputstva za postupanje ili izvođenje konkretne akcije te terorističke grupe.

Ovo je jedna od korištenih tehnika Al-Qa'ide, izbjegavanjem fizičkog traga papira i/ili e-pošte. Ovu tehniku je uspješno koristio Khaled Sheikh Mohammed za komunikaciju s globalnom mrežom Al-Qa'ide, inače osumnjičen kao vođa terorističkog napada od 11. rujna 2001.[44]

Sigurnosne službe danas raspoloživom tehnologijom mogu nadzirati jedino promet između pojedinih točno određenih elektronskih adresa, dakle poštu koja kruži mrežom. Međutim, ako sa određene elektronske adrese nema prometa prema vani, prema mreži, odnosno prema trećim adresama, zasad nema načina nadzora što se događa na tim otvorenim virtualnim poštanskim sandučićima. Zbog toga je opisani model međusobne komunikacije terorista danas najčešći način na koji terorističke grupe izbjegavaju nadzor sigurnosnih službi nad komunikacijom njihovih pripadnika, a vjerojatnost da će sigurnosne službe otkriti ovu komunikaciju je vrlo mala, s obzirom da bi za to službe trebale znati točnu adresu, korisničko ime i lozinku preko kojeg se takva komunikacija odvija.[45]

Drugi način, danas vrlo uobičajen u komunikaciji terorističkih organizacija, je komunikacija šifriranim porukama preko različitih internet foruma, gdje terorističke organizacije u obliku šifriranih tekstova ostavljaju poruke svojim terorističkim ćelijama, koje ih mogu tada javno pročitati. Društvene mreže, *chat* sobe i igre popularan su način prikrivanja poruke u naizgled bezazlenim interakcijama među online "igračima". Mnogi online forumi su šifrirani i zahtijevaju lozinke kako bi im se moglo pridružiti, međutim u

[44] Isto

[45] Mina Zirojević Fatić. Zloupotreba interneta u terorističke svrhe, MP 3, 2011. URL: *http://www.doiserbia.nb.rs/img/doi/0025-8555/2011/0025-85551103417Z.pdf. Učitano 12*. lipnja 2014.

neke od njih se ipak mogu dobro infiltrirati pripadnici sigurnosnih službi koji se predstavljaju kao *online* militanti. Napadi mogu biti različite prirode, a jedan od njih je JPEG kompresija

Gifshuffle je jedan od programa koji sakriva digitalnu informaciju. Ovaj je postupak poznat kao „steganografija" ili umijeće skrivanja poruka u tekst. Digitalne slike ovako kodirane mogu se upotrebljavati za prijenos drugih podataka, koristeći bezazlene naslove predmeta (poruka).

Za razbijanje i otkrivanje ove komunikacije također je potrebno nabaviti šifrarnike svake pojedine grupe, kako bi se takve poruke mogle identificirati i dešifrirati. Identifikacija korisnika koji se na određenim internet forumima koriste takvom komunikacijom u terorističke svrhe je zasad vrlo teška ili gotovo nemoguća.

Kao sredstvo za širenje svojih ideja koriste se sva dostignuća interneta, među kojima moramo posebno istaknuti i programe za čavrljanje (IRC-*Internet Relay Chat*), koji zasad jedini omogućavaju neposredno komuniciranje među točno određenim korisnicima u realnom vremenu, čime se omogućava neposredna povezanost. Ovo dalje znači da članovi terorističkih organizacija mogu sinkronizirati svoje djelovanje pred akciju i/ili dobiti povratnu informaciju odmah (*feedback*). Ova metoda je za teroriste relativno sigurna, jer sigurnosne agencije ne mogu pratiti ove istovremene razgovore na internetu (nema prepoznavanja glasa kao kod telefona, svi tragovi se brišu odmah).

Nadalje, razvoj posebnih tipografija otežava rad sigurnosnih službi. Naime, koriste se posebni znakovi ASCII znakovi *(American Standard Code for Information Interchange*, Američki standardni znakovnik za razmjenu informacija ili Američki standardni znakovnik za razmjenu obavijesti*)* koji su vizualno veoma slični arapskim slovima, što omogućava sporazumijevanje na računalima koji ne podupiru arapski jezik, ali isto tako se ne prikazuju kao arapski znakovi, čime izbjegavaju programsko prepoznavanje. Usporedo sa ovim znakovima, mladi Arapi posebno u Europi su razvili poseban jezik sporazumijevanja čije pismo se sastoji usporedo sa arapskim i engleskim slovima.[46]

Internet sadržaji poput popularnih programa Facebook i Google programa za detaljno pretraživanje zemlje (Google Earth) se također zloupotrebljavaju u ove svrhe. Izraelska

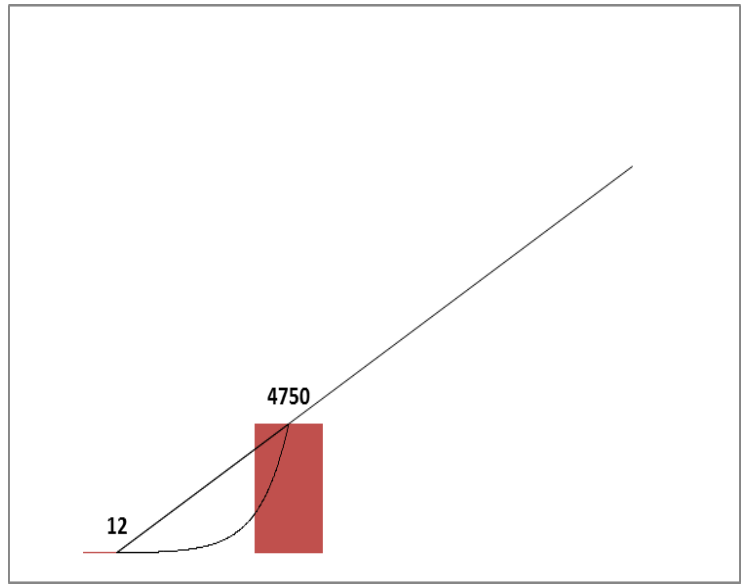
[46] Mina *Zirojević Fatić. Zloupotreba interneta u terorističke svrhe, MP 3, 2011. Str. 420-422.* URL: *http://www.doiserbia.nb.rs/img/doi/0025-8555/2011/0025-85551103417Z.pdf. Učitano 12. lipnja 2014.*

služba Shin Bet objavila je upozorenje da teroristička organizacije regrutiraju putem internet stranica Facebooka.

Državni sud u Indiji tražio je ukidanje Google programa za detaljno pretraživanje zemlje koji omogućava virtualni 3D prikaz zemljine površine. Indijska pravosudna tijela smatraju da su teroristi koji su krivi za krvavi napad u glavnom gradu Mumbaiju koristili navedeni program prilikom planiranja napada u kojem je poginulo više od 170 ljudi. Policija u Mumbaiju tvrdi da su teroristi koristili satelitske snimke gradskih ulica i hotela da bi uspješno izveli plan napada. Jedan od pripadnika terorističke organizacije Lashkar-e-Taiber priznao da je imao satelitske snimke Indije sa spomenutog programa.[47]

Rast broja mrežnih ekstremističkih stranica prikazan u Grafičkom prikazu 3 vrlo zorno pokazuje da se radi o problemu koji iz godine u godinu postaje sve veći.

Grafički prikaz 3: PRIKAZ TRENDA RASTA BROJA DŽIHADISTIČKIH MREŽNIH STRANICA 0D 1998. DO 2005. GODINE



Izvor: Izvor: http://www.arifyildirim.com/ilt510/vinay.lal.pdf, učitano 5.travnja 2015.

[47] Isto

Iz svega dosad prezentiranog, očito je da ekstremisti i terorističke skupine vrlo učinkovito koriste internet za svoje potrebe.

Kako i koliko teroristi koriste internet za vršenje *cyber* napada - pitanje je koje je prelazi okvire ovog rada, ali je vrlo zanimljivo, jer se takvim napadima nanose velike štete, bez izvođenja fizičkih napada.

3. Odgovori politika na korištenje interneta od strane ekstremista

Europski pravni okvir, između ostalog, pokriven je dvjema konvencijama Vijeća Europe (CoE) koje doprinose preveniranju upotrebe interneta od strane terorista: Konvencija o prevenciji terorizma, 2005[48] i Konvenicja o cyber-kriminalu, 2001.[49] Obje su otvorene za potpis nečlanicama Europske unije.

Konvencija Vijeća Europe o cyber kriminalu je međunarodni sporazum koji se bavi materijalnim i procesnim pravom u cyber području kriminala, uključujući upotrebu interneta u terorističke svrhe. Ova Konvencija olakšava međunarodnu suradnju u istragama i procesuiranju kompjuterskog kriminala.

Konvencija Vijeća Europe o prevenciji terorizma sadrži odredbe koje su relevantne u borbi protiv upotrebe interneta od strane terorista.

Od 2005. godine naovamo Europska komisija te Pravosuđe i unutarnji poslovi Vijeća (*Justice and Home Affairs*) su počeli sa stavljanjem visokih prioriteta na suzbijanje radikalizacije. Ometanje aktivnosti mreža ispitujući načine sprječavanja (ometanja) terorističkog novačenja korištenjem interneta postao je glavni cilj EU-a.

Europska komisija je podržala informacijski portal „*Check the Web*“,[50] inicijativu koja je strijemila suradnji i podjeli zadaća nadzora i procjene otvorenih internetskih izvora na dragovoljnoj bazi. Inicijativa je potekla od strane Europskog vijeća i njegovih zaključaka[51] od 15/16. lipnja

[48] Convention on thePrevention of Terrorism, 2005, CETS No 196. URL: http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG, učitano 2. svibnja 2014.

[49] Convention on Cybercrime, 2001, CETS No 185. URL: http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG, učitano 2. svibnja 2014.

[50] URL: http://register.consilium.europa.eu/pdf/en/07/st08/st08457-re03.en07.pdf, učitano 5. svibnja 2014.

[51] Doc. 10633/06 CONCL 2 BRUSSELS EUROPEAN COUNCIL 15/16 JUNE 2006 PRESIDENCY CONCLUSIONS, Brussels, 16. June 2006.

2006. godine u kojima stoji kako internet igra značajnu ulogu u logističkim, operativnim i komunikacijskim aktivnostima terorističkih organizacija, da se koristi za širenje terorističke propagande, za radikalizaciju, novačenje i obuku terorista, za širenje instrukcija kako izvesti konkretni napad, za prijenos informacija, kao i za svrhe financiranja terorista. Kao prioritetne zadaće EU je postavio onemogućavanje korištenja interneta kao temelja za radikalizaciju i novačenje terorista. EU u ovoj inicijativi posebno ističe značenje suradnje među državama članicama u borbi protiv korištenja interneta u terorističke svrhe. Europol i države članice Europske unije aktivno nadziru i procjenjuju terorističke mrežne stranice (posebice islamističke) te u međusobnoj komunikaciji, koja se odnosi na novačenje terorista i utvrđivanje faktora koji doprinose nasilnoj radikalizaciji, istražuju mogućnosti uklanjanja s interneta sadržaja koji se koriste za radikalizaciju pojedinaca u terorističke svrhe. Ovakve aktivnosti iziskuju enormne ljudske i tehničke potencijale, tako da je uspjeh moguće postići jedino podjelom zadaća između država članica, na dragovoljnoj osnovi. Odgovornost svake pojedine članice u konkretnom slučaju odnosi se na praćenje, ometanje ili gašenje pojedine terorističke mrežne stranice. Suradnja kroz informacijski portal dopunjena je redovnim susretima nacionalnih stručnjaka. Zemlje članice su tad započele raditi na zajedničkim projetkima i to podjelom zadaća oko analiziranja Al Qa'idinog medijskog odjela „As-Sahab“, kojeg smo već naveli kao jednog od tri najznačajnije organizacije ovog tipa.

Direktiva Audiovisual Media Service (AMS) Directive (2010) je propisala da države članice Europske unije trebaju na odgovarajući način osigurati da audiovizualne medijske usluge koje pružaju pružatelji medijske usluge u njihovoj nadležnosti ne sadrže bilo kakvo poticanje mržnje na temelju rase, spola, religije ili nacionalnosti.[52]

Godine 2010. EU je utemeljila Clean IT project[53] s namjerom započinjanja otvorenog i konstrutivnog dijaloga između vlada, poslovnog i javnog (civilnog) sektora (društva) kako bi istražili načine, donijeli zajedničke zaključke i

[52] Direktiva 2010/13/EU Europskog parlamenta i Vijeća od 10. ožujka 2010. o koordinaciji određenih odredaba utvrđenih zakonima i drugim propisima u državama članicama o pružanju audiovizualnih medijskih usluga (Direktiva o audiovizualnim medijskim uslugama). URL: http://europa.eu/legislation_summaries/audiovisual_and_media/am0005_en.htm, učitano 10. ožujka 2014.

[53] Europska komisija financira istraživački projekt za utvrđivanje alata i tehnologija raspoloživih za detektiranje radikalizacije na internetu, te potiče razmjenu i promociju najboljih praksi između EU članica. URL: http://www.cleanitproject.eu, učitano 10. ožujka 2014.

istaknuli najbolje prakse za reduciranje korištenja interneta od strane terorista, a koje će podržati javni i privatni sektor. Valja istaknuti kako je internet u velikoj mjeri u privatnom vlasništvu i upravljanju. Projekt je započeo u lipnju 2011. godine s financijskom potporom Europske komisije i pet partnerskih vlada (Belgija, Njemačka, Nizozemska, Španjolska i Ujedinjeno Kraljevstvo).Tijekom provođenja projekta priključilo se još šest vlada partnera (Austrija, Danska, Grčka, Mađarska, Rumunjska, Portugal).

Dokument *Reducing terrorist use of the Internet* publiciran je u siječnju 2013. godine i rezultat je strukturiranog javno-privatnog dijaloga između predstavnika vlada, znanstvenika, internetske industrije, internetskih korisnika i nevladinih organizacija u Europskoj uniji. Dokument se sastoji iz tri dijela. U Poglavlju 1 su navedene definicije. Preambula (Poglavlje 2) je skicirana od strane predstavnika vlada, zato što je prioritetna zadaća vlada opisivanje opasnosti terorizma i kako teroristi koriste internet, zašto je teško smanjiti upotrebu interneta od strane terorista i zašto bi javni i privatni sektor trebali raspravljati i surađivati na smanjenju upotrebe interneta od strane terorista. Opći principi u Poglavlju 3 određuju 9 uvjeta[54] za bilo koju akciju koja će se poduzimati s ciljem reduciranja upotrebe interneta u terorističke svrhe. Poglavlje 4 ističe 12 najboljih praksi koje mogu smanjiti upotrebu interneta u terorističke svrhe. Obzirom da se radi o vrlo konkrektnim podacima o uočenim problemima, te navođenju najboljih praksi o tome kako prevladati postojeće probleme, ukratko ćemo opisati svih 12 slučajeva: 1. Upotreba interneta u terorističke svrhe često nije jasno objašnjena. Pravni okvir bi

[54] Ukratko: 1. Sve organizacije se moraju suprotstavljati upotrebi interneta od strane terorista, 2. Bilo koja akcija poduzeta na ovom polju mora biti u skladu s nacionalnim, EU i međunarodnim zakonodavstvom, uz uvažavanje temeljnih prava i ljudskih sloboda, 3. Ovaj dokument neće preporučivati akcije koje nisu u skladu s ustavnim i ljudskim pravima, 4. Akcije moraju biti učinkovite, srazmjerne i opravdane, 5. U slučaju nezakonitog terorističkog korištenja interneta, teba poduzeti neposrednu i srazmjernu akciju da se prekine protuzakonito stanje (situacija), 6. Ukoliko situacija nije protuzakonita, ali se može smatrati štetnom, organizacije (ovlaštena tijela i ISPs-ovi) će najprije nastojati situaciju razriješiti među sobom što je brže moguće, u okviru pravnih obveza i kompetencija, 7. Čak i kad nisu pravno odgovorne za terorističke sadržaje na svojim stranicama, oni će i dalje djelovati u skladu s ovim dokumentom i pomoći, 8. Internet korisnici bi trebali imati način (sredstva) za izbjegavanje podvrgavanju terorističkoj upotrebi interneta (user-friendly mehanizmi bi trebali postojati za to), 9. Budući javno-privatni dijalog i suradnja, utemeljeni na međusobnom povjerenju i razumijevanju, su potrebni kako bi osigurali kontinuitet i buduća poboljšanja kod nastojanja smanjenja upotrebe interneta u terorističke svrhe i konstantnom razvoju interneta.

trebao biti jasan i objašnjen korisnicima, nevladinim organizacijama, ovlaštenim tijelima i internet kompanijama, kako bi njihov posao bio učinkovitiji. Zemlje članice bi trebale imati jasne procedure kako bi se suprotstavile upotrebi interneta u terorističke svrhe. 2. Države bi trebale preuzeti aktivnu ulogu kod smanjenja korištenja interneta u terorističke svrhe. Politike često nisu sveobuhvatne, jasno definirane ili objašnjene. Vlade bi trebale težiti međunarodnoj suradnji i stimuliranju suradnje s internet kompanijama i nevladinim organizacijama.[55] 3.Sve internet kompanije ne navode jasno u svojim uvjetima korištenja da neće tolerirati upotrebu interneta u terorističke svrhe na svojim platformama, te kako oni definiraju terorizam. Neke internet kompanije eksplicitno i s primjerima navode što je to upotreba interneta u terorističke svrhe. 4. Upotreba interneta u terorističke svrhe nije široko poznata ili shvaćena. Javnost uopće, osobito ranjive grupe kao djeca, tinejdžeri i mladi te krugovi kojima su oni okruženi su u velikoj mjeri nesvjesni da su bili meta terorista i njihovih grupa za podsticanje i novačenje. Profesionalci kao što su oni iz „prvog reda" (stručnjaci koji rade s ranjivim skupinama) trebaju znati što napraviti u ovakvim situacijama. Najbolja praksa je podizanje svijesti kroz strategije kibernetičke sigurnosti, edukaciju i programe informiranja koji postoje u brojnim zemljama EU članica. Neke od njih sadržavaju dio koji govori o upotrebi interneta u terorističke svrhe. Važno je upoznati korisnike interneta, a osobito ranjive skupine, kako prepoznati znakove *online* radikalizacije.

5. Internet korisnici trenutno nemaju dovoljno lak način izvješćivanja o terorističkoj upotrebi društvenih medija. Najbolja praksa je što neke mrežne stranice na svojim platformama nude jednostavne i korisnicima prijateljske sustave označavanja, gdje imaju odvojene, specifične kategorije za označavanje upotrebe njihovih usluga od strane terorista. Dok sadržajni portali (kao društvene mreže, video ili portali fotografija) mogu ponuditi mogućnosti označavanja, drugim platformama (mrežne stranice-domaćini) često nedostaje takav mehanizam uz pomoć kojeg bi krajnji korisnici mogli izvijestiti internet kompaniju o korištenju interneta u terorističke svrhe.[56] 6. Internet

[55] Ovaj segment mnoge vlade uključuju kao sastavni dio svojih sigurnosnih strategija i vanjske politike. Vlade moraju biti sigurne da ovlaštena tijela imaju dovoljno kapaciteta kako bi se učinkovito suprotstavili upotrebi interneta u terorističke svrhe.

[56] Štoviše, ne postoji jedan međunarodni, razumljiv (user-friendly) mehanizam za izvješćivanje raspoloživ svim internet korisnicima. Najbolja praksa je da izvještajni mehanizmi bazirani na preglednicima mogu biti razvijeni tako da omoguće krajnjim korisnicima izvješćivanje o

kompanije imaju potencijalne slučajeve korištenja interneta u terorističke svrhe koje im je dojavljeno, ali njima često nedostaje specijalističkih znanja o terorizmu da bi odredili je li takav sadržaj nelegalan. Određivanje je li nešto nelegalno primarno je zadaća policije odnosno tijela zaduženih za provedbu zakona. Najbolja je praksa da pojedine vlade održavaju (zadužuju) jednu ili više organizacija za upućivanje (davanje obavijesti) kojima internet kompanije, nevladine udruge i krajnji korisnici mogu dojaviti potencijalne slučajeve terorističkih aktivnosti na Internetu.[57] 7. Kad su internet kompanije izvještene o mogućim slučajevima korištenja interneta u terorističke svrhe, procedure kojima se nadalje rukuje ovakvim izvješćima često nisu djelotvorne i dovoljne. Najbolja praksa je da pojedine internet kompanije imaju svoje djelotvorne obavijesti i procedure za provođenje akcije te su neke ugovorile korištenje standarda za obavijesti i poduzimanje odgovarajućih akcija. U nekim članicama EU-a odgovorna tijela postavljaju standarde naloga za skidanje neprimjerenih sadržaja. Neprikladni i nezakoniti sadržaji trebaju biti uklonjeni što je brže moguće. 8. Vlade, internet kompanije, odgovorna tijela i nevladine organizacije često ne znaju koga kontaktirati kada dođu do saznanja o korištenju interneta u terorističke svrhe. Najbolja praksa je da neke vlade, ovlaštena tijela, internet kompanije i nevladine organizacije imaju točke za dojavu o korištenju interneta u terorističke svrhe. 9. Kad ovlaštena tijela sumnjaju na ilegalnu upotrebu interneta u terorističke svrhe i kontaktiraju internet kompanije da pomognu u istragama trećih strana, suradnja među dvjema stranama često nije djelotvorna i učinkovita. Najbolja praksa je da neke internet kompanije i ovlaštena tijela imaju postignut dogovor o tome kako surađivati učinkovito, djelotvorno i pravno u istragama o mogućoj ilegalnoj terorističkoj aktivnosti na internetu.[58] 10. Većina internet kompanija se mora baviti s nekoliko

korištenju interneta u terorističke svrhe, na način da nadležnoj internet kompaniji automatski bude odaslan signal o tome, što bi im onda omogućilo da o tome izvijeste svoje klijente, koji bi onda mogli poduzeti odgovarajuće korake.

[57] Dobro organizirane organizacije za upućivanje (javni sektor) i dežurni telefoni-hotlines (privatni sektor) imaju odgovarajući tim iza sebe s potrebnim kompetencijama i vještinama, koji će pomoći internet kompanijama da pravilno postupe s prijavama o korištenju interneta u terorističke svrhe. Organizacije za upućivanje trebaju biti oglašavane i promovirane.

[58] Treba imati na umu kakav je pravni status zahtjeva za suradnjom: obavezan - utemeljen na zakonu ili dragovoljan - prema slobodnoj odluci internet kompanije kojoj je zahtjev upućen.

slučajeva terorizma na svojim platformama. Kad je nelegalni sadržaj uklonjen, teroristi često pokušavaju i uspijevaju postaviti isti sadržaj u okviru usluga druge internet kompanije. Najbolja praksa je da neke internet kompanije razmjenjuju informacije o vrstama zlouporaba svoje mreže s drugim kompanijama, koristeći pouzdane posredničke partnerske organizacije. Ovakva praksa privatnog sektora bi mogla biti proširena i uključivati ilegalnu upotrebu interneta u terorističke svrhe. 11. Različite vrste dragovoljnih kontroliranih usluga od strane krajnjih korisnika postoji za identifikaciju, prijavu pristupa ili blokiranje neželjenog ili nezakonitog sadržaja. Ovakve usluge rijetko uključuju korištenje interneta u terorističke svrhe. Najbolja praksa je roditeljska i druga dragovoljna usluga kontrole krajnjeg korisnika koja učinkovito prepoznaje korištenje interneta u terorističke svrhe. Generalno, opcije blokiranja i filtriranja smatraju se kao loša praksa, osobito ako se provode na državnoj razini. Filtriranje i kontroliranje pristupa na privatnim mrežama ne može u cijelosti zaustaviti ilegalnu upotrebu mreže. 12. Razumijevanje o tome što je upotreba interneta u terorističke svrhe je rezultat rada mnogih individualnih javnih i privatnih organizacija koje proučavaju upotrebu interneta od strane terorista i razmjenjuju svoje ekspertize. Kod upotrebe interneta u terorističke svrhe nema jednog koordinirajućeg i autoritativnog tijela na koje bi se sve zainteresirane organizacije trebale upućivati. Najbolja praksa je akademska mreža (na subnacionalnoj, nacionalnoj i/ili međunarodnoj razini) koja je respektabilna za sve zainteresirane strane i koja treba proširiti postojeće znanje o korištenju interneta u terorističke svrhe, te kako takvo korištenje najefikasnije ograničiti.

Kako je ovaj projekt nastao iz javno-privatnog dijaloga, bilo koja buduća primjena može biti samo na dragovoljnoj osnovi i u skladu s postojećim pravnim propisima i regulama.

The Radicalisation Awareness Network (RAN)[59] je mreža utemeljena u sklopu unutarnjih poslova EU-a (EU Home Affairs office) i pokrenuta u rujnu 2011. s namjerom pružanja pomoći i olakšavanju razmjene informacija između „*first-liners*“ – osoba koje su izravno angažirane s rizičnim pojedincima ili grupama unutar Europske unije (socijalni radnici, učitelji, policija, akademici i nevladine udruge). RAN je prvenstveno fokusiran na internet.

[59] URL: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/index_en.htm), učitano 20. lipnja 2014.

The European Network of Experts on Radicalisation (ENER)[60] je organizacija pokrenuta od strane EU-a kojom je uspostavljena mreža organizacija i eksperata o pitanjima radikalizacije. Mreža predstavlja nastojanje Komisije da produbi razumijevanje radikalizacije preko publikacija, seminara i radionica.

Glavni dio proturadikalizacijskog angažmana odvija se na lokalnoj razini. EU nudi okvir za koordinaciju nacionalnih politika i omogućavanje razmjene informacija o najboljim praksama.

U odnosu na konkretne primjere iz prakse u okviru zemalja članica Europske unije, navodimo primjer uhićenja u Nizozemskoj, gdje je tamošnja policija 2012. godine uhitila osumnjičenika koji je pretraživao internet s ciljem pronalaska priručnika koji opisuju način izrade eksploziva. Drugi je primjer iz 2012. godine kad je u Italiji uhićena jedna osoba koja je konvertirala na islam, a koji je aktivno bio uključen u internetsko širenje terorističke propagande i dokumenata o obuci i rukovanju oružjem i eksplozivima.[61] Suprotstavljanje terorističkim aktivnostima u svakom smislu je od velike važnosti za svaku državu, društvo, integraciju.

Sjedinjene Američke Države imaju istih problema s korištenjem interneta u terorističke svrhe jednako kao i Europska unija.

Jedan od najtežih izazova za SAD je suprotstavljanje upotrebi interneta od strane terorista za širenje njihove propagande i ideološke agende. Taj problem je dio mnogo šireg "rata ideja" protiv ekstremističkog islamskog pokreta.

U svojoj Nacionalnoj strategiji za borbu protiv terorizma ističe se kako će SAD zajedno sa međunarodnom zajednicom voditi rat ideja, kako bi svima postalo jasno da su svi akti terorizma nelegitimni i kako bi se osiguralo okruženje da ideologije koje promoviraju terorizam neće pronaći plodno tlo nigdje. Kao strateški pravac djelovanja SAD-a u protuterorizmu, navedeno je kako je dobar napad najbolja obrana.[62]

Prema izjavama bivšeg američkog ministra obrane Donalda H. Rumsfelda, „Amerika gubi 'rat ideja', više mora

[60] URL: http://www.changeinstitute.co.uk/index.php?option=com_content&task=view&id=83, učitano 20. lipnja 2014.

[61] Europol Trend Report 2013. str. 17-19. URL: https://www.europol.europa.eu/content/te-sat-2013-eu-terrorism-situation-and-trend-report, učitano 21. studenog 2014.

[62] *National Strategy for Combating Terrorism (February 2003.). str.24. URL:* http://georgewbush-whitehouse.archives.gov/), učitano 4. travnja 2015.

biti napravljeno kako bi se reducirao mamac ekstremističke ideologije".[63]

Američki *State Department* održava mrežne stranice na više jezika (uključujući arapski, perzijski i francuski) posvećenih suzbijanju lažnih priča koje se pojavljuju u ekstremističkim izvorima. Nažalost, Amerikancima ostaje puno posla kako bi ovakvi primjeri postali pravilo, a ne iznimka. Američka nacija na rat ideja mora gledati s jednakom važnošću kakvu imaju vojni i policijski aspekti rata protiv terorizma. U tu svrhu SAD treba usredotočiti više resursa na dva područja: suprotstavljanje operativnim učinkovitostima povezanima s terorističkim korištenjem interneta, te podrivanju terorističkog utjecaja kojeg ostvaruju putem interneta.[64]

ICSR izvješće[65] opisuje tri tipa negativnih mjera koje vlade i tijela kaznenog progona mogu primijeniti kako bi se suprotstavili terorističkoj upotrebi Interneta:

1. Filtriranje (ograničeni ulaz korisnika i kontrola razmjene informacija).
2. Skrivanje (manipuliranje rezultatima pretraživača tako da je neželjene sadržaje puno teže pronaći).

U širem političkom smislu, upotrebi interneta od strane ekstremista i terorista moguće se suprotstaviti upotrebom tri široka pristupa:

1. Tvrdom strategijom nulte tolerancije.
2. Mekšom strategijom koja ohrabruje internetske krajnje korisnike na izravni izazov ekstremističkih priča (*narrative*).
3. Izvješćivanjem o uvredljivim ili nelegalnim materijalima te obavještajno vođenom strategijom nadzora koja vodi otkrivanju, istragama, ometanjima i uhićenjima.

Mnoge su zemlje prihvatile mješoviti pristup, koristeći kombinaciju svih triju metoda, u ovisnosti o prirodi sadržaja,

---

[63] Rumsfeld, *CBS News Report*, 27.03.2006. URL: http://www.cbsnews.com/news/rumsfeld-us-losing-war-of-ideas/. Učitano 11. srpnja 2014.

[64] Irving Lachow i Courtney Richardson. *Terrorist Use of the Internet - The Real Story*, *2007.* URL: http://www.au.af.mil/au/awc/awcgate/jfq/terr_internet_2q07.pdf. str. 100. Učitano 2. srpnja 2015.

[65] The International Centre for the Study of Radicalisation and Political Violence - ICSR report. *Countering Online Radicalisation*, A policy report published by the International Centre for the Study of Radicalisation and Political Violence, 2009. str. 22. URL: https://cst.org.uk/docs/countering_online_radicalisation1.pdf, učitano 15. travnja 2015.

identitetu njihovih kreatora ili domaćina, te alatima koji su im na raspolaganju.

Postoje također i upozorenja o prevelikoj upotrebi negativnih mjera (alata). Štoviše, zaključuje se da bi sustavna, velika primjena negativnih mjera, bila nepraktična, pa čak i kontraproduktivna, te da će generirati značajnu (prije svega političku) cijenu, dok će istovremeno malo doprinositi borbi protiv nasilnog ekstremizma.[66]

Nadalje, postoje i etičke dileme o tome kako balansirati potrebu za interveniranjem s potrebom zaštite civilnih prava i temeljnih ljudskih sloboda. Konačno, postoje teškoće kod prosudbe koju treba donijeti o tome gdje se nalaze povrede i onda shodno tome gdje intervenirati.

Kao jedan od konkretnih primjera interveniranja u terorističke i ekstremističke sadržaje na internetu navodimo primjer Ujedinjenog Kraljevstva.

Vlada Ujedinjenog Kraljevstva je u prvi plan borbe protiv terorizma postavila upotrebu interneta u terorističke svrhe. Od srpnja 2006., kada je britanska Vlada javno obznanila svoju Strategiju za suprotstavljanje međunarodnom terorizmu,[67] internet je prepoznat kao područje „gdje se mnoge vrste radikalnih stavova snažno promoviraju". U ožujku 2009. Vlada je publicirala revidiranu verziju CONTEST-a[68] koja je postavila više sofisticirani pristup *online* protuterorizmu. Ovaj je dokument ustvrdio da „Internet predstavlja značajne izazove za CONTEST u cjelini".[69] Novi je pristup stavio prioritet na rad s tvrtkama za filtriranje, ometanje upotrebe interneta za razmjenjivanje poruka između terorista i pojačanu upotrebu interneta za promoviranje alternativnih pogleda radikaliziranim porukama, kojima se može drugačije pristupiti. U 2. Poglavlju Odjeljku 9 ove Strategije pod naslovom Internet i prevencija se navodi da je suzbijanje uporabe interneta od strane terorista stoga ključni dio strategija progona i sprječavanja.[70]

[66] Isto. Str. 15.

[67] *Countering International Terrorism: The United Kingdom's Strategy, July* 2006 (CONTEST, 2006). URL:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/272320/6888.pdf, učitano 14. svibnja 2015.

[68] *Pursue Prevent Protect Prepare, The United Kingdom's Strategy for Countering International Terrorism, March 2009.* URL:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228644/7547.pdf

[69] Isto. Str. 15.

[70] Isto. Str. 94.

Godine 2010. u Ujedinjenom Kraljevstvu je formirana protuteroristička jedinica za upućivanje,[71] uspostavljena u svrhu izvješćivanja o sadržajima koji su ekstremistički ili su ilegalni, omogućavajući građanima korištenje jednostavnog sučelja. CTIR uklanja ili modificira nezakonite sadržaje na internetu, vrši identifikaciju pojedinaca odgovornih za postavljanje ovakvih sadržaja na internet, te podržava policijsku protuterorističku mrežu u istraživanju i procesuiranju *online* terorističkih ili radikalizacijskih aktivnosti. Proaktivno skenira mrežu u potrazi za sadržajima koji promoviraju ili veličaju terorizam. Članak 58. Govori o prikupljanju ili snimanju podataka koje će vjerojatno biti korisno za počinjenje ili pripremu terorističkog čina, ili posjedovanje podataka dokumenata ili zapisa (fotografskih ili elektronskih) koji sadrže tu vrstu informacija.

Nakon što stručnjaci utvrde da određena internet stranica krši zakone Ujedinjenog Kraljevstva, CTIRU uz pomoć internetskih mrežnih poslužitelja (ISPs) nastoji ukloniti takvu stranicu s interneta. CTIRU razvija i koristi nove tehnologije kako bi obradili zanimljive internetske sadržaje i kako bi povećali učinkovitost policijskih odgovora na nezakonite sadržaje. Od veljače 2010. do rujna 2012. bilo je oko 3,100 prijava (upućivanja) prema CTIRU, što je rezultiralo sa 410 uklanjanja nezakonitih sadržaja (13.2 %). Od srpnja 2012. do rujna 2012. bilo je 341 prijava. Najvećim su se dijelom odnosile na Facebook, Twitter i Blogger i/ili Blogspot. Prijave su rezultirale sa 105 uklanjanja s Interneta u istom razdoblju (31%).[72]

Jedan od najvažnijih područja u smislu odgovora na terorističku upotrebu interneta je protunaracija (protupriča) - razvoj i širenje protunaracije *online*. Očituje se u tri moguće forme:

1. Poruke odabrane za protunaraciju su različite od terorističke ideologije.
2. Poruke za protunaraciju koje teže ismijavanju, redikulizaciji ili potkopavanju kredibiliteta terorista.
3. Poruke protunaracije koje promoviraju pozitivne alternative.

[71] The UK Counter-Terrorism Internet Referral Unit.

[72] Charlie Edwards i Luke Gribb. Pathways to Violent Extremism in the Digital Era., The RUSI Journal Publication, 30.10.2013. str. 46. URL: http://dx.doi.org/10.1080/03071847.2013.847714 učitano 24. travnja 2015.

Ovo je potencijalno jedno od najučinkovitijih područja za borbu protiv korištenja Interneta od strane terorista, ali nedvojbeno i najteže za vlade.[73]

Dva su pristupa za *online* kritiziranje terorista:

1. Prvi se odnosi na kritiziranje njihove ideologije, nudeći alternativne interpretacije ključnih tekstova i govora te ukazivanju o tome kako su metode i značenja koje su prihvatili nekonszistentna njihovim osobnim vjerovanjima. Bivši ekstremisti mogu biti osobito snažni prenositelji ove vrste poruka.
2. Drugi tip protunaracije je pokušaj potkopavanja džihada, ali ne u smislu kredibiliteta i autentičnosti njihove ideologije i motivacije, nego u smislu njihove učinkovitosti.

Kod kritiziranja se može koristiti i više osobni pristup, nastojeći potkopati njihov „džihadistički *cool*" brand, ismijavajući ih kao grupe ili pojedince, te se koristiti humorom kako bi ih dehumanizirali.

Nadalje, postoji interes za uspostavom datoteka žrtava terorizma, koje bi mogle komentirati i analizirati aktualne terorističke trendove, jer su žrtve jedan od najsnažnijih i najvažnijih prijenosnika poruka, a čiji su glasovi konzistentno tihi i ignorirani. Inače, žrtve imaju jaku, uvjerljivu i neodoljivu priču koja svjedoči o uzaludnosti terorizma.

Jedno od područja sa znatnim potencijalom za budući razvoj protuterorizma odnosi se na promociju pozitivnih i vjerodostojnih alternativa kroz upotrebu *online* društvenih medija kombiniranih s *offline* kampanjama i drugim tehnikama organiziranim od strane šire društvene zajednice. Ovim bi se inicijativama kreirala ne samo zajednica interesa, nego pokret za promjene koji bi po svojoj prirodi trebao ići organski, odozdo prema gore, kako bi bio vjerodostojan i shvaćen ozbiljno. Izazovi za realizaciju ovog pristupa u praksi su znatni.

Idealni prenositelj poruka protunaracije, na više načina, je dio same publike.

Brojne su sugestije oko potencijalnih projekata i aktivnosti u odnosu na protunaraciju:

1. Pojačana vladina podrška oko prevođenja i distribucije poruka od strane bivših radikala, pokajnika.
2. Optimizacija internetskih pretraživača kako bi na vrh rezultata pretraživanja postavili protunaraciju.

[73] Vlade će se, naime, susretati s potencijalnim nedosljednostima u onome što govore i rade u zemlji i svom pristupu u vanjskoj politici, što bi moglo biti iskorišteno protiv njih od strane ekstremista kao odgovor na protunaraciju vlade.

3. „*One-stop-shop*“ ili skladište za protunaraciju, izgradnja knjižnice tekstova i drugih materijala koji opovrgavaju ekstremističke poglede, promoviraju alternative, uključujući prezentacije izjava žrtava i izlaganje lažnih iskaza.
4. Upotreba okruženja igara i virtualnih svjetova.
5. Izgradnja kapaciteta s pojedincima iz zajednice, civilnog sektora i grupa, kroz tehničku potporu, obuku i umrežavanje.
6. Razvoj baze podataka žrtava terorizma (kako je opisano ranije).
7. Angažman iskusnih pojedinaca za protuargumentaciju na oba dva foruma: specijalističkim džihadističkim forumima, ali i sve više na puno otvorenijim forumima kao što su to Facebook i YouTube.

Pobrojane aktivnosti i mjere koje za cilj imaju suzbijanje korištenja interneta u terorističke svrhe dosad su polučile određene rezultate. Da je tomu tako govori podatak da se na crnoj listi terorista ISIL-a, osim brojnih vođa zapadnog svijeta, karikaturista i novinara, nedavno našao i suosnivač Twittera Jack Dorsey. Smrću se, međutim, ne prijeti samo njemu, nego i svim ostalim zaposlenicima te američke tvrtke, a sve zbog blokiranja korisničkih računa terorista koji su društvene mreže koristili kao idealne platforme za lansiranje džihadističke propagande. „Vaš virtualni rat prema nama izazvat će pravi, krvavi rat prema vama“, stoji u jednoj od poruka upućenih Dorseyu, a koju su gomile pristaša ISIL-a prosljeđivale diljem svijeta. Crna poruka, koju je krasila karakteristična crna zastava ISIL-a, obznanjena je na Pastebinu, popularnoj stranici baziranoj u Poljskoj, na kojoj programeri ostavljaju određene kodove. Blokiranje korisničkih računa nije se nikako svidjelo džihadistima te su poručili ne samo Dorseyu, nego i ostalim djelatnicima i osnivačima društvenih mreža, kako će se „uvijek vraćati“.

Teroristička propaganda diljem svijeta nikad nije bila jača. S druge strane, raste broj uhićenja osoba zaduženih za regrutiranje mladih pristaša u redove „Islamske države“, a naročito poslije napada na francuski satirički tjednik Charlie Hebdo. U ISIL-u su čak obilato koristili Svjetsko nogometno prvenstvo u Brazilu. Tom su prigodom ukrali popularne „*hashtagove*“, odnosno ključne riječi, svojevrsne „egide *tweetova“*, pod kojima su odašiljali pozive na sveti rat i pridruživanje njihovim redovima.

Broj mrežnih stranica povezanih s terorizmom raste velikom brzinom iz godine u godinu. Ilustracije radi, dajemo

prikaz rasta broja ovih stranica u jedanaestogodišnjem razdoblju.

Tablica 6: USPOREDNI PRIKAZ BROJA MREŽNIH STRANICA POVEZANIH S TERORIZMOM PO GODINAMA

Godina	*1998.*	*2003.*	*2009.*
Broj mrežnih stranica povezanih s terorizmom	*12*	*2630*	*6940*

Izvor: The Internet as a Terrorist Tool For Recruitment&Radicalization of Youth. Homeland Security Institute, 2009.

Društvene mreže postale su idealnim alatima za radikalizaciju mladosti, a sve su glasniji pozivi na njihovo potpuno gašenje, sve u nadi kako bi se obuzdala virtualna indoktrinacija, ali i namicanje značajnih financijskih sredstava. Twitter je krenuo u obračun s ISIL-ovcima, a prijetnje koje je odmah nakon toga primio pokazale su da je na dobrom putu.[74]

Neosporna je činjenica kako su pripadnici terorističkih skupina uglavnom osobe mlađe dobi, što znači da je njihova radikalizacija započela u dobi dok su bili tinejdžeri ili čak djeca. Upravo zbog toga posebnu pozornost želimo posvetiti načinima na koje terorističke organizacije u današnjem informacijskom dobu dolaze do svojih mladih pristaša te kako ih novače.

Mrežne stranice sponzorirane od strane Hamasa, al-Fateh (Osvajač - „The Conqueror“) ažurira se svakog tjedna i dizajnirana je za djecu te prikazuje crtane filmove i dječje priče.[75] Likovi iz crtanih filmova prenose poruke nasilja, promoviraju mržnju prema Izraelu, hvale džihad i mučeništvo.

Neke organizacije emitiraju video igre namijenjene djeci i adolescentima. Hezbollah je razvio seriju igara nazvanih Specijalne snage i Specijalne snage 2 koje stimuliraju vojne misije protiv izraelskih vojnika. Igra Specijalne snage 2 je dostupna na arapskom, farsi i engleskom jeziku. Postoji još jedna *online* igra koja se zove Noć Bushovog uhićenja, koja

[74] Vlado Ozretić. Slobodna Dalmacija, 4.3.2015.,

[75] Gabriel Weimann. *Terror on the Internet: The New Arena, The New Challenges*, Washington, DC: United States Institute of Peace Press, 2006.

za cilj pred igrače postavlja uhićenje i ubijanje bivšeg američkog predsjednika George-a W. Bush-a.

Mrežni forumi i pričaonice su formirani kako bi privukli starije tinejdžere. Na ovim forumima mladi komuniciraju s vršnjacima i prelaze iz pasivne faze prikupljanja radikalnih informacija u aktivno sudjelovanje u raspravama o radikalnim temama.

Posebna pozornost je usmjerena prema mladim ženama. Muslimanke se susreću s tradicionalnim ograničenjima i upravo ih ovim putem mogu prevladati. Mogu anonimno komunicirati s drugim muslimankama i čak muškarcima, na način koji u njihovoj kulturi ne bi bio prihvaćen, u osobnom kontaktu.

Irfan Raja je 19 godišnji britanski učenik čija se cijela radikalizacija odvijala *online*. Provodio je na internetu sate skidajući ekstremistička videa, poruke i razgovarajući s drugim radikalima. Godine 2007. stupio je u *online* kontakt s ekstremističkim unovačiteljem i zajedno s još četiri Britanca, koje nikad nije osobno susreo, se pripremio za put u obučni kamp u inozemstvu.[76]

Aabid Husein Khan, 22 godišnji britanski musliman, koji je još s dvojicom utemeljio terorističku ćeliju u Ujedinjenom Kraljevstvu, je u dobi od 12 godina postao strastveni obožavatelj svega do čega je mogao doći na internetu, a odnosilo se na džihad i mudžahedine. Počevši oko 1997., Khanova razina *online* aktivnosti povećala se i on je počeo koristiti *newsgrupe* i forume za razgovor kako bi se pridružio ljudima u raspravama o tim pitanjima - džihad i suvremena pitanja koja su zaokupljala muslimane u raznim zemljama. Interes mu je bio vezan za skupine koje su tamo štitile muslimane i sprečavali štete od ljudi koji su se borili protiv njih.

Prema izjavama Khana koje je dao kroz postupak svjedočenja,[77] na interaktivnim *newsgrupama* i forumima, Khan je otkrio obilje informacija o "vojnim pitanjima ... taktikama skupina, kako su otišli u obranu različitih područja, koje su strategije koristili, koje su oružje koristili, tko je sve bio uključen, profili tih ljudi i slične stvari. Koristeći znanje

[76] The Internet as a Terrorist Tool For Recruitment&Radicalization of Youth.Homeland Security Institute, 2009., URL: http://www.homelandsecurity.org/docs/reports/Internet_Radicalization.pdf

[77] Evan F. Kohlmann. Anatomy of a Modern Homegrown Terror Cell: Aabid Khan et al. (Operation Praline). Testimony of Aabid Hussain Khan. Blackfriars Crown Court; London, U.K. July 16, 2008. URL: http://acsa2000.net/TW/samples/Kohlman.pdf, učitano 5. lipnja 2014.

dobiveno putem interneta, Khan je odlučio nastaviti svoju takozvanu "e-ratnu strategiju".[78]

Upotreba interneta od strane mladih osoba dramatično je narasla u posljednjoj dekadi. Naime, u posljednjih desetak godina upotreba interneta je evoluirala od pasivne, individualno usmjerene na proces traženja (nazvane „Web 1“), do aktivne, društveno povezane u okruženju gdje mladi komuniciraju, diskutiraju, kreiraju i prosljeđuju sadržaje (nazvane „Web 2.0“). Mrežne stranice kao YouTube i Facebook bilježe ogromni porast korisnika, tako da je 2008. godine dosegla brojku od 108.3 milijuna korisnika. Među mladima u dobi od 14 do 24 godine njih 70% redovno koristi društvene mreže. Vrijeme provedeno na društvenoj mreži i mrežnim stranicama za *bloganje* raste trostuko više od ukupnog rasta Interneta.[79] Oko 80% mladih diljem svijeta posjećuje stranice kao što je YouTube. U skladu s rezultatima jedne kanadske studije, mladi smatraju da se mreže na koje se spaja veliki broj njihovih vršnjaka imaju smatrati izvorima vjerodostojnih informacija. Tipični korisnik interneta u Kanadi ostavlja neku vrstu osobnih podataka desecima različitih web stranica. Ako računate kolačiće i IP adrese kao osobne podatke, onda su internet korisnici iza sebe ostavili osobne informacije svugdje gdje su bili. Ostavili su "digitalne mrvice kruha" po cijelom *cyber* području - i oni imaju malo pojma o tome kako se ti podaci mogu koristiti i koliko su dobro zaštićeni.[80]

Napori na suprotstavljanju radikalizaciji mladih daleko zaostaje za sposobnostima terorista i promoviranju njihovih ideja. Čini se kako Al Qa'ida_bolje prenosi svoje poruke preko interneta, nego Amerika, Europska unija te brojne druge integracije i države svoje poruke.

Kod suprotstavljanja radikalizacijskim porukama upućenih mladima, mnoge vlade su potražile pomoć umjerenih i utjecajnih muslimanskih religijskih dužnosnika da utvrde vodeće zablude i izobličenja islamskog učenja kojeg terorističke grupe često propagiraju. Konkretno, Singapur se za postizanje velikih rezultata na ovom području udružio s umjerenim imamima. Singapurska vlada je osnovala Religijsku rehabilitacijsku grupu koja producira mrežne stranice koje sadrže odgovore na krive interpretacije Islama, članke o radikalizmu i umjerenom Islamu te multimedijski odjeljak.[81]

[78] Isto. Str. 2.
[79] The Nielsen Company, 2009., str. 3
[80] Ann Cavoukian. Privacy by design, 2009. Str.254.
[81] Homeland Security Institute, 2009. The Internet as a Terrorist Tool For Recruitment&Radicalization of Youth. Str. 7. URL:

Za uspješnu protuterorističku borbu na internetu je potrebno razumjeti alate, tehnike i poruke koje teroristi koriste. Potrebno je pojačati razumijevanje alata, tehnika i poruka na koje mladi odgovaraju i utvrditi osnovne potrebe koje mlade osobe čine podložnima terorističkim obraćanjima.

Ovdje je potrebno posegnuti za lekcijama naučenim od privatnog sektora.

Postoje privatni entiteti koji su posvetili značajne resurse kako bi razumjeli mlade, njihove promjenjive interese, ponašanja, preferencije i potrebe. Nužno je povećati razumijevanje o tome kako su oni prišli tržištu mladih, koje su metode upotrijebili kako bi razvili odnos s mladim ljudima i njihovim promjenjivim potrebama i preferencijama, koje poruke su im bile posebno zvučne i prihvatljive i imaju li preporuke kako testirati efekte odaslanih poruka.

Predstavnici Instituta domovinske sigurnosti (*Homeland Security Institute* - HSI) su 2009. u Los Angelesu održali okrugli stol s predstavnicima strateških komunikacijskih tvrtki (Outside Eyes Inc.) te rukovodstvom i marketingom jedne tinejdžerske glazbene grupe koja je postigla multimilijunsku dolarsku popularnost, gotovo isključivo preko interneta.[82]

Raspravljeni su sljedeći pristupi i utvrđeno je sljedeće:

1. Doprijeti do mladih gdje su *online*. Istaknuto je kako, da bi se doprlo do mladih, treba iskoristiti iste platforme koje su popularne među mladim ljudima (interaktivne video stranice za spajanje s drugima i međusobnu razmjenu informacija-video uradaka, fotografija i sl.). Direktnim angažiranjem mladih na ovim platformama, rukovodstvo benda je došlo u priliku iskoristiti stotine tisuća prethodno uspostavljenih socijalnih mreža, koji tada postaju kanali za prenošenje njihovih poruka.
2. Iskoristiti virusnu prirodu *online* sadržaja. Grupa je koristila interaktvine stranice kao što su Facebook, MySpace i YouTube kako bi postavili materijale (video, foto, glazbeni klipovi) koji se mogu pokupiti i dalje širiti njihovim slušateljstvom (publikom), koji sada služe kao prijenosnici, šireći materijale unutar njihove vlastite mreže.

---

http://www.homelandsecurity.org/docs/reports/Internet_Radicalization.pdf

[82] Isto. Str. 8.

3. Autentičnost je presudna. Grupa je ustvrdila kako je važno ne podcijeniti sposobnost mladih ljudi da odrede autentičnost poruka i njihovih prijenosnika. Poruke i njihovi glasnici moraju biti autentični i uvjerljivi kako bi imali odjeka kod mlade publike.
4. Razviti i upotrijebiti mehanizme povratne veze. Bend je iskoristio neposrednost interneta pregledavajući i odgovarajući na reakcije publike kroz njihove poruke i postove. Neposrednost ovakve povratne veze omogućavao je bendu da slijedi efekte svojih poruka skoro u realnom vremenu. Bend je kontinuirano skenirao odgovore na svoje postove mjereći kako pozitivno ili negativno su njihove poruke primljene, te kako su često njihovi postovi pregledavani.
5. Odgovoriti pozitivno i fluidno. Bend je razmatrao kako su njihove *online* poruke primljene i koje poruke motiviraju obožavatelje da čine, kako bi sljedeći odgovor što bolje oblikovali.[83]

Terorističke grupe su prepoznale gore opisanu dinamiku i započele su s prodorom prema mladima koristeći iste platforme i načine s ciljem indoktrinacije mladih s radikalnim porukama.

Privatni sektor predstavlja niz najboljih praksi za učinkovito dolaženje do mladih *online*, od kojih je pet ovdje prikazano. Upotrebom istih lekcija koje su upotrijebili marketinški i stručnjaci za zabavu privatnog sektora kako bi uspješno razumjeli, došli do njih i utjecali na milijune mladih ljudi *online*, proturadikalizacijski napori na internetu mogu biti značajno poboljšani.

Zaključak

Ovim smo radom potvrdili tezu da se internet koristi kao glavni izvor informacija za teroriste i ekstremiste, te da predstavlja medij za komunikaciju i propagandu ekstremističkih pogleda. Također, da je važan alat za teroriste i ekstremiste, jer je uključen u radikalizacijski proces, može doprinijeti novačenju i od velike je koristi u njihovom operativnom radu u vidu komunikacije i suradnje. Internet kao *online* medij pruža puno veće mogućnosti nego *offline* svijet za potvrdu ekstremističkih vjerovanja. Potvrdili smo tezu da internet predstavlja „eho komoru“ za ekstremističke i terorističke poglede, dok tezu pojedinih

[83] The Internet as a Terrorist Tool For Recruitment&Radicalization of Youth. Homeland Security Institute, 2009., Str. 8-10. URL: http://www.homelandsecurity.org/docs/reports/Internet_Radicalization.pdf

znanstvenika da on omogućava radikalizaciju bez fizičkih kontakata nismo potvrdili, jer je u svim analiziranim slučajevima (15) tzv. *offline* svijet igrao važnu ulogu u radikalizacijskom procesu. Internet stoga ne zamjenjuje potrebu pojedinaca da se osobno sastaju tijekom procesa radikalizacije. U odnosu na samoradikalizaciju putem interneta, ustvrdili smo da su analizirani pojedinačni slučajevi pokazali da su pojedinci komunicirali s vanjskim svijetom te da nisu do kraja ostali izolirani. Ustvrdili smo da je vrlo važan međusobni utjecaj između *online* i *offline* svijeta, zbog čega uloga interneta u radikalizacijskom procesu mora biti sagledavana u širem kontekstu osobne povijesti svakog pojedinca i njegovih društvenih odnosa. Internet treba sagledavati kao način, a ne kao jedinstvenu metodu radikalizacije. On omogućava radikalizaciju i može, ali je ne mora ubrzati.

Protuteroristički napori i politike usmjereni na reduciranje korištenja interneta za terorističke svrhe opisani su u ovom radu i ustvrdili smo da su polučili određene rezultate. Pokrenute su brojne inicijative i projekti za smanjenje dostupnosti nezakonitih materijala koji promiču radikalizaciju terorista na internetu. Također, pronađeni su načini otkrivanja sadržaja koji promiču radikalizaciju i novačenje terorista te se provode i postupci uklanjanja ovakvih sadržaja s interneta. Svako nacionalno iskustvo je oblikovano političkim, kulturnim i pravnim elementima svojstvenim toj zemlji, pa ne možemo govoriti o jedinstvenom protuterorističkom odgovoru u ovom području.

Uz sve pobrojane i druge brojne protuterorističke aktivnosti, teroristi i dalje vrlo efikasno koriste internet za svoje radikalizacijske, operativne i druge potrebe.

S ciljem iznalaženja još efikasnijih odgovora protuterorističkih politika na ovaj problem, od velikog je značaja da vlade razmjenjuju informacije o projektima, aktivnostima i „naučenim lekcijama“, kako bi izbjegli moguće greške kod suprotstavljanja ovom fenomenu te povećali učinkovitost provođenih mjera.

Također je važno za vlade da nastave voditi računa o etičkim dilemama kao i onima praktičnima – kada intervenirati, kako balansirati sigurnosne i imperative civilnih sloboda.

Kako bi se iznašla odgovarajuća sveobuhvatna rješenja i povećala otpornost društva na problem radikalizacije, u rješavanje ovog problema potrebno je povezati sve segmente društva. Tu mislimo na specifična znanja akademskih stručnjaka, stručnjaka iz prakse, tvoraca politika, uz povezivanje javnog i privatnog sektora te

poticanje međunarodne suradnje i razmjene najboljih praksi, tako da odgovor cijelog društva bude samo jedan i sveobuhvatno uspješan.

Literatura

Al-Lami, Mina. *Studies of Radicalisation: State of the Field Report*. Politics and International Relations Working Paper Series, No. 11, London: University of London, 2009.

Awan, Akil N. *Virtual Jihadist Media: Function, Legitimacy and Radicalizing Efficacy*. European Journal of Cultural Studies, 10(3), 2007.

Bjelopera, Jerome P. *American Jihadist Terrorism: Combating a Complex Threat*. Congressional Research Service Report for Congress: Washington, DC, Congress Research Service, 2011.

Bjelopera, Jerome P. *American Jihadist Terrorism: Combating a Complex Threat*. Congressional Research Service Report for Congress: Washington, DC, Congress Research Service, January 23, 2013.

Briggs, Rachel and Strugnell, Alex. *Radicalisation: The Role of the Internet*. Policy Planners, Network Working Paper: London, Institute for Strategic Dialogue, 2011.

Cavoukian Ann. *Privacy by design*, Information and Privacy Commissioner of Ontario, Canada, 2009.

Edwards, Charlie i Gribb, Luke*. Pathways to Violent Extremism in the Digital Era*., The RUSI Journal Publication, 30.10.2013.

Klausen, Jytte. *Al Qaeda-Affiliated and 'Homegrown' Jihadism in the UK: 1999-2010*. Institute for Strategic Dialogue, 2010.

Kohlmann Evan F. *Anatomy of a Modern Homegrown Terror Cell: Aabid Khan et al. (Operation Praline). Testimony of Aabid Hussain Khan*. Blackfriars Crown Court: London, U.K. July 16, 2008.

Lachow, Irving i Richardson, Courtney. *Terrorist Use of the Internet - The Real Story*, 2007.

Vinay Lal. *Virtual Terrorism: How Modern Terrorist Use the Internet,* URL: http://www.arifyildirim.com/ilt510/vinay.lal.pdf, učitano 1.svibnja 2015.

O'Rourke, Simon. *Virtual Radicalisation: Challenges for Police*. Edith Cowan University Research Online, 2007. URL:http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1041&context=isw, učitano 12. travnja 2015.

Pantucci, Raffaello. *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists*. Developments in Radicalisation and Political Violence, International Centre for the Study of Radicalisation and Political Violence, 2011.

Precht, Tomas. *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, December 2007.

Sageman, Marc. *Leaderless Jihad: Terrorist networks in the twenty-first century*. University of Pennsylvania Press, 2008.

Singer Peter W. *The New Children of Terror. The Making of a Terrorist: Recruitment, Training and Root Causes*, vol. 1. James J.F. Frost (ed.) Praeger, November 2005.

Tomić, Zoran; Musa, Ilija i Primorac, Marijan. *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.

Von Behr, Ines; Anaïs Reding; Charlie Edwards, Luke Gribbon*. Radicalisation in the digital era - The use of the internet in 15 cases of terrorism and extremism*. Rand Corporation, 2013.

Weimann, Gabriel. *Terror on the Internet: The New Arena, The New Challenges.* Washington, DC: United States Institute of Peace Press, 2006.

Zirojević Fatić, Mina. *Zloupotreba interneta u terorističke svrhe,* MP 3, 2011. URL: *http://www.doiserbia.nb.rs/img/doi/0025-8555/2011/0025-85551103417Z.pdf, učitano 12*. lipnja 2014.

Dokumenti

Audiovisual Media Services (AMS) Directive. 2010/13/EU, 2010.

Clean IT project (URL:http://www.cleanitproject.eu/, učitano 12. rujna 2014.)

Countering International Terrorism: The United Kingdom's Strategy, CONTEST, 2006.

Radicalisation Awareness Network (RAN) URL: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/index_en.htm, učitano 15. lipnja 2014.

The European Network of Experts on Radicalisation (ENER) URL: http://www.changeinstitute.co.uk/index.php?option=com_content&task=view&id=83, učitano 12. srpnja 2014.

Convention on the Prevention of Terrorism, CETS No 196, 2005.

Convention on Cybercrime, CETS No 185, 2001.

Countering International Terrorism:The United Kingdom's Strategy, July 2006 (CONTEST, 2006). URL:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/272320/6888.pdf, učitano 14. svibnja 2015.

Countering Online Radicalisation, A policy report published by the International Centre for the Study of Radicalisation and Political Violence (ICSR), 2009. URL: https://cst.org.uk/docs/countering_online_radicalisation1.pdf, učitano 11. lipnja 2015.

Direktiva 2010/13/EU, Europskog parlamenta i Vijeća o koordinaciji određenih odredaba utvrđenih zakonima i drugim propisima u državama članicama o pružanju audiovizualnih medijskih usluga (Direktiva o audiovizualnim medijskim uslugama), 10. ožujka 2010.

Doc. 10633/06 CONCL 2 Brussels, European Council 15/16 June 2006 Presidency Conclusions, Brussels, 16. June 2006.

Europol Trend Report 2013. URL: https://www.europol.europa.eu/content/te-sat-2013-eu-terrorism-situation-and-trend-report, učitano 21. studenog 2014.

National Strategy for Combating Terrorism, February 2003. URL: http://georgewbush-whitehouse.archives.gov/), učitano 4. travnja 2015.

Pathways to Violent Extremism in the Digital Era, URL:http://www.tandfonline.com/loi/rusi20#.VXPcmlL4YgA, učitano 10. ožujka 2014.

Pursue Prevent Protect Prepare: The United Kingdom's Strategy for Countering International Terrorism,UK Home Office, Cm 7547, March 2009.

Radicalisation: The role of the Internet. A working paper of the PPN. Institute for Strategic Dialogue URL: http://www.strategicdialogue.org/allnewmats/idandsc2011/StockholmPPN2011_BackgroundPaper_FINAL.pdf, učitano 15. svibnja 2015.

Recruitment and Radicalization of School Aged Youth by International Terrorist Groups, Final Report, April 23, 2009. USA Department of Education. HSI. URL:http://www.cleanitproject.eu/wp-content/uploads/2012/07/2009-recruitment-and-radicalization.pdf, učitano 15. svibnja 2014.

Rezolucija Vijeća sigurnosti 1963, S/RES/1963, 2010.

Terrorism Act, 2000, URL: http://www.legislation.gov.uk/ukpga/2000/11/pdfs/ukpga_20000011_en.pdf, učitano 22. travnja 2014.

Terrorism Act, 2006 URL: http://www.legislation.gov.uk/ukpga/2006/11/pdfs/ukpga_20060011_en.pdf, učitano 22. travnja 2014.

The Internet as a Terrorist Tool For Recruitment & Radicalization of Youth. Homeland Security Institute, 2009. URL: http://www.homelandsecurity.org/docs/reports/Internet_Radicalization.pdf, učitano 15. svibnja 2014.

The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism. 14781/1/05, Brussels, Council of the European Union, European Commission, 2005.

Tiskani i elektronski mediji

Slobodna Dalmacija
Global News
CBS News