UNIVERZITET U BEOGRADU
FAKULTET POLITIČKIH NAUKA

Ivana Luknar

BORBA PROTIV KIBERTERORIZMA U STRATEŠKIM DOKUMENTIMA REPUBLIKE SRBIJE

doktorska disertacija

Beograd, 2019. godine

UNIVERSITY OF BELGRADE
FACULTY OF POLITICAL SCIENCES

Ivana Luknar

FIGHT AGAINST CYBERTERRORISM IN THE STRATEGIC DOCUMENTS OF THE REPUBLIC OF SERBIA

Doctoral Dissertation

Belgrade, 2019

Mentor:

vanredni prof. dr Ivana Damnjanović, Univerzitet u Beogradu – Fakultet političkih nauka

Članovi komisije:

1. prof. dr Dragan Simeunović**,** Univerzitet u Beogradu – Fakultet političkih nauka
2. pukovnik docent dr Dejan Vuletić, Institut za strategijska istraživanja

Datum odbrane: _____

Izjava zahvalnosti

Mudra izreka glasi: „*Nauka traži žrtve. Prisustvo obavezno!*“ Jer, rad na pripremi doktorske disertacije podrazumeva: mnogo odricanja, neprospavanih noći, propuštenih trenutaka sa prijateljima i porodicom, dosta slomljenih snova, nekada i slomljenog srca mog i nečijeg tuđeg, ne odgledanih filmova, pozorišnih predstava, koncerata,... Puno je tu suza bilo, padova i ponovnih ustajanja, mnogo preispitivanja, ali kada se sve zbroji entuzijazam i interesovanje za bavljenje temom je prevagnulo. Načinjen je i taj korak, privedena je disertacija kraju. Ali, ponovo sam na samom početku. Bavljenje temom je podstaklo mnoga nova interesovanja i otvorena pitanja koja strpljivo čekaju pravi trenutak za odgovor.

Hvala veliko na podršci i savetima profesoru dr Draganu Simeunoviću, kao i mojoj mentorki profesorki dr Ivani Damnjanović što su imali strpljena i razumevanja za sva moja naučna lutanja i nedoumice. Hvala mojim roditeljima i sestrama bez čije podrške ne bih mogla da istrajem. Rad posvećujem svom sinu Luki koji je uprkos malom broju godina umeo da razume, da „hvatanje u koštac“ sa naukom nije šala i da iziskuje ozbiljan rad i strpljenje. Bez Lukine podrške ovaj rad ne bi imao smisla. Luka od srca hvala do neba i nazad.

Autor

BORBA PROTIV KIBERTERORIZMA
U STRATEŠKIM DOKUMENTIMA REPUBLIKE SRBIJE

Rezime

Savremeni tehnološki razvoj nameće pitanje: da li države aktuelnim antiterorističkim zakonodavstvom i merama bezbednosti koje primenjuju garantuju sigurnost od kiberterorizma? Iako u svetu postoji velika spremnost među državama za saradnjom po pitanju suočavanja sa aktuelnim problemom kiberterorizma, intenzivan trend razvoja informaciono-komunikacionih tehnologija zahteva konstantni napor za praćenje razvoja savremenih tehnologija i rizika koji iz tog razvoja proizilaze. Tehnološke inovacije su zaista pružile brojne mogućnosti, ali i nove potencijalne pretnje i zloupotrebe. U radu su prikazane mere borbe protiv kiberterorizma koje se primenjuju u strateškim dokumentima Republike Srbije. Savremeno društvo očigledno počiva na tehnološkim postavkama, zato blag zakonski pristup problemu kiberterorizam može da predstavlja velik rizik ne samo za jednu državu, nego i globalno društvo uopšte. Pitanje kiberterorizma je kompleksno pitanje koje se ne postavlja samo pred određenu nacionalnu državu, njeno krivično zakonodavstvo i bezbednosne mere, nego je pitanje koje je otvoreno za celu međunarodnu zajednicu.

Ključne reči: kiberterorizam, kiber bezbednost, kiber kriminal, internet
Naučna oblast: Političke nauke
Uža naučna oblast: Politička teorija, politička istorija i metodologija političkih nauka
UDK broj: 323.28:004:343.346.8(497.11)

FIGHT AGAINST CYBERTERRORISM
IN THE STRATEGIC DOCUMENTS OF THE REPUBLIC OF SERBIA

Abstract

Contemporary technological development imposes question: Do current states anti-terrorism legislation and security measures guarantee cyber-terrorism defence? Despite great willingness among world countries to cooperate on behalf of actuel problem of cyberterrorism, intensive trend of information and communication development requires constant effort for monitoring this technology growth and its risks. Indeed, technological innovations create new opportunities, but they also provide a new potential threats and abuses. This paper presents fight measures against cyberterrorism in the strategic documents of the Republic of Serbia. Obviosly modern society is based on technological settings so soft legal approach to the cyberterrorism can be huge risk not only to one country, but also to global society in general. Cyberterrorism is complex issue that not concern one specific national state, its criminal legislation and security measures, but that is serious issue which concern whole international community.

Key words: cyberterrorism, cybersecurity, cybercriminal, internet

Scientific field: Political science

Scientific subfields: Political theory, political history, methodology of political science

UDS number: 323.28:004:343.346.8(497.11)

SADRŽAJ

Prilozi

Prilog 1 – Izjava o autorstvu

Prilog 2 – Izjava o istovetnosti štampane i elektronske verzije doktorskog rada

Prilog 3 – Izjava o korišćenju

Tabele

Slike

Internet je od „informacione auto-strade“ postao krvotok savremenog društva.

Ivana Damnjanović (5.avgust 2018)

1. UVOD

1.1.Predmet i cilj istraživanja

1.1.1. Problem istraživanja

Terorizam predstavlja jedan od najznačajnijih bezbednosnih izazova savremenih država i aktuelan predmet debate među mnogim autorima. Efikasno suzbijanje terorizma pretpostavlja njegovo poznavanje i razumevanje, kao i razumevanje faktora koji u znatnoj meri utiču na njegovo nastajanje i dalji razvoj. Imajući u vidu da je savremeni terorizam multikauzalne i multimanifestne prirode, potrebno je uzeti u obzir mnoštvo njegovih pojavnih oblika. Uzevši u obzir činjenicu da proces globalizacije oblikuje svakodnevnicu i da njen intenzitet razvoja potpomaže brzi razvoj tehnologija, može se reći da je kiberterorizam naročito aktuelan oblik terorizma za razmatranje, ali i pretnja savremenoj društvenoj bezbednosti.

Savremenim autorima proces globalizacije nije stran, štaviše u akademskim krugovima globalizacija je prepoznata kao fenomen koji se ne dešava negde "*vani*" i nekome drugom, nego se odvija upravo "*ovde*" i snažno utiče i zahvata skoro sve aspekte savremenog života. Zato je bilo kakvo sagledavanje kiberterorizma bez uzimanja u obzir *globalno sistemske teorije* gotovo nezamislivo i neozbiljno. Za sagledavanje sadašnje društveno-političko-ekonomske, pa i kulturne situacije Lesli Skler (Sklair, 2001) se naročito zalaže za primenu ove teorije ukazujući na neosporan značaj koji danas imaju tehnološke, ekonomske, političke i kulturno-ideološke inovacije u drugoj polovini XX veka. Uzimanje u obzir Sklerove teorije omogućava širi prikaz istraživanog pojma, jer globalno sistemska teorija može da objasni ne samo uzroke nastanka i razvoja kiberterorizma, nego i ponire dublje, jer objašnjava razlike među zemljama koje su pod pretnjom različitog intenziteta od kiberterorizma. Skler govori o globalnom društvu, ali navodi razlike između zemalja centra i periferije. Neosporno je da su, u savremenom svetu upotreba i značaj informacionih tehnologija sve intenzivniji i pokrivaju gotovo sve aspekte savremenog života. Takođe, države se sve više oslanjaju na informaciono-komunikacionu tehnologiju u svom radu, otuda online bezbednost sve više dobija na značaju.

Razvoj informatičkih tehnologija, prevashodno interneta „*povezuje udaljena mesta na takav način da lokalna zbivanja uobličavaju događaji koji su se odigrali hiljadama kilometara daleko i vice versa*" (Gidens, 1998, 69). Na taj način terorističke pretnje i napadi u kiber prostoru dovode u pitanje bezbednost ne samo pojedinih država, nego predstavljaju pretnju i za globalnu bezbednost uopšte.

Jer, iako nisu svi svetski regioni podjednako uključeni u proces globalizacije ona direktno ili posredno utiče na sve njih. Otuda jedna od hipoteza ovog rada glasi: *Posledice savremenog procesa globalizacije stvaraju pogodno tle za razvoj posebnog oblika terorizma - kiberterorizam*. Međutim, kao što primećuju Nagar i drugi autori (Nagar et all, 2002, 257–285) proces globalizacije karakterišu protivurečnost, dinamičnost i višestrukost. Globalizacija ima dvostruki efekat. S jedne strane imamo, "*globalno izjednačavanje očekivanja, koje je nastalo kao rezultat unapređenja u obrazovanju, globalnoj komunikaciji i transportu, koji su vodili širenju i sve većem prihvatanju normi i vrednosti kao što su pravičnost, jednakost i ljudska prava – građanska i politička, kao i ekonomska i socijalna*" (Kaul, 1994, 2). Dok je, sa druge strane potvrđeno u praksi da princip jednakosti razjedinjuje ljude i onemogućava bilo kakav harmonični prirodni poredak, te time postojano produbljuje jaz između razvijenog i nerazvijenog dela sveta, bogatih i siromašnih. Otuda kako Frances (Frances, 2004) navodi siromašne prožima hronična ekonomska ranjivost i nesigurnost, koja ih ograničava na usvajanje kratkoročnih strategija preživljavanja. Na taj način oni ostaju u začaranom krugu siromaštva, sa gotovo nikakvom perspektivom i mogućnostima da ostvare svoje potencijale i razvoj u bilo kom smislu. Otuda Jejts (Yeates, 2001) primećuje da autori dijametralno različito gledaju na globalizaciju, otuda je jedni vide kao rešenje brojnih socijalnih problema, a drugi je smatraju osnovnim uzrokom brojnih socijalnih problema.

Brz razvoj tehnologija, sve jeftiniji internet i njegova sve veća pristupačnost omogućavaju gotovo svakome da postane učesnik u svetskim događanjima i da prati dešavanja na svetskoj sceni. Takođe, razvoj savremene tehnologije menja formu društveno-političkog aktivizma te on porpima online odrednicu. Gore navedeni uslovi pogoduju širenju terorističkih aspiracija putem interneta, dok online komunikacija omogućava posebnu vrstu terorizma, kiberterorizam. Razni autori: Vajman (Weimann, 2006), Bobit (Bobbitt, 2008, 55-57) i Ger (Geer, 2006) navode da se terorističke grupe služe savremenim informacionim tehnologijama za komunikaciju i organizovanje napada zbog raznih pogodnosti koje internet pruža, uglavnom zbog mogućnosti anonimne komunikacije i niskih troškova. Da nove informacione tehnologije značajno olakšavaju međunarodni terorizam takođe ukazuje i praktičan primer Islamske države, koja se služila društvenim mrežama za propagiranje i ostvarivanje svojih ideja.

Ukoliko posmatramo mikro nivo (pojedinca u savremenom društvu) otuđenje (alijenacija) je sve prisutnija kao posledica umrežavanja sveta u jednu celinu zahvaljujući informacionim tehnologijama i drugim savremenim oblicima komunikacija. To znači da su „*kontakti licem u lice*“ sve ređi. Poznanstva postaju virtuelna i nastaje novi vid društvenih zajednica i kiberkulture. Značajnu ulogu u formiranju identiteta igraju društvene mreže i online sadržaji. Porodica kao jedna od osnovnih društvenih formi, takođe se suočava sa novim izazovima uzrokovanih savremenom tehnološkom revolucijom, koja dovodi u pitanje negdašnje društvene uloge i identitete koji se sada multipliciraju uz stvaranje novih online identiteta, koji mogu da izazovu krizu i rascep identiteta.

S obzirom na činjenicu da se razne terorističke organizacije služe pogodnostima kiberprostora za plasiranje informacija u medijima, organizovanje napada i regrutovanje novih članova, borba protiv kiberterorizma sve više dobija na značaju. Ali, kako bismo se adekvatno suočili sa određenim problemom nužno je da ga prethodno precizno definišemo. Međutim, na samom početku nameće se pitanje: Koje su to aktivnosti na internetu koje možemo da smatramo terorističkim u pravom smislu te reči? Razni autori su pokušali da ponude odgovor i pomenute aktivnosti klasifikuju.

Vajman je predložio da „*sve aktivnosti terorista na internetu možemo da klasifikujemo u osam različitih grupa: 1) psihološki rat; 2) publicitet i propaganda; 3) traženje informacija; 4) prikupljanje fondova; 5) regrutovanje i mobilizacija; 6) umrežavanje; 7) deljenje informacija; 8) planiranje i koordinacija*“ (Weimann, 2004, 5-10). Mojra Konvej predlaže skalu koja aktivnosti terorista na internetu karakteriše kao upotrebu, zloupotrebu, ofanzivnu upotrebu i sajberterorizam (Konvej u: Damnjanović, 2009, 238).

Petrović akt kiberterorizma pragmatično definiše kao „*korišćenje informacionih resursa u vidu pretnje ili ucene da bi se ostvario određeni teroristički cilj*“ (Petrović, 2000, 649). Kiber napadi ne samo da nanose značajne materijalne štete finansijskim institucijama, nego „*mogu takođe ciljano da ugrožavaju rad nacionalnih odbrambenih sistema*“ (O’Harrow, 2005, 10). Upravo zbog brojnih štetnih posledica koje ovi napadi mogu da uzrokuju nužno je preduzeti adekvatne mere za sprečavanje kiberterorizma.

Različite države se na razne načine suprostavljaju ovoj vrsti terorizma. U radu nastojimo da odgovorimo na pitanje: Koje su to adekvatne mere i metode koje države mogu da usvoje da bi se zaštitile od kiberterorizma? Prostor Zapadnog Balkana koji čine: Hrvatska, Albanija, Bosna i Hercegovina, Makedonija, Srbija, Kosovo, Crna Gora (Europarl, 2017) je bezbednosno nestabilan region pod konstantnom pretnjom i pritiscima od terorizma, gde je procenat muslimanskog stanovništva visok. Iako se smatra da Srbija trenutno nije aktuelna meta napada međunarodnih terorista, nužno je uzeti u obzir bezbednosnu situaciju na Kosovu koja je duži vremenski period izvor nestabilnosti na prostoru Republike Srbije. Inače, Kosovo je oduvek bilo zbog brojnih razloga pogodno tle za dejstvo i širenje terorističkih aktivnosti. OVK se nakon formiranja 1993. godine zbog potreba za naoružanjem i opremanjem povezala sa Albancima koji su bili na privremenom radu u mnogim zemljama: Nemačkoj, Švedskoj, Belgiji, Švajcarskoj i drugim, te je na taj način kao što navodi Simeunović: „*postignuta čvrsta veza Albanaca sa Kosova i Metohije i Albanaca iz Albanije od kojih su dobili veliku pomoć tokom građanskih sukoba na Kosovu i Metohiji, kao i NATO agresije na SRJ*“(Simeunović, 2016, 172). „*Dolaskom međunarodnih snaga na Kosovo i Metohiju izvršena je dezintegracija i formalna demilitarizacija OVK, a ova skupina ni do danas nije prekinula svoje delovanje. Deo sastava preusmeren je sa aktivnostima na političkom planu kroz stranke Demokratska partija Kosova (DPK), dok je 10.000 pripadnika obuhvaćeno transformacijom OVK u Kosovski zaštitni korpus (KZK) i Kosovsku policijsku službu (KPS)*“ (Simeunović, 2016, 173) Potom je usledilo formiranje ANA terorističke organizacije i samoproglašenje nezavisnosti Kosova, što nakon 2008.godine ostavlja brojna problematična pitanja nerazrešena. Masovne migracije izbeglica sa prostora Iraka, Sirije i Avganistana tokom 2015. godine su ove već postojeće pretnje dodatno ojačale. Kroz istoriju je potvrđeno da terorizam predstavlja političko nasilje i pretnju koja nikada ne jenjava. „*Da bi se razumela potencijalna opasnost od kiberterorizma, moraju se uzeti u obir dva faktora: prvo, da li postoje ciljevi koji su ranjivi na napade koji mogu dovesti do nasilja ili ozbiljne štete; i drugo, da li postoje akteri koji poseduju sposobnost i motivaciju da ih sprovedu*“ (Denning, 2000, 7). Stoga, imajući u vidu ove činjenice, razmatranje terorizma, odnosno kiberterorizma kao jednog njegovog pojavnog oblika u Srbiji je više nego aktuelno.

U savremenoj društveno-političkoj javnosti, fenomen kiberterorizma prepoznat je kao jedna od najaktuelnijih opasnosti po očuvanje međunarodnog mira i bezbednosti. Karakteristike kiberterorizma, kao što su: teška uhvatljivost počinioca i štetne posledice sa dalekosežnim efektom ne umanjuju potrebu za njegovim istraživanjem, nego ukazuju na poteškoće bavljenja ovim problemom i potrebu da mu se ozbiljno pristupi. Stepen značaja ovako prepoznatog problema je prvorazredan i obuhvata: ovladavanje savremenim pojmom kiberterorizma, saznanje o tome kako on funkcioniše u savremenim društveno-istorijskim uslovima, faktore koji ga oblikuju, kao i metode borbe u strateškim dokumentima Republike Srbije. Ovo istraživanje posebno doprinosi proširenju znanja o kiberterorizmu u oblastima teorije politike, studija bezbednosti ili spoljne politike, kao i sagledavanje istraživanog problema kroz proces političkog odlučivanja i delovanja na primeru Srbije.

Namera autora je da upotrebom metode analize sadržaja definiše kiberterorizam, prikaže da su mere borbe protiv kiberterorizma u strateškim dokumentima Srbije neadekvatne i ponudi predloge za njihovo unapređenje. Ovim istraživanjem ćemo pokušati da predvidimo put kojim će se razvijati dalje kiberterorizam, radi postizanja opšteg cilja rada: suzbijanje kiberterorizma i iznalaženje najboljeg rešenja i mera za njegovo onemogućavanje na prostoru Srbije.

Dakle, u radu ćemo prikazati:

1. osnovne karakteristike kiberterorizma;
2. ključne faktore koji ga oblikuju;
3. naučna shvatanja kiberterorizma;
4. dosadašnje metode sučeljavanja sa ovom vrstom terorizma u svetu s posebnim osvrtom na strateška dokumenta Srbije;
5. mogućnost primene dosadašnjih metoda borbe protiv kiberterorizma u svetu na području Srbije.

Problem identifikacije i upoznavanje sa organizacijom i načinima funkcionisanja i sprovođenja kiberterorističkih aktivnosti, kao i suprostavljanje njima od strane određenih državnih organa i međunarodnih organizacija u cilju otkrivanja i sprečavanja kiberterorizma u postojećim uslovima na prostorima, a naročito na prostoru Republike Srbije je značajno pitanje, kako u sferi nauke, tako i u postojećoj praksi.

1.1.2.Predmet istraživanja

1.1.2.1.Teorijsko određenje predmeta istraživanja

a) Postojeća saznanja o predmetu istraživanja

Predmet ovog istraživanja je kiberterorizam i analiza kiberterorizma u strateškim dokumentima Republike Srbije. Postojeće naučno saznanje na temu kiberterorizma: istraživanja, naučni radovi, studije i procene nesumnjivo predstavljaju povoljnu osnovu za istraživanje ove teme. Takođe, tumačenju ovog fenomena je doprineo značajan fond nenaučne građe: informacije štampanih i elektronskih medija, iskustvena znanja i rezultati sa raznih skupova i konferencija, izveštaji i dokumenta pojedinih institucija koje su bile pod različitim pretnjama ili napadima od strane kiberterorista itd. Imajući u vidu da štampani i elektronski mediji neretko izveštavaju neobjektivno i u službi politike, prilikom ovog istraživanja poštovaće se standardi naučne konkretizacije i naučne usmerenosti na sadržaj predmeta istraživanja. Vrednost istraživanja je u tome što nastoji da ponudi mnogo više od novootvorenih pitanja, da ukaže na veliki broj nerešenih problema, kao i da ponudi konkretna rešenja, odgovore i predloge na tekuće i otvorene probleme u borbi protiv kiberterorizma, naročito u Srbiji.

Literatura obiluje opštim razmatranjima o terorizmu. Međutim o kiberterorizmu, naročito o njegovom sagledavanju u specifičnim nacionalim okvirima kroz strategije borbe protiv kiberterorizma gotovo da nema literature. Ovo je ozbiljan nedostatak, obzirom na aktuelnu pretnju u savremenom svetu od kiberterorizma. Istaknuti domaći autori koji se bave opšte temom terorizma su: Simeunović (Simeunović 1989; 1991; 2009), Talijan (Talijan, 2004), Kovačević (Kovačevć, 1992), Damnjanović (Damnjanović, 2005), Radovanović i Lazarević (Radovanović & Lazarević, 2015) i drugi. Dok su za temu kiberterorizma u Srbiji zainteresovani Damnjanović (Damnjanović, 2009, 237-253), Petrović (Petrović, 2001, 100-122), Popović (Popović, 2017) i dr. Dela pomenutih autora će biti korišćena u radu kao naučna građa, odnosno polazna osnova za realizaciju ovog istraživanja, koje će biti proširivano. Iako je reč o borbi protiv kiberterorizma u strateškim dokumentima Republike Srbije, u naučni fond polaznih saznanja ovog istraživanja, će takođe u manjoj ili većoj meri biti uključeni strateški dokumenti i rezultati stranih naučnih i stručnih radova.

Uspešno sprečavanje kiberterorizma je jedna od osnovnih funkcija kriminalne politike i podrazumeva organizovani oblik društvene prevencije i kriminalnu profilaksu (niz kriminalnih mera i procedura). Međutim, kiberterorizam nije isto što i kiberkriminal. Razlikuje ih osnovni cilj napada. Kiberterorizam podrazumeva „*politički motivisane hakerske operacije koje imaju za cilj da nanesu ozbiljne štete, kao što su gubitak života ili teška ekonomska šteta*" (Denning, 2001, 241), dok je osnovni motiv kiberkriminalaca ekonomska dobit. Složenost istraživanog fenomena upućuje na potrebu za njegovim preciznim određenjem i neophodnu primenu višedimenzionalnog pristupa tokom analize kiberterorizma.

Države primenjuju različite metode za suprostavljanje kiberterorizmu. Pojedine države imaju specijalne timove (*Computer Emergency Response Teams - CERT*) za hitno reagovanje i borbu sa online pretnjama. Dogrul i dr. (Dogrul, Aslan &Celik, 2011, 35) navode SAD i Veliku Britaniju kao dobar primer bezbednosne politike za suprostavljanje kiberterorizmu i razlikuju dve vrste metoda kiberodbrane: aktivne i pasivne. Šinder (Shinder, 2002, 35- 41, 44) ukazuje da su nesumnjivo mere borbe protiv kiberterorizma značajne, međutim potrebno je njihovo precizno definisanje, kao i adekvatna edukacija onih koji te mere primenjuju i upotreba odgovarajuće tehnologije. U aktivne metode odbrane (*Active Cyber Defense*) ubrajamo direktnu odbranu i prevenciju, odnosno „*aktivnosti koje su usmerene da onemoguće, ublaže ili poništе kiberpretnje*" (Denning, 2014, 3) koje su upućene prema civilima i imovini. Dok pasivne metode odbrane podrazumevaju različite sigurnosne kompjuterske tehnike i mere zaštite (Stallings & Brown, 2015) kao što su: kriptografija (Talbot & Welsh, 2006), upotreba antivirus softvera i *Firewall*-a (Walsh, 1997), različiti sistemi za otkrivanje upada i zaštitu lozinki, ključevi za šifrovanje (*DES, 3DES i RSA*[1]) (Kuljanski, 2010, 65-77) i dr.

[1] Ključevi za šifrovanje su kriptografski algoritmi koji služe za očuvanje bezbednosti podataka. Mogu da budu klasični i moderni. Najpopularniji asimetrični metod za kriptovanje podataka je RSA algoritam, koji je dobio naziv po početnim slovima svojih izumitelja: Rivest, Shamir i Adleman. RSA i 3DES spadaju u moderne vrste ključa za šifrovanje. DES i 3DES spadaju u najpoznatije algoritme simetričnih kriptosistema. Više možete pronaći u: Stalings, Wiliam (2011). *Cryptography and Network Security Principles and Practices*. Prentice Hall. Retrieved July 3, 2017 from: https://wanguolin.github.io/assets/cryptography_and_network_security.pdf

b) Kategorijalno-pojmovni sistem

Mogućnost da se kiberterorizam posmatra i definiše na osnovu različitih kriterijuma usložava i otežava stvaranje jedne opšte prihvaćene definicije.

Damnjanović izdvaja osnovne definicione elemente pojma kiberterorizma:

„1. *upotreba informacionih/kompjuterskih tehnologija kao oružja (a ne samo kao logističke podrške, sredstva komunikacije ili mete);*

2. politička motivacija;

3. orijentacija ka simbolici/spektakularnosti/publicitetu;

4. značajna materijalna šteta i/ili ljudske žrtve, ili pretnja takvim posledicama, što dovodi do

5. širenja straha većih razmera“ (Damnjanović, 2009, 244).

Kiberterorizam je prema Doroti Dening (Dorothy Denning) „*konvergencija između kiberprostora i terorizma. On se odnosi na protivzakonite napade i pretnje napadima protiv kompjutera, mreža i informacija uskladištenih u njima kada su počinjeni da bi se zastrašila ili prinudila vlada ili njen narod u promociji političkih ili društvenih ciljeva. Dalje, da bi se okvalifikovao kao kiberterorizam, napad mora da rezultira nasiljem protiv lica ili imovine, ili u najmanju ruku da nanese dovoljno štete da bi izazvao strah*“ (Dening u: Damnjanović, 2009, 242-243).

Radi postizanja ciljeva kiberteroristi se služe različitim taktikama, kao što su zastrašivanje, mrežni upadi i sabotaže, online terorističke obuke itd. Najčešći motivi kiberterorizma su političke prirode. Neretko se kiberteroristi služe i kiberkriminalom, ali to najčešće ne čine kao primarni cilj, nego samo kao usputno protivzakonito pribavljanje sredstava (finansijskih i drugih) radi ostvarenja ili lakše realizacije svog primarnog cilja. Kiberterorizam predstavlja posebnu vrstu kiberpretrnje i nije isto što i kibekriminal, informacioni rat ili kiberšpijunaža.

1.1.2.2.Operacionalno određenje predmeta istraživanja

a) Činioci sadržaja predmeta istraživanja su:

1.Osnovne karakteristike kiberterorizma;

- Specifičnosti kiberterorizma u odnosu na druge vrste kibernapada (Faktori i njihovo međusobno dejstvo i dinamika, koji umnogome utiču na pojavni oblik kiberterorizma i izdvajaju ga od ostalih vrsta kibernapada);

2. Faktori koji utiču na stvaranje kiberterorizma (U radu ćemo analizirati dva nivoa faktora: makronivo (globalni, regionalni, državni- ekonomska ne/razvijenost, tehnološka ne/razvijenost, geostrateški položaj zemlje), i mikronivo (pojedinačni);

3. Dosadašnje politike i mere koje su primenjivane u borbi sa kiberterorizmom u svetu;

4. Prevencija, predložene politike i mere u borbi sa kiberterorizmom u Srbiji

- Sagledavanje odnosa prema kiberterorizmu kroz strateška dokumenta Srbije:

a) „*Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma*“ (Službeni glasnik RS, broj 3/15);

b) „*Nacionalna strategija za sprečavanje i borbu protiv terorizma za period od 2017-2021. godine*“ (Službeni glasnik RS, broj 94/17);

c) „*Odluka o usvajanju Strategije nacionalne bezbednosti Republike Srbije*“ (Službeni glasnik RS br. 88/09);

d) „*Odluka o usvajanju Strategije odbrane Republike Srbije*“ (Službeni glasnik RS br. 88/09);

e) „*Nacionalna Strategija održivog razvoja*“ (Službeni glasnik RS, br. 57/08)

f) „*eSEE Agenda za razvoj informacionog društva*“ (Službeni glasnik RS, broj 29/09)

g) „*Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine*“ (Službeni glasnik RS, br. 51/10)

h) „*Strategija razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine*“ (Službeni glasnik RS, broj 68/10)

i) „*Strategija razvoja industrije informacionih tehnologija za period od 2017. godine do 2020. godine*“ (Službeni glasnik RS, broj 95/16)

j) „*Strategija razvoja mreža nove generacije do 2023. godine*“ (Službeni glasnik RS, br. 33/18)

k) „*Strategija zaštite podataka o ličnosti*“ (Službeni glasnik RS, br. 58/10).

Kako bismo dobili potpunu sliku o kiberterorizmu u Srbiji, istraživanjem će biti obuhvaćena oba prethodno navedena nivoa: makro i mikro nivo. Što se tiče samog makronivoa, reč je o neodvojivom delu državne i društvene strukture, i njihovom međuodnosu koji je postojan, tako što ova dva nivoa društvene stvarnosti konstantno međusobno deluju, dok su njihovi efekti srednjoročni ili dugoročni. Nećemo zanemariti ni sagledavanje kiberterrozma sa aspekta pojedinačnih (mikroelemenata): otuđenje, kriza identiteta, pripadanje virtuelnim zajednicama i td. U radu ćemo takođe razmatrati metode borbe protiv kiberterorizma u svetu, dok će se mogućnost njihove primene u Srbiji ustanoviti kritičko-uporednom analizom.

b) Vremensko određenje predmeta istraživanja

Određenje vremenskog okvira u kome se pojava kiberterorizam izučava je nezahvalno, imajući u vidu sledeće činjenice:

1. predmet istraživanja je kompleksan društveni fenomen;

2. kiberterorizam predstavlja poseban oblik terorizma;

3. geneza opšteg pojma - terorizam je dugotrajna pojava i bez njenog sagledavanja je teško uočiti nastanak i razvoj kiberterorizma;

4. mogućnost njegove primene je tesno povezana sa IT tehnologijom i njenim razvojem, što varira od zemlje do zemlje;

5. pretnja i posledice od kiberterorizma su međunarodnog karaktera. Međutim, kada sagledavamo borbu protiv kiberterorizma u Strateškim dokumentima Republike Srbije, nužno je uzeti u obzir dokumenta koja su do sada usvojena:

- „*Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma*“ (Službeni glasnik RS, broj 3/15);

- „*Nacionalna strategija za sprečavanje i borbu protiv terorizma za period od 2017-2021. godine*“ (Službeni glasnik RS, broj 94/17);

- „*Odluka o usvajanju Strategije nacionalne bezbednosti Republike Srbije*“ (Službeni glasnik RS br. 88/09);

- „*Odluka o usvajanju Strategije odbrane Republike Srbije*“ (Službeni glasnik RS br. 88/09);

- „*Nacionalna Strategija održivog razvoja*“ (Službeni glasnik RS, br. 57/08)

- „*eSEE Agenda za razvoj informacionog društva*“ (Službeni glasnik RS, broj 29/09)

- „*Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine*“ (Službeni glasnik RS, br. 51/10)

- „*Strategija razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine*“ (Službeni glasnik RS, broj 68/10)

- „*Strategija razvoja industrije informacionih tehnologija za period od 2017. godine do 2020. godine*“ (Službeni glasnik RS, broj 95/16)

- „*Strategija razvoja mreža nove generacije do 2023. godine*“ (Službeni glasnik RS, br. 33/18)

- „*Strategija zaštite podataka o ličnosti*“ (Službeni glasnik RS, br. 58/10)

Imajući u vidu da je „*Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma*“ usvojena 5. januara 2015. godine, dok je „*eSEE Agenda za razvoj informacionog društva*“ usvojena 2002. godine i predstavlja prvi značajniji korak uređenja oblasti informacionih tehnologija. Otuda izučavanje mera borbe protiv kiberterorizma na primeru Srbije u ovom radu obuhvata period od 2002. godine do danas.

c) Prostorno određenje predmeta istraživanja

Tumačenje kiberterorizma nemoguće je bez razumevanja pojma kiberprostor (*cyberspace*), koji nema prostornih granica. Međutim, radi potpunog razumevanja predmeta istraživanja, prilikom tumačenja preduzetih i predloženih mera koje primenjuju zemlje iz okruženja u borbi protiv kiberterorizma, u istraživanju će se razmatrati i prostor susednih država ili oblasti, kao i mere koje su donešene i predložene na međunarodnom nivou.

d) Disciplinarno određenje predmeta istraživanja

Proučavanje kiberterorizma, kao i mere borbe protiv kiberterorizma u strateškim dokumentima Republike Srbije zahteva interdisciplinarni pristup, jer podrazumeva oslanjanje na naučna saznanja iz više naučnih oblasti. Otuda ćemo u radu primenjivati znanja raznih društvenih nauka (pravo, političke nauke, istorija, bezbednost, psihologija, sociologija i kultura) i znanja inženjersko - tehničkih nauka (informatika i računarstvo).

1.1.2.3. Ciljevi istraživanja

Naučni ciljevi ovog rada su naučna deskripcija kiberterorizma i njegovih osnovnih odrednica, naučno objašnjenje faktora koji su ga oblikovali i razumevanje dosadašnjih mera borbe protiv kiberterorizma u svetu i na prostoru Republike Srbije. Iako se smatra da naučna deskripcija (opis istraživane pojave) predstavlja najniži naučni cilj u postupku naučnog saznanja, ona omogućava sistematični prikaz svih relevantnih činjenica i okolnosti vezanih za problem istraživanja.

Ubrzan razvoj tehnologije i njena sve veća primena pored toga što pruža brojne olakšice u svakodnevnom životu, ostavlja prostora i za razne zloupotrebe (kiberkriminal) od strane određenih organizacija ili pojedinaca. Imajući u vidu da je kiberterorizam jedna od aktuelnih pretnji savremenom društvu potrebno je da šira društvena javnost bude upoznata sa ovim društvenim izazovom.

Društveni ciljevi rada su skretanje pažnje javnosti na pojavu kiberterorizma, kao i predlaganje određenih mera, radi preventivnog delovanja, sprečavanja i suzbijanja kiberterorizma u Republici Srbiji. Zbog moguće opasnosti od zloupotrebe savremene tehnologije i negativnih posledica terorističkih aktivnosti na prostorima Republike Srbije, kao i zemalja u regionu, predlaganje mogućih mera borbe protiv terorizma kod nas, i u svetu može da bude veoma korisno, ne samo iz naučnog, nego i praktičnog ugla.

Dakle, praktični (društveni) cilj istraživanja je skretanje pažnje na posebne forme terorizma, odnosno njegove specifične oblike. Iako su istraživanjem obuhvaćene mere borbe protiv kiberterorizma konkretno na primeru strateških dokumenata Srbije, rad pored toga što nudi bolje razumevanje problema kiberterorizma, može da podstakne nova naučna razmatranja u zemljama regiona, ali i sveta uopšte, što potencijalno doprinosi njegovoj sveobuhvatnijoj prevenciji.

1.2. Osnovne hipoteze istraživanja

Opšta hipoteza

U radu polazimo od generalne hipoteze koja glasi: Strateški dokumenti u Srbiji ne predviđaju adekvatne mere za borbu protiv kiberterorizma.

Posebne hipoteze

Prva posebna hipoteza

Posledice savremenog procesa globalizacije stvaraju na makro i mikro nivou pogodno tle za razvoj posebnog oblika terorizma - kiberterorizam.

Druga posebna hipoteza

Na makronivou posledice savremenog procesa globalizacije koje stvaraju pogodno tle za razvoj kiberterorizma su: umrežavanje, razvoj IT, jaz između bogatih i siromašnih.

Treća posebna hipoteza

Posledice globalizacije koje na mikronivou stvaraju pogodno tle za razvoj kiberterorizma su: otuđenje, kriza identiteta, virtuelne zajednice, nastanak različitih vrsta kiberkulture.

Četvrta posebna hipoteza

Svest o problemu kiberterorizma kako na međunarodnom, tako i na državnom nivou nedovoljno je razvijena.

Peta posebna hipoteza

Dosadašnje savremene aktivne i pasivne metode odbrane od kiberterorizma ne razvijaju se istim intenzitetom, kao i tehnološki razvoj i sve veće umrežavanje društva.

Šesta posebna hipoteza

Razvoj tehnologije omogućava sve sofisticiranije oblike kiberterorizma, pa samim tim i zahteva unapređenje dosadašnjih aktivnih i pasivnih metoda odbrane.

Sedma posebna hipoteza

Opšte mere borbe protiv kiberterorizma ne možemo efikasno da primenimo na specifične pojavne oblike kiberterorističkih akcija.

Osma posebna hipoteza

Društveno-politički milje jedne države, njena tehnička opremljenost i IT znanje (IT stučnjaci) su faktori koji utiču na mere borbe protiv kiberterorizma u toj državi.

1.3. Metodološki okvir istraživanja

Za potrebe istraživanja koristićemo ***osnovne naučne metode istraživanja***:

1. ***Generalizacija*** – Teorijska metoda koja podrazumeva misaono uopštavanje odnosno saznavanje opšteg na osnovu pojedinačnog. Konkretno u radu će biti primenjena generalizacija prilikom teorijskog uopštavanja dosadašnjeg naučnog fonda o istraživanom predmetu;

2. ***Indukcija*** - U radu ćemo se služiti metodom indukcije koja podrazumeva dolazak do naučnog saznanja sintezom i generalizacijom od pojedinačnih elemenata ka opštem. Konkretno na primeru osnovnih elemenata i obeležja kiberterorizma doći ćemo do saznanja o celokupnom društvenom fenomenu - kiberterorizam;

3. ***Dedukcija*** – Za razliku od indukcije, dedukcija podrazumeva naučno saznanje do kojeg se dolazi polazeći od opšteg ka posebnom, pojedinačnom. U radu će ova metoda biti primenjena tako što će se poći od generalnog poimanja pojma kiberterorizma, da bi se potom on raščlanio na njegove sastavne elemente;

U toku naučno-istraživačkog procesa metode indukcije i dedukcije su međusobno povezane i uslovljene, neodvojive. Obzirom da je kiberterorizam složen društveni fenomen, neophodna je primena metoda analize i sinteze. Najvažnije osobenosti kiberterorističkih aktivnosti prikazaćemo deskriptivnom analizom. Dalje, da bi što jednostavnije došli do zaključka o celini, odnosno kiberterorizmu kao aktuelnom društveno-političkom fenomenu i kako bismo uvideli određene pravilnosti, koristićemo se metodom sinteze.

4. ***Analiza*** – Ova metoda istraživanja podrazumeva da se predmet istraživanja rastavi na njegove sastavne delove;

5. ***Sinteza*** – Ova metoda istraživanja podrazumeva dolaženje do saznanja o celini (istraživanom fenomenu) spajanjem i stavljanjem u razne međusobne veze i odnose njegovih pojedinačnih delova;

6. ***Klasifikacija*** – Vrsta metode specijalizacije, podrazumeva dolazak do saznanja posebnog u opštem. U ovom slučaju tako što se opšti pojam kiberterorizam raščlanjava i razvrstava po određenom kriterijumu. Upotreba ove metode omogućava nam da klasifikujemo dosadašnju borbu protiv kiberterorizma zabeleženu u strateškim dokumentima u raznim zemljama širom sveta.

Za potrebe istraživanja pored gore navedenih osnovnih naučnih metoda primenićemo i ***opštenaučne metode istraživanja***. U radu se polazi od hipotetičko-deduktivne metode istraživanja. Komparativna metoda će poslužiti za poređenje sličnosti ili različitosti metoda borbe protiv kiberterorizma u strateškim dokumentima različitih društveno-političkih prostora, odnosno u različitim državama u kojima kiberterorističke organizacije deluju ili su pod potencijalnim rizikom.

Kombinovan i multidisciplinaran metodološki pristup je neophodan, imajući u vidu složenost predmeta istraživanja. Tako ćemo se za potrebe istraživanja služiti znanjem koje nude nauke o politici, sociologija, kulturologija, psihologija i nauke o bezbednosti.

U radu ćemo koristiti ***analizu sadržaja*** dokumenata i ostale građe.

1.4. Naučni i društveni doprinos istraživanja

Činjenica je da je kiberterorizam društveno-politički fenomen koji usled procesa globalizacije i umrežavanja sveta predstavlja sve aktuelniju pretnju u savremenom društvu. Iako su tendencije za sprečavanje i iskorenjivanje kiberterorizma aktuelne u današnje vreme kako na državnom, tako i na međunarodnom nivou, literatura koja se bavi kiberterorizmom i njegovim određenjem sa aspekta strateških dokumenata i drugih mera borbe za njegovo suzbijanje je oskudna.

Aktuelnost ovog društvenog fenomena, kao i međunarodna pretnja uslovili su hiperprodukciju nenaučne građe iz ove oblasti (informisanje od strane štampanih i elektronskih medija itd.). Međutim, jedino se naučnim tumačenjem postavlja stabilna osnova za buduća istraživanja i suočavanja sa ovim međunarodnim problemom. Otuda se naučni doprinos ovog istraživanja ogleda pre svega, u tome što se s jedne strane, uvećava fond kritičkog i analitičkog saznanja, i s druge strane potpomaže iznalaženje najboljih metoda borbe protiv kiberterorizma, kao i predloga za ublažavanje njegovih negativnih posledica.

Dakle, od ovog istraživanja se očekuje da sa naučnog aspekta rasvetli pojam kiberterorizma, njegove korene, motive i interese nastanka, subjekte koji sudeluju u kiberterorističkim akcijama, njihove ciljeve i druge činioce koji na poseban način oblikuju ovu vrstu terorizma, kako bi pružili adekvatna rešenja za problem kiberterorizma i preduzeli korake za poboljšanje bezbednosnog ambijenta.

Društvena opravdanost ovog istraživanja proističe iz njegovih potencijalnih doprinosa, jer rezultati istraživanja treba da posluže kao vredan input prakse i metoda suočavanja sa kiberterorizmom na prostoru Srbije. Imajući u vidu da je istraživanje zasnovano na analizi i predlaganju najbolje prakse koje mogu da posluže u borbi sa kiberterorizmom, vrednost ovog istraživanja proizilazi i iz saznanja do kojih će se doći putem komparacije sa strategijama borbe protiv kiberterorizma i u drugim državama.

2. KIBERTERORIZAM

2.1. Terorizam

Svetska scena se suočava sa novom erom terorizma tzv. „*globalni terorizam*“ (Cronin, 2009, 63), čije su posledice svetskih razmera, a motivacija uglavnom etnonacionalistička i religijska. Pretnje i strahovi od terorizma ne jenjavaju, a naročito dobijaju na značaju nakon terorističkih napada SAD-a od strane Al Kaide 11. septembra 2001. godine. Obzirom da terorizam u savremenom svetu predstavlja značajan izazov po globalnu bezbednost, njegovo razumevanje i definisanje je najvažnija faza suočavanja i borbe sa ovim fenomenom. Dok je utvrđivanje njegovih ključnih karakteristika jedan od osnovnih ciljeva savremenih nauka (društvenih, pravno-političkih, bezbednosnih i dr.).

Iako pojavu terorizma vezujemo za savremeno društvo, terorizam nije pojava savremenog doba. Tokom istorije terorizam je postojao u različitim oblicima. Zato je za njegovo razumevanje veoma važno uzeti u obzir sledeće:

- društveno-istorijske okolnosti u kojima se terorizam javlja
- vrstu i kvalitet društveno-političkih i ekonomskih odnosa u zemlji i okruženju
- aktuelne političke stavove
-„*klimu*“ međunarodne zajednice
- delovanje i ponašanje drugih država
- postojanje / nepostojanje eventualnih podsticaja za mešanje u unutrašnje odnose i vršenje spoljnih pritisaka na pojedine suverene zemlje.

Opšte je poznato da terorizam indirektno utiče na spoljnu politiku, tako što može da ugrožava integritet jedne države, otežava, usporava ili onemogućava njenu integraciju u pojedine međunarodne organizacije ili institucije. Odnosno, bavljenje terorizmom zahteva višeslojnu intervenciju od strane međunarodne zajednice, što može da podstakne dezintegraciju i sprovođenje određenih oblika sankcija. Takođe, terorizam značajno može da utiče i na promociju određene vlade na međunarodnoj sceni i prikaže je kao nesposobnu da se izbori sa terorizmom, čak može da prikaže određenu državu kao podržavaoca terorizama. Dakle, veoma je značajno da naučno razumemo pojavu terorizma zbog njegove mogućnosti da utiče na spoljnopolitički plan, kao i zbog posledica koje može da ima po nacionalnu bezbednost.

Tokom istorije se menjalo značenje reči terorizam. Ovaj izraz se upotrebljavao tokom XIX veka da označi anarhiste, koji su sami sebe tako nazivali. Lehi, borci za oslobođenje Izraela tokom 40-tih godina XX veka sebe su predstavljali kao jevrejsku terorističku grupu. Inače, ovaj termin je proistekao od latinskog izraza „*terror*“, „*terroris*“ koji znači „*užas, veliki strah, vladavina zastrašivanjem, način vladanja ulivanjem straha i nasiljem*“ (Vujaklija, 1975, 947). Dakle, „*teror je pretežno vršenje nasilja u okviru procesa sprovođenja moći sa ciljem održanja na vlasti, odnosno zadržanja ili uvećanja moći vladajućih, dakle nasilja vlasti*“ (Simeunović,1989, 144-145).

Uprkos njegovom dugom trajanju, još uvek nije utvrđena jedna opšte prihvaćena definicija terorizma. Tako je navedeno u francuskom rečniku pojmova da je terorizam „*skup akata nasilja koje neka politička organizacija vrši da bi uticala na stanovništvo i stvorila klimu nesigurnosti*“ (Pauli dr., 1978), dok je u engleskom rečniku terorizam određen kao „*metod vladavine ili suprotstavljanja nekoj vladi koji pokušava da prouzrokuje strah*“ (Flaxner, 1987). Dalje, u italijanskom rečniku definisan je ovaj pojam kao „*sredstvo ekstremnog i ilegalnog nasilja u političkoj borbi*“ (Palazzi,1965).

Teroristi su vremenom menjali i prilagođavali metodologiju svog delovanja aktuelnim istorijskim procesima, otuda je terorizam do danas ostao nerešen problem koji odlikuju složenost i promenljivost kao njegove primarne karakteristike. Kao što primećuje Simeunović, termin terorizam je tokom istorije najpre služio da označi nasilno preuzimanje vlasti od strane revolucionara, da bi „*tokom 19. veka bio vezan za nasilno delovanje anarhističkih i nihilističih organizacija. U dvadesetom veku je dva puta termin terorizam ponovo vezivan za nasilje vlasti, prvo povodom delovanja režima strahovlade kakvi su bili nacistički i staljinistički, a zatim i povodom neslaganja zapadnih velikih sila sa oslobodilačkim projektima kolonijalnih naroda koji su se služili i nasiljem u svojoj borbi za oslobođenje, da bi sedamdesetih godina do danas ponovo bio vezan za nasilje protiv neke i nečije vlasti, mada povremeno i za nasilje nekih država koje su označavane kao sponzori terorizma, osovine zla i sl*.“ (Simeunović, 2009, 19).

Opasnost od terorizma ne jenjava. Brojni autori su pokušali da daju svoj doprinos u istraživanju ovog fenomena. Međutim, „*savremeni terorizam, kao višedimenzionalni politički fenomen, iako prisutan od samog početka klasnog društva u svim društveno-političkim sistemima poprima tako opasne i široke razmere da se danas smatra jednim od najvećih pošasti na planeti*” (Savić, 2006, 211-212).

Brojni autori su pokušali da definišu ovu pojavu sa aspekta raznih naučnih disciplina, što je iznedrilo veliki broj različitih definicija terorizma. Tomaševski to objašnjava time što se pod „*pojmom terorizma obuhvataju različiti akti nasilja i ugrožavanja ljudskih prava i ljudskih života, kao i javnih, odnosno zajedničkih i individualnih dobara. U tom mnoštvu i raznolikosti akata koji se podvode pod pojam terorizma, ostaje deo razloga zbog kojih nije mogla biti utvrđena jedna sveobuhvatna i opšteprihvatljiva definicija terorizma*“ (Tomaševski, 1983, 13). Međutim, iako se definicije terorizma razlikuju, one sadrže u sebi sličnosti, odnosno njegove osnovne karakteristike. Tako se u gotovo svakoj definiciji o terorizmu pominju strah i nasilje. Neki od primera definicija koje smo za ovu priliku izdvojili su:

- „*Pod opštim pojmom terorizam podrazumeva se doktrina, metod i sredstvo izazivanja straha i nesigurnosti kod građana sistematskom upotrebom nasilja radi ostvarivanja određenih, prvenstveno političkih ciljeva*” (Skakavac, 2010, 331).

- Gaćinović kao glavnu karakteristiku terorizma vidi nasilje i njegovu upotrebu i smatra da je to: „*organizovana primena nasilja (ili pretnja nasiljem) od strane politički motivisanih izvršilaca, koji su odlučni da izazivanjem straha, zebnje, defetizma i panike nameću svoju volju organima vlasti i građanima*“ (Gaćinović, 1998, 31). Odnosno vidi ga kao „*produženu ruku politike, koja se vodi drugim (nelegalnim) sredstvima*“ (Gaćinović, 2011, 18) za postizanje svojih ciljeva.

- Kegli (Kegley, 2003, 13) predlaže određenje terorizma na osnovu njegovog opisa. Smatra da je najpre potrebno:

- utvrditi njegove osnovne elemenate

- ponuditi objašnjenje ovog fenomena pomoću uzroka koji motivišu aktere da realizuju svoje ciljeve praktikujući terorističko delovanje

- razmotriti do sada postojeće, predložene i primenjivane mere, kako preventivne, tako i represivne za suzbijanje terorizma na globalnom nivou.

- Šmid i Jongman definišu terorizam pomoću nasilja i u zavisnosti od osnovnog cilja tog nasilja, odnosno željene poruke koju treba poslati medijima. Tako oni pišu: „*Terorizam je strahom inspirisan metod ponavljanja nasilne akcije vršene od strane individua, grupa ili državnih aktera iz kriminalnih ili političkih razloga, pri čemu – za razliku od ubistva–konkretna meta nasilja nije ključna meta. Neposredne ljudske žrtve nasilja generalno su birane iz ciljane populacije nasumično (mete po prilici) ili selektivno (predstavnici ili simbolične mete) i služe*

kao generatori poruka. Baziran na pretnji i nasilju, proces komuniciranja između terorista (organizacije), (ugroženog) žrtve i glavne mete služi da se manipuliše glavnom metom (javnošću-medijima) pretvarajući je u metu putem terora, zahteva ili skretanje pažnje zavisno od toga da li su u prvom planu zastrašivanje, prinuda ili propaganda" (Schmid & Jongman, 2005, 28). Dalje, Lemkin izučava osnovne motive terorizma i navodi da je njegov primarni motiv zastrašivanje ljudi koje se postiže izvođenjem različitih vrsta nasilništva kako bi se stvorila „*danger commun*" (Lemkin, 1933, 900–901), tj. jedna sveopšta opasnost koja predstavlja pretnju kako interesima građana, tako i pojedinim državama.

Bilo koja forma terorizma: manifestna (čiji je cilj da odjekne u medijima i uznemiri što širu javnost) ili latentna forma terorizma (kamuflirana, formalno pravno legalna) podrazumeva „*vid individualnog, nelegitimnog i neinstitucionalnog nasilja*" (Simeunović, 1993, 736) i predstavlja pretnju po neko društvo, državu ili neke njene institucije, te „*nema legitimne osnove u relevantnom pravnom i etičkom kodeksu međunarodne zajednice*" (Simeunović, 1993, 736).

2.2. **Kriterijumi klasifikacije terorizma**

Terorizam se može klasifikovati prema različitim kiterijumima. Međutim, ovaj poduhvat nije nimalo lak, zbog njegove kompleksnosti i postojanja mnoštva pojavnih oblika terorizma u svetu. Otežavajuća okolnost je to što pojedine terorističke organizacije može da odlikuje istovremeno nekoliko različitih zajedničkih karakeristika, a ne jedna karakteristika koja bi svrstala taj određeni vid terorizma u jednu konkretnu kategoriju. Dakle, kompleksnost ovog fenomena znatno usložnjava i otežava njegovu iscrpnu klasifikaciju.

Zbog mnoštva pojavnih oblika, terorizam možemo da klasifikujemo na različite načine. Upravo zbog toga različiti autori predlažu različite klasifikacije terorizma.

Simeunović predlaže klasifikaciju terorizma prema:

„*Programsko-ciljnoj orijentaciji:*

1. Ideološki motivisan terorizam

1.1. Levičarski terorizam

1.2. Desničarski terorizam

2. Etno-separatistički terorizam

3. Verski fundiran terorizam

3.1. Terorizam sekti

3.2. Terorizam fundiran na interpretacijama velikih religija

- prema sredstvima i metodima

1. Klasifikacija terorizma prema sredstvima

1.1. Klasični (konvencionalni) terorizam

1.2. Biohemijski terorizam

1.3. Nuklearni terorizam

2. Klasifikacija terorizma prema metodima

2.1. Klasični (konvencionalni) terorizam

2.2. Samoubilački terorizam

2.3. Sajber - terorizam (upotreba interneta u terorističke svrhe)

2.4. Narko- terorizam

- prema tipu aktera - subjekata terorizma

1. Individualni terorizam

2. Terorizam organizacija i ilegalnih grupa

3.Institucionalni terorizam (državni i sl.)“ (Simeunović, 2009, 82-85)

Milašinović predlaže klasifikaciju terorizma prema načinu izvršenja terorističkog napada. Otuda pominje: „*tzv. promišljeni (koji izvode teroristi koji ne žele da budu uhvaćeni niti ubijeni) i samoubilački terorizam (koji izvode politički, verski, nacionalistički i drugi fanatici, koristeći konvencionalne ili improvizovane eksplozivne naprave, ne mareći za svoj život). Središnju, umerenu taktiku koristi tzv. aktivni strelac koji, koristeći vatreno, ređe hladno oružje ili oruđe pogodno za napad, ubija što više nevinih ljudi oko sebe, najčešće na javnom mestu (na ulici, u školi, u crkvi, u sredstvima javnog prevoza, u samousluzi, na sportskom stadionu itd.)*“ (Milašinović, 2011, 6).

Šikman klasifikuje terorizam na osnovu njegovih sledećih odrednica: „*motiv izvršenja, sredstvo izvršenja, način izvršenja, objekat napada ili neki drugi kriterijum*“ (Šikman, 2011, 46). Pokretački motivi terorista tokom vremena su se menjali. Nekadašnji „*tradicionalni*“ teroristi uglavnom su bili usmereni protiv tekovina savremene demokratske države, njenih struktura moći i nastojali su da broj žrtava bude što je moguće veći. Dok je savremeni terorizam usmeren uglavnom protiv postojećih ekonomsko-energetskih sistema, kako u nacionalnim tako i u međunarodnim okvirima, na primer kao što su tzv.„*energetski terorizam*“ ili je tzv.„*racionalni/kalkulišući*“ terorizam koje pominje Milašinović (Milašinović, 2011, 6). Težnje savremenih terorista usmerene su na stvaranje ekonomske štete što većih razmera i prekidanje dotadašnjih tokova novca, kako bi ugrozili postojeći životni standard i promenili trenutnu ekonomsku situaciju.

Prema sredstvima izvršenja, odnosno u zavisnosti od oružja koje se koristi u terorističkim aktivnostima razlikujemo: „*nuklearni, kiberterorizam, biološki, hemijski ili kombinovani terorizam*“ (Milašinović, 2011, 6). Obzirom da se upotrebom ovog oružja postiže masovno uništenje i materijalna šteta velikih razmera zajednički naziv za ovu vrstu terorizma je „*postindustrijski terorizam*“, odnosno „*super(mega)terorizam*“ (Milašinović, 2011, 7). Osnova karakteristika postmodernih nekonvencionalnih formi terorizma je zloupotreba visoko razvijene tehnologije savremenog društva.

Harmon ukazuje na „*ekološki terorizam*“ (Harmon, 2000 : 137–185), kao posebnu vrstu terorizma koji odlikuje primena nasilja radi ostvarenja jednog jasno određenog cilja, a to je ukazivanje na konkretne ekološke probleme zbog kojih se vrši pritisak na organe vlasti kako bi oni inicirali donošenje zakonskih propisa kojim bi se ti problemi rešili. Dalje, terorizam možemo da razlikujemo u zavisnosti od prostora u kojem se pretežno ispoljava tzv. „*urbani*“ ili „*ruralni*“ (Simeunović, 2009, 82), i u zavisnosti od toga da li je prisutan na tlu jedne konkretne države- „*unutrašnji*“ ili „*spoljni*“ - kada njegove posledice prevazilaze nacionalne granice (Simeunović, 2009, 82).

2.3. Teorijsko određenje pojma kiberterorizam

Kiberterorizam je savremena pojava novijeg datuma koja je nedovoljno istražena. Sve veća upotreba interneta i savremenih tehnologija iziskuje tumačenje mogućih pretnji i opasnosti u kibernetskom prostoru. Kiberterorizam se odigrava u specifičnom okruženju - virtuelnom koje raspolaže sopstvenim sredstvima i principima, gde su dešavanja i opasnosti neprimetni golim okom u stvarnom fizičkom svetu, dok njegove posledice i pričinjena šteta mogu direktno da utiču na svakodnevni život ljudi, na medije, javno mnjenje, infrastrukturu i bezbednost. U savremenom društvu je tehničko-tehnološki faktor dobio na značaju, toliko da tehnološka nadmoć na svetskoj sceni danas znači mnogo. Zato su se težnje za razvijanjem novih tehnologija uvećale. Infrastruktura savremenih država je pored fizičkih sredstava značajnim delom sačinjena od sredstava u kibernetskom prostoru. Dok je znanje, naročito u IT oblasti postalo primarni resurs. Savremene države ulažu veliku količinu finansijskih sredstava u naoružanje, čime se enormno uvećavaju kapaciteti za uništenje planete. Na taj način je tehnološki razvoj uvećao opasnost i ozbiljnost posledica od upotrebe savremenih IT tehnologija po bezbednost kako državnu uopšte, tako i pojedinih društvenih grupa ili pojedinaca. Otuda su kibernetski prostor, kiber ratovanje i kiberterorizam sve više aktuelna tema za razmatranje od strane stručnjaka i teoretičara iz oblasti bezbednosnih, pravnih, vojnih, informatičkih, političkih i drugih nauka.

Kao što navodi Kolin termin kiberterorizam skovan je krajem dvadesetog veka (Collin, 1997, 15). Međutim još uvek nije uspostavljena opšta saglasnost o tome šta predstavlja kiberterrorizam. Ovaj termin uglavnom služi da označi bezbednosne pretnje i različita kriminalna dela i sabotaže koja su izvršena pomoću računarske tehnologije. Ono što predstavlja otežavajuću okolnost za otkrivanje počinioca su uglavnom prednosti koje kiberterorizam ima nad tradicionalnim oblicima terorizma, a to su: anonimnost - mogućnost lakog kreiranja virtuelnog (sajber) identiteta, mogućnost kiberterorizma da nanese štetu velikih razmera nezavisno od realne udaljenosti počinioca i mete, relativno lak je za izvršenje, osim znanja iz IT oblasti i tehnološke opremljenosti ne zahteva neke dodatne organizacije i rizike.

Kada je reč o kiberterorizmu, izdvajaju se dva osnovna pravca razmišljanja. Prvi pravac, podrazumeva usko definisanje pojma tako da: „*On obuhvata politički motivisane hakerske operacije koje su namenjene da izazovu ozbiljnu štetu, kao što su gubitak života ili teške ekonomske štete*“ (Denning, 2001, 241).

Dakle, ovakvo usko definisanje kiberterorizma ga jasno razlikuje od običnog haktivizma politički motivisanog kompjuterskog kriminala. Dakle, kiberteroristi su oni počinioci, hakeri koji insistiraju na tome da su prvenstveno motivisani politikom, a ne nekakvom zlom namerom ili željom da ostvare finansijsku korist.

Drugi pravac razmišljanja koji uglavnom zastupaju vladini zvaničnici i lica vojne odbrane podrazumeva šire definisanje pojma kiberterorizma kao bilo koji napad u virtuelnom kibernetskom prostoru kojim se ugrožava bezbednost. Ovom, širem obliku određenja kiberterorizma pripada Šinder kada navodi: „*Napadi na kompjutere i računarske mreže mogu se definisati kao kibernetski terorizam ukoliko su njihovi efekti dovoljno destruktivni toliko da izazvaju strah koji je uporediv sa fizičkim terorističkim aktom*“ (Shinder, 2002, 19). Kiberterorizam je savremena forma terorizma koja se odnosi na „*nezakonite napade i pretnje napada na računare, mreže i informacije koje se tamo čuvaju*“ kako bi „*zastrašili ili primorali vladu ili njen narod da radi na ostvarenju političkih ili društvenih ciljeva*“ (Manap & Tehrani, 2012, 409) koji pogoduju teroristima. Kiberterorizam predstavlja značajnu pretnju, obzirom da podrazumeva „*upotrebu kompjuterskih mreža i internet alata za ometanje kritičnih nacionalnih infrastruktura (kao što su energija, javni prevoz, vladine aktivnosti) ili za zastrašivanje ili prisiljavanje vlada jedne zemlje ili njenih građana*“ (Lewis, 2002, 1).

Bez obzira na pravac razmišljanja precizna definicija kiberterorizama, treba da sadrži elemente koji ga jasno razlikuju od običnog kibernetičkog kriminala, haktivizma, pa čak i kiber ekstremizma. Pomenuti elementi prema Ekgaru i saradnicima su:

„a) *Pravni kontekst (namera, zavera, samo pretnja ili čin?);*

b) Kibernetski prostor služi kao oružje ili je cilj;

c)Cilj (i) zlonamerni postupak sadrže neku vrstu nasilja sa dalekosežnim psihološkim efektima kod ciljanog auditorijuma;

d) *Namera je kombinovana sa dugoročnim ciljem (npr. društvene ili političke promene, uticaj na političko odlučivanje) kojima teži terorista ili teroristička grupa*“ (Akhgar i dr., 2014, 13).

Opšte gledano pojam terorizam je kompleksan fenomen. Imajući u vidu da je reč o njegovom pojavnom obliku u specifičnom okruženju - kibernetskom prostoru, kompleksnost ovog fenomena se još više usložnjava, što dalje zahteva multidisciplinarni pristup prilikom njegove analize.

Kako bismo bolje razumeli kiberterorizam potrebno je „*da analiziramo sledeća pitanja:*

1) Ko su počinioci kiberterorizma (da li ih podržava država, da li ih država odbacuje, bilo da su kvazi formacije, hakerske grupe ili ljudi na vlasti koji se bave špijunažom);

2) Koje alate i tehnike primenjuju u procesu planiranja i izvršenja samog napada;

3) Kako primenjuju tehnike, taktike i postupke za izvođenje kibernapada (metod socijalnog inženjerstva, stvaranje i oslobađanje virusa, zlonamerni softveri);

4) Nakon izvršenja napada koje su kategorije meta ili potencijalne mete terorističkih kiber napada (informacione i komunikacione mreže, podaci, objekti u "stvarnom" svetu, energija, bankarstvo i finansije, vitalne usluge jedne zemlje);

5) Zašto vrše napad, odnosno šta ih motiviše za sprovođenje kiberterorističkih napada;

6) Kada se napad izvede, koji su rezultati, prednosti i mane takvih akcija“ (Ashley, 2003).

2.4. Karakteristike i pojavni oblici kiberterorizma

Kiberterorizam predstavlja spoj sedam ključnih elemenata:

1) ljudski (indivudalni - pojedinac, terorista ili grupni- organizacije u čije ime pojedinci deluju);

2) IT znanje (značajan resurs savremenog doba),

3) tehnološki (IT sredstva);

4) virtuelni (kibernetski prostor, online identiteti i online zajednice),

5) nasilje (nasilni upad na mrežu, pribavljanje podataka i td.)

6) strah

7) politička motivisanost za ostvarenje dugoročnog cilja.

Svaki napad na računar ili mrežni sistem, kiber pretnje, incidente i različite vrste vandalizma u kibernetskom prostoru ne možemo da svrstamo u terorizam. Jer, kiberterorizam nije isto što i kompjuterski kriminal. Ove dve pojave moramo da posmatramo odvojeno. Dešavalo se da mediji pojedine događaje pogrešno opisuju kao kiberterorizam, iako oni to nisu. Kao primer može da posluži slučaj iz 2000. godine kada je „*jedan Australijanac hakovao sistem upravljanja komunalnim otpadom i „izbacio“ milione litara otpadnih kanalizacionih voda u parkove, reke i preduzeća*“ (Smith, 2001). Pomenuti slučaj predstavlja kiber kriminal, a ne kiberterrorizam, obzirom da je počinioc delovao vođen isključivo individualnim motivima, a ne željom da promoviše određenu versku ili političku ideologiju. Tik i saradnici (Tikk i dr., 2010, 18.) smatraju da je napad u Estoniji 27. aprila 2007. godine bio jedan od prvih primera velikih kiberterorističkih napada, čiji je osnovni cilj bio da ugrozi nacionalnu sigurnost i destabilizuje finansijski sistem ove zemlje i izazove što veći broj neželjenih efektata na funkcionisanje javne uprave i privrede.

Postoje različita stanovišta o značenju termina kiberterorizam. Tako jedni smatraju da je upotreba ovog pojma neprimerena i previše usiljena, jer kiber napade ne možemo da okarakterišemo kao teror, nego pre više kao neku neprijatnost. Dok, se drugi autori pozivaju na njegove nepredvidive efekte i razorne posledice po državnu infrastrukturu, kao i na njegovu mogućnost da ugrozi kredibilitet neke vlade ili proizvede strah i nesigurnost širokih razmera u međunarodnoj zajednici.

Kako bi razlikovali kiberterorizam od klasičnog kiber napada, moramo dobro da razumemo oba pojma. Kiber napad, podrazumeva sukob koji se odvija u virtuelnom (kiber) prostoru. Može da bude vođen samostalno ili kao vid podrške nekom drugom sukobu. Kiberterorizam možemo da posmatramo kao posebnu vrstu kiber napada.

Uslovi koji su potrebni za uspešno izvođenje kiber napada su:

„a) *poznavanje ciljanog sistema, uključujući funkcije, servise, konfiguraciju, politike i alate zaštite i administriranje;*

b) *efikasno korišćenje programa koji će automatski eksploatisati ranjivosti za provaljivanje u računar (ti programi su poznati pod nazivom exploits);*

c) *kapacitet napadača da prikrije svoje tragove da bi izbegao mogućnost da bude detektovan i praćen;*

d) *brzina napada čime se smanjuje mogućnost da se sa preduzetim merama zaštite zakasni*“ (Vuletić, 2011, 22).

Dakle, pre izvršenja kiber napada potrebno je da se napadač detaljno pripremi, odnosno da prikupi što više informacija o meti napada, ciljanim sistemima, eventualnim „*rupama u sistemu*“ i ranjivostima (ljudskim, tehničkim i organizacionim), da se upozna sa njihovim mehanizmima zaštite i nivoima kontrole.

Postojeću literaturu koja se bavi evaluacijom kiber napada možemo da podelimo u tri šire kategorije: „*tehnološko-centrični modeli, socijalno- centrični modeli i situacioni model*“ (Hapa, 2017, 169-185). Obzirom da dela kiberterorizma predstavljaju posebnu vrstu kiber napada koji su izvršeni od strane teroriste i u skladu sa terorističkim ciljevima, pomenute kategorije možemo da primenimo i za tumačenje kiberterorizma.

Tehnološko-centrični model tumači kiber napade prevashodno sa tehnološkog aspekta. Brojni autori se zalažu za različite alate koji im omogućavaju otkrivanje kiber napada. Tako recimo, Bišop tumači kiber napade sa aspekta „*šest ključnih karakteristika: suštinska priroda defekta koji je prouzrokovan kiber napadom, vreme, dobitak ekspolatacije, oblast/područje kiber napada i izvor identifikacije ranjivosti prozrukovane kiber napadom*“ (Bishop, 1995).

Koen takođe pripada tehnološko- centričnom modelu i kada je reč o kiber odbrani zalaže se za tzv. „*model ogledala*“, na osnovu sledećeg seta karakteristika:

1. „*ortogonalna neispunjenost (Non-orthogonality)*“,

2. „*korelacija (Correlation)*“,

3. „*hardverska nespecifičnost (Hardwarenonspeci city)*“,

4. „*opis (Description)*“,

5. „*primenljivost (Applicability)*“

6. „*nepotpunost (Incompleteness)*“ (Cohen, 1997, 29-46).

Hačins i saradnici tumače „*cyber Kill-chain*“ prema tehnološko-centričnom modelu i navode sledeće faze kiber napada:

1. „*izviđanje (reconnaissance)*“ – podrazumeva istraživanje, identifikaciju i odabir meta, pribavljanje mailing liste (adrese e-pošte), stvaranje socijalnih veza ili prikupljanje informacija o specifičnim tehnologijama;

2. „*naoružavanje (weaponization)*“ – podrazumeva stvaranje mogućnosti za uspešnu isporuku automatskog alata (oružja) i ostvarenje željenog cilja/eksploatacije pomoću udaljenog pristupa. U praksi se sve više zloupotrebljavaju podaci poznatih ekstenzija, kao što su podaci u PDF formatu (*Adobe Portable Document Format*) ili *Microsoft Office* dokumenti.

3. „*isporuka (Delivery)*“ – najčešći nosioci alata/kiber oružja koji izazivaju kompjuterske incidente su e-mail prilozi, sajtovi i prenosive USB memorije.

4. „*eksploatacija (Exploit)*“ – isporuka alata domaćinu/žrtvi pokreće upadni kod koji omogućava eksploataciju operativnog sistema ili određene aplikacije.

5. „*instalacija (Installation)*“ – omogućava uprkos fizičkoj udaljenosti napadač/žrtva konzistentnost napada.

6. „*komanda & kontrola (Command & Control (C2))*“– ova faza podrazumeva aktivnu uključenost i manuelne operacije „*ruke na tastaturi*“.

7. „*aktivnosti prema ciljevima (Action on Objectives)*“ – nastupa tek nakon što su izvršene prethodne faze. Napadači preduzimaju akcije u skladu sa ciljevima, bilo da je to rušenje integriteta žrtava, prikupljanje poverljivih informacija, šifrovanje i dr. (Hutchins, Cloppert & Amin, 2011).

Tabela 1. Faze kiber napada (Hutchins et al., 2011, 12)

Phase	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	[Recipient List] Benign PDF	[Recipient List] Benign PDF	[Recipient List] Benign PPT
Weaponization	Trivial encryption algorithm		
	Key 1		Key 2
Delivery	[Email subject] [Email body]	[Email subject] [Email body]	[Email subject] [Email body]
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Exploitation	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp		
C2	202.abc.xyz.7 [HTTP request]		
Actions on Objectives	N/A	N/A	N/A

Kiberteroristi mogu da koriste različite metode za izvođenje napada:

- Upotreba konvencionalnog oružja (npr. vatreno oružje ili eksploziv) podrazumeva klasični fizički napad koji je usmeren protiv kompjuterske opreme, objekta ili dalekovoda čiji je cilj da ometa rad, pouzdanost opreme i onemogući njihovo funkcionisanje.

- Upotreba elektromagnetne energije podrazumeva upotrebu elektromagnetnog pulsa za izvršenje elektronskog napada koji je usmeren protiv kompjuterske opreme ili s ciljem da ometa prenos podataka. Pregrevanjem struje ili ometanjem komunikacija, elektronski napadi ometaju pouzdanost opreme i integritet podataka.

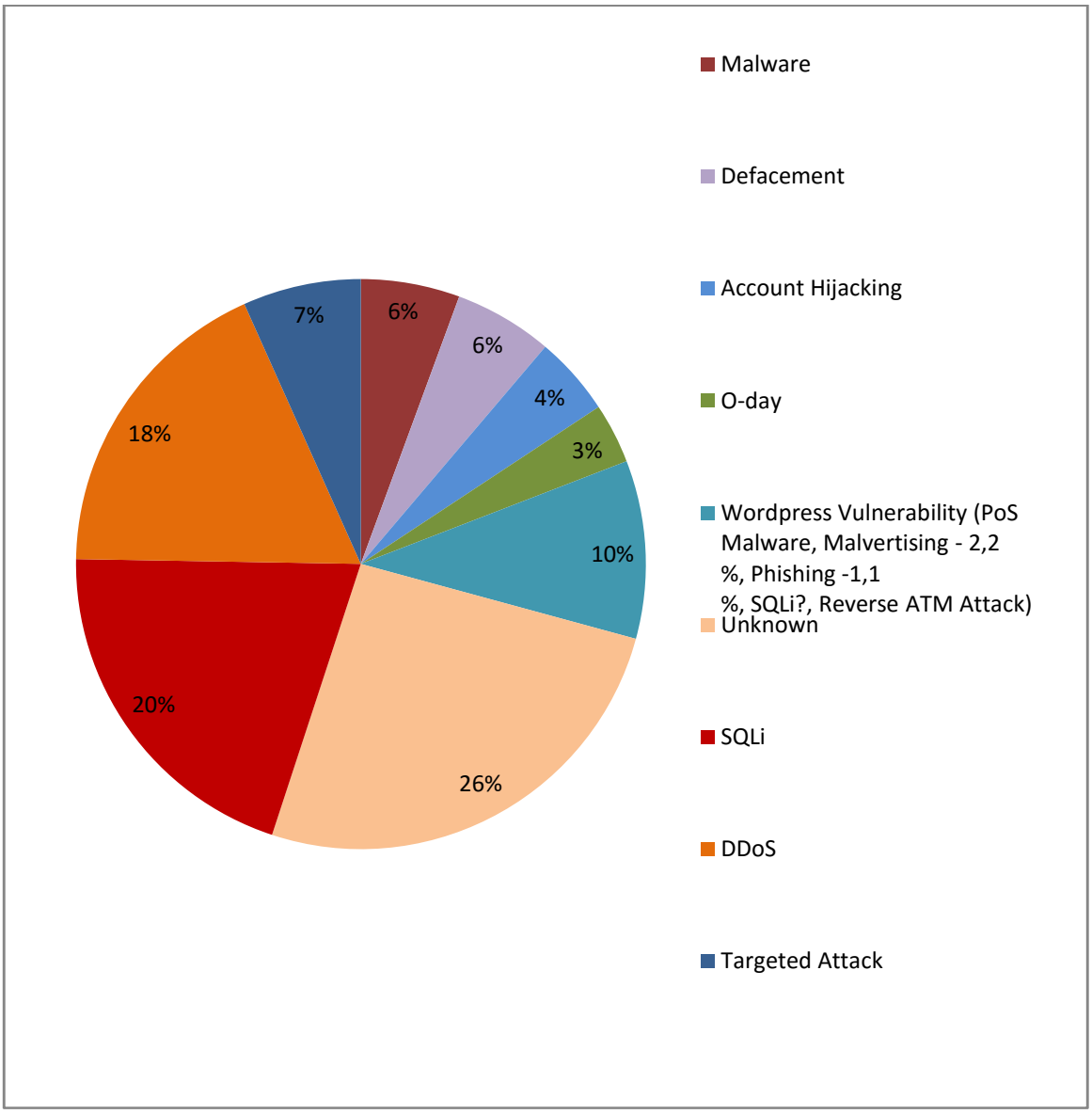
- Napad na kompjuterske mreže (*CNA- Computer Network Attack*) podrazumeva kibernetski napad koji je usmeren na računarski procesni kod, njegovu logiku i instrukcije ili podatke. Ovakav napad generiše tok štetnih mrežnih paketa koji su namenjeni za ometanje podataka ili logike, a služe se slabostima računarskog softvera i sigurnosnim propustima u sistemu računara određene organizacije koja je meta napada (Weiman, 155-156). Dela kiberterorizma su složena i mogu da uključe sve tri navedene metode ukoliko je politička namera terorista da namenski ciljaju određene kompjuterske objekte primenom: fizičkog, elektronskog i kibernetskog napada. Najznačajniji i najdestruktivniji kiber napadi su: napad na *SCADA* sisteme, napad na „*bot mreže*“, „*DDoS* napad“ i „*START/STOP napad*“[2], koji se odvija sledećim redosledom *SCAN*, *STOP* and *START*. Kod ovih vrsta kiber napada jedino se konstantnim sistematskim nadzorom postiže efikasna odbrana i bezbednost.

Tabela 2. Primer start/stop napada (Yılmaz & Gönen, 2018, 98)

Feature	**Content (Hexadecimal/ Decimal)**
Attack signature	0300001e02f08072
Sequence Number	237
Identification	0x0193 (403)
Source	192.168.10.18
Source port	34347
Destination	192.168.0.4
Destination Port	102
Type	Ipv4 (0x0800)
Flags	PSH, ACK
Version	4
Data	7202000f32000004f2000000834000000000072020000

[2] O pomenutim napadima će detaljnije biti reči u poglavlju 2.6. Posledice kiberterorizma.

Slika 1. Tehnike kibernapada (Munkhdorj & Yuji, 2015, 110)



Socijalno-centrični model karakteriše nastojanje da se kiber napadi razumeju i predvide pomoću ljudskog (socijalnog) faktora. Ovakav pristup podrazumeva identifikaciju pojedinaca koji ne uživaju potpuno poverenje i koji bi mogli da predstavljaju znatan rizik po kiber bezbednost. Istaknuti autori (Greitzer & Ferrymann, 2013, 90-97; Kandias et al., 2013, 261-266; Stavrou, 2014, 119-131) koji se zalažu za primenu ovog modela nude metode i metrike za procenu i predviđanje „*insajderskih pretnji*“. Za identifikaciju/mapiranje potencijalnih problema i slučajeva narušavanja kiber sigurnosti/poverljivosti potrebno je da uključimo u analizu ljudsko

ponašanje i interakciju sa interfejsom, odnosno sve odnose između korisnika međusobno, njihovih ciljeva i okruženja (Akhgar, et. al., 2014, 51).

Tabela 3. Socijalno-centrični model, faktori kiber napada (Akhgar et al., 2014, 51)

Faktori (Factors)	**Sistemske karakteristike(System Characteristics)**
Faktori pružaoca usluga (Service provider factors)	•Privatnost, sigurnost i sigurnosne karakteristike (Privacy, assurance and security features)
	•Robustnos (Robustness)
	•Neuspešne karakteristike (ili redundantnost) (Fail safe characteristics (or redundancy)
Karakteristike korisnika (User characteristics)	•Propustljivost poverenja (Propensity to trust/confidence)
	•Iskustvo i poznavanje upotrebe interneta (Experience and proficiency in internet usage)
	•Očekivanje onoga što se pruža (Expectation of what is being provided)
	•Nivo svesti o pretnjama kiber bezbednosti (Levels of awareness about cyber-security threats)
Sigurnosni alati (Security tools)	•Znaci društvene prisutnosti (Social presence cues)
	•Kapacitet prilagođavanja i personalizacije (Customization and personalization capacity)
	•Ograničeni interfejsi koji omogućavaju slobodnu upotrebu (npr. Sposobnost prenosa detalja preko sigurne mreže) (Constrained interfaces that allow free use (e.g., ability to convey details over a secure network)
	•Dinamička priroda bi trebala da bude besprekorna (i prodorna) (Dynamic nature should be seamless (and pervasive)
Bezbednosni zadaci (Security tasks)	•Korisnički interfejs ima visok stepen korisnosti (User interface has high degree of usability)
	• Izrične sigurnosne karakteristike (Explicit security characteristics)
	• Informacije kvalitet / kvantitet / pravovremenost (Information quality/quantity/timeliness)
	• Grafičke karakteristike (Graphical characteristics)
Operativno okruženje (Operational environment)	• Iskustvo i upoznavanje sa on-line kompanijom (Experience and familiarity with the online company)
	• Jednostavnost upotrebe u različitom kontekstu upotrebe (Ease of use in different contexts of use)
	• Komunikacija različitih nivoa opasnosti (Communicating different threat levels)

Situacioni model - Pobornici ovog modela za razumevanje kiber napada primat daju situacionim elemenatima, odnosno faktorima iz okruženja. Međutim, za adekvatno tumačenje kiber napada od suštinskog je značaja da se uzmu u obzir sva tri pomenuta aspekta.

Za evaluaciju kiberterorizma takođe možemo primeniti kvalitativne kriterijume koji služe za evaluaciju kiber-napada:

„1. *Jačina - Određuje se po obimu, trajanju i intenzitetu posledica kiber napada.*

2. Neposrednost - Odnosi se na brzinu kojom se posledice manifestuju.

3. Direktnost -Ispituje lanac uzročnosti.

4. Invazivnost - Odnosi se na stepen do kojeg operacije u kibernetskom prostoru predstavljaju ciljane upade na državu ili na njene mrežne sisteme koji štete interesima te države.

5. Merljivost efekata - Odnosi se na činjenicu da što je više posledica kvantifikovano i identifikovano, država će lakše da proceni situaciju nivoa upotrebljene sile tokom kiber napada.

6. Vojni karakter - Verovatnoća veze između kiber operacije i vojnih intervencija.

7. Uključenost države.

8. Međunarodno pravo“ (Pipyros i dr., 2018, 376) odnosno u kojoj meri je njegovo kršenje.

Kako da razlikujemo običan (ili kombinovan) kiber napad od onog koji je izvršio terorista? Ekgar i saradnici predlažu sledeće elemente:

- „*Integritet informacija*“ (npr. neovlašćeno brisanje, neovlašćene promene) što dovodi do gubitka poverenja u *IKT (Informaciono komunikacione tehnologije)* i društvo. Ciljevi bi mogli da budu baze podataka koje su ključne za društvo: lična dokumentacija, dokumentacija za registraciju vozila, vlasničku imovinu, finansijski podaci i računi.

- „*Poverljivost informacija*“ - Povreda poverljivosti velikih razmera kada se dovede u pitanje poverljivost ličnih podataka ili podataka od pojedinih organizacija koja može da se svrsta u društveni poremećaj, npr. objavljivanje kompletne zdravstvene evidencije o HIV-inficiranim licima u naciji mogla bi da pokrene niz uznemiravanja i samoubistava.

- „*Dostupnost IKT usluga (servisa)*“ - Odnosi se na otežavanje, onemogućavanje dostupnosti brojnih usluga koje Informaciono-komunikacione tehnologije pružaju. Na primer, onemogućavanje usluga tokom dužeg vremena, neovlašćeni prekid rada pojedinih sistema, mreža ili fizički, ili elektromagnetni napad na data centre i kritične komponente IKT sistema.

- „*Procesi zasnovani na IKT koji kontrolišu fizičke procese u stvarnom svetu*“, npr. kiberteroristi su usmereni na ometanje rada nuklearnih elektrana, rafinerija, saobraćaja vozila i drugih oblika transporta, monitoring i kontrolu zdravlja, na upad u tzv. pametne mreže i pametne gradove (Akhgar et al., 2014, 14).

Rolins i Vilson navode dva ključna elementa koja treba da budu ispunjena kako bi se određeni akt smatrao kiberterorističkim: prvi je „*efekat- kada napad na računarski sistem izaziva strah, kao i tradicionalni akt terorizma; drugi namera - postizanje političkih ciljeva*“ (Rollins & Wilson, 2007, 3). Dakle, jedino „*politički motivisanu upotrebu kompjutera kao oružje ili kao metu/cilj, od strane podnacionalnih grupa ili tajnih agenata, čija je namera da nasilno utiču na javnost ili vladu kako bi ona promenila svoju politiku*“ (Wilson, 2003, 4) možemo smatrati delima kiberterorizma.

Obzirom da na globalnom nivou nisu taksativno nabrojana dela koja možemo da svrstamo u kiberterorizam, slobodno možemo reći da su strah i neznanje pojmovi koji su prevashodno tesno povezani sa tumačenjem ovog pojma. Povelja *UN (United Nations)* ne daje precizne kriterijume za određivanje kada određeno delo možemo da smatramo kao „*upotrebu sile*“ ili kao „*oružani napad*“, odnosno koje mere se mogu preduzeti i do koje mere kako bi se održao ili obnovio međunarodni mir i sigurnost. Postoji čak „*podela između onih koji se kiberterorizmom bave na: „hypers“- oni koji veruju da su se kiber napadi zaista i dogodili - i „de- hypers“ - oni koji veruju da se takva vrsta napada još uvek nije dogodila*“ (Dunn-Cavelty, 2008).

Tallinn Manual, međunarodna grupa eksperata u Priručniku o međunarodnom pravu koje se primenjuje za tumačenje kiber napada, predlaže da se sve kiber aktivnosti kategorizuju na osnovu dva kriterijuma: „*intenzitetu pričinjene štete i kršenju međunarodnog prava*“ (Schimitt, 2013). Stoga nude sledeću kategorizaciju:

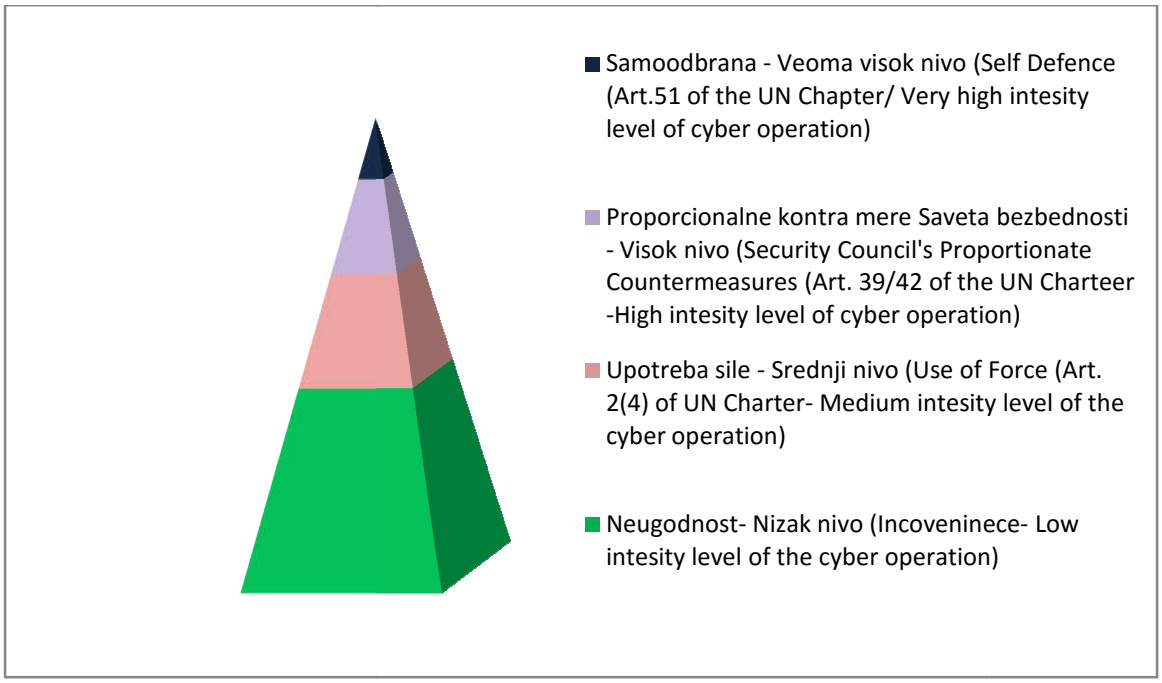
1) Napade najnižeg stepena ugroženosti, čiji intenzitet napada ne podrazumeva ništa više od jednostavnih neugodnosti po funkcionisanje države. Takvi problemi nisu izazvani, niti imaju uticaj na učesnike u napadu i ne predstavljaju „*upotrebu sile*“ ili pretnju zbog kršenja međunarodnog prava.

2) Drugi stepen intenziteta obuhvata one kiber napade koji se dotiču nivoa „*upotrebe sile*“, što je predviđeno članom 2 (4) Povelje UN-a „*svi članovi će se u svojim međunarodnim odnosima uzdržati od pretnje ili upotrebe sile usmerene protiv teritorijalnog integriteta ili političke nezavisnosti bilo koje države ili bilo kojeg drugog načina koji nije u skladu sa ciljevima Ujedinjenih Nacija*“ (Povelja UN u: Schmitt, 2013, 47).

3) Treći nivo se odnosi na kiber napade takvog intenziteta da ugrožavaju međunarodni mir i stabilnost. Ovakvi slučajevi kiber napada podrazumevaju aktivnu uključenost Saveta bezbednosti, i pozivanje na Rezoluciju Saveta bezbednosti prilikom utvrđivanja obima pretnje ili pričinjene štete, agresije ili kršenje mira, što dalje zahteva privremene mere (ekonomske ili trgovačke sankcije) ili daje ovlašćenja svojim mirovnim snagama da upotrebi silu.

4) Najveći stepen su kiber operacije čiji je intenzitet merljiv oružanom napadu. U ovim slučajevima postoji inherentno pravo na samoodbranu, prema poglavlju VII UN (Schimitt, 2013, 42-54).

Slika 2. Nivo intenziteta kiber operacija prema odredbama Povelje UN (Pipyros i dr., 2018, 375)



Veoma je značajno da dobro razumemo sve pojavne oblike kiberterorizma, kako bismo mogli adekvatno da se odbranimo. Otuda je važno uzeti u obzir postojanje sva tri osnovna nivoa napada kiberterorista: „*jednostavno - nestrukturirani, napredno- strukturirani i složeno-koordinirani*“ (Jalil, 2003; Fallico, 2013).

Prvi, „*jednostavno- strukturirani*“ napadi za izvršenje ne iziskuju kompleksne alate i veštine upravljanja. Otuda je ovo najniži nivo napada. Najčešće je to brisanje/uklanjanje podataka (*data remove*), gde napadač poseduje osnovne veštine i služi se alatima koje je napravio neko drugi.

Drugi, „*napredno-strukturirani*“ nivo kibeterorizma podrazumeva da napadač poseduje veštine da izvrši naprednije napade na više sistema i mreža istovremeno, da modifikuje ili kreira osnovne hakerske alate. Najčešće su to online pljačke sa bankovnih računa.

Treći, „*složeno-koordinirani*“ napadi su najkompleksniji, podrazumevaju viši nivo pripreme i organizacije za sprovođenje napada, upotrebu sofisticiranih hakerskih alata i znanja za izvršenje masovnih poremećaja upotrebom kompjutera. Najčešće su to iniciranje: avionskih nesreća, kolapsa saobraćaja, nestanka struje, telekomunikacijskih lomova.

Ekgar i saradnici ukazuju da: „*kiber teror protiv zemlje i njenih građana može da se odvija na nekoliko nivoa sofisticiranosti, pri čemu svaki nivo zahteva sposobnosti u smislu tehnologije i investicija napadača. Pričinjena šteta je direktno proporcionalna nivou ulaganja*“ (Akhgar i dr., 2014, 168). Dalje, oni razlikuju prema skali pričinjene štete „*tri osnovne kategorije kiber napada: 1. napad na pristupnu mrežu organizacije (attack on the gateway of an organization), 2. napad na informacione sisteme organizacije (attack against the organization's information systems; 3. napad na osnovne operativne sisteme (attacks on an organization's core operational systems*“ (Akhgar, et. al., 2014, 168).

Prvi, najosnovniji i najjednostavniji nivo kiberterorizma predstavljaju uglavnom:

- *Websites* napadi – direktni upadi na internet stranice, koji onemogućavaju pristup veb stranici, ometaju njen rad tako što manipulišu informacijama i podacima, dok je pričinjena šteta kratkotrajna i brzo rešiva.

- *DdoS* napadi- distribuirano poricanje usluga. Najčešće mete napada su banke, mobilni operateri, pružaoci usluga kablovske i satelitske televizije, razne berzanske usluge, mediji i dr.

- Napadi na *DNS (Domain Name System)*[3] servere –služe da usmere protok informacija putem interneta pružajući određene lokacije i informacije na koje napadači žele da usmere internet saobraćaj. Ovo se postiže tako što se zahtev korisnika prebacuje sa njegovog računara na lokaciju napadača, a ne na stvarnu lokaciju koju je korisnik odabrao za pretragu ili rad na internetu *(surf)*. Najčešća šteta je pored uskraćivanja usluga klijentima, krađa informacija, što dovodi u pitanje funkcionalnost i reputaciju servisa. Takođe, teroristi se služe propagandom svojih aktivnosti i ciljeva, te im ova vrsta napada služi da preusmere internet saobraćaj na odgovarajuću stranicu i sadržaje koji ih promovišu.

Druga vrsta kiber terorizma na skali pričinjene štete u kibernetskom prostoru podrazumeva srednji nivo, jer uključuje različite napade na informacionei računarske sisteme u kojima se pohranjuju i obrađuju podaci (serveri, baze podataka). Za izvođenje ove vrste napada potrebno je da napadač raspolaže naprednijim tehnološkim sredstvima i veštinama. Takođe, ova vrsta napada zahteva pristup računarima iznutra, odnosno učestvovanje zaposlenih lica u organizaciji kojoj nastoji da se nanese šteta i onemogući pružanje usluga. Najčešće mete napada su banke, mobilni operateri i internet provajderi. Jasna razlika između ove vrste napada kiberterorista i trećeg najsofisticiranijeg oblika kiberterorizma je u tome što ovi napadi ne rezultiraju fizičkim oštećenjima, ali se, ipak, oslanjanju na virtuelne usluge i pristup njima, te mogu da proizvedu značajnu štetu. Kao primer može da posluži napad na kompjutere naftne kompanije u Saudijskoj Arabiji poznatoj pod imenom *Aramco* koji se desio u avgustu 2012. godine. Napadači su koristili kompjuterski virus *Shamoon* koji je onesposobio funkcionisanje 30.000 računara. Iako napad nije uticao na osnovne operativne sisteme kompanije, ugrozio je njen rad tako što su brojni podaci organizacije izbrisani sa računara, što je znatno otežalo i usporilo dalje radove kompanije u dužem vremenskom periodu. To se potom znatno odrazilo na naftnu industriju i poremetilo tadašnju ravnotežu moći naftnih kompanija u toj zemlji.

Treća vrsta podrazumeva napad na kritičnu infrastrukturu, odnosno osnovne operativne sisteme organizacija. Ovakva vrsta kiberterorističkih napada je najsložena i može da se odvija na nekoliko različitih nivoa, u zavisnosti od tehnoloških sredstava i sposobnosti kojima kiber napadač raspolaže, dok je pričinjena šteta direktno srazmerna nivou ulaganja.

[3] DNS je baza podataka pomoću koje se prevode imena hostova u IP adrese. Na primer, ime hosta kao što je www.google.com prevodi se u IP adresu kao što je *216.58.217.46*. Zavaljujući tome je pretraga u bilo kojem poznatom pretraživaču jednostavna tako što ukucate adresu koja se potom šalje u DNS server koji prebacuje traženu adresu u IP adresu za lako pronalaženje željene stranice.

Najčešći primeri ove vrste napada su napadi na sisteme koji upravljaju i kontrolišu rad industrijskog sektora neke zemlje (gorivo i gas, vodovod, struja, sistemi javnog transporta ili bankarski sistemi plaćanja itd.). Ovakvi napadi su najsofisticiraniji, jer sadrže u sebi momenat kada se pričinjena šteta preliva iz kibernetskog prostora u realnost i uzrokuje fizičku štetu, čiji efekti mogu da budu značajno destruktivni po određenu državu i njenu naciju.

Dželel navodi: „*pet glavnih tipova kiberterorističkih napada:*

1) upad (incursion);

2) uništenje (destruction);

3) dezinformacija (disinformation);

4) odbijanje usluge (denial service);

5) diskreditovanje sajtova (defacement of web sites)" (Jalil, 2003, 8). Navedeni napadi se razlikuju po težini pričinjene štete i ciljevima.

2.5. Glavni učesnici i mete

Bavljenje bilo kojom formom terorizma podrazumeva i razumevanje pojma teroriste. Tako na primer, „*Ujedinjene nacije smatraju da je terorista svaka osoba koja, delujući nezavisno od znanja neke zemlje, ili kao pojedinac, ili kao član grupe koja nije priznata kao zvanično telo ili deo neke nacije, postupa na taj način što uništava ili oštećuje imovinu civilnog stanovništva ili vlada da bi postigao neki politički cilj*“ (Gaćinović, 2011, 23).

Intenzivan razvoj tehnologija i globalno umrežavanje proizvele su novi oblik terorizma, koji je proistekao iz integracije čovek-računar (socijalna fuzija i fisija). Socijalna fuzija koja proističe iz te relacije se odnosi na brojne prednosti koje računari daju ljudima (brža i lakša komunikacija, baze podataka, pretraživanje i dr.). Otuda nastaje *IoT– The Internet of Things* aktuelna sisitemska paradigma koja podrazumeva isprepletanu mrežu percepcija, kiber interakcije, društvene odnose, uključuje i kognitivno mišljenje. *IoT* predstavlja „*savršenu integraciju novog kiber-fizičko-društvenog mišljenja (CPST, cyber-physical-social-thinking) u kiberprostoru, što nastaje kao rezultat međuljudske interakcije, umrežavanja različitih uređaja i manipulacije u njima*” (Ning et al., 2016, 504-522). Dok, socijalna fisija podrazumeva korišćenje tih prednosti na destruktivan način, bilo autodestruktivno (socijalna izolacija) ili destruktivno po širu društvenu zajednicu (kiberteroristički napad i sl.). Obzirom da su „*internet i društvene mreže idealno mesto za sprovođenje terorističkih aktivnosti i operacija jer omogućavaju geografski neograničene akcije i njihovo brzo sprovođenje*“ (Wagner, 2005, 7), nova generacija terorista usmerena je na korišćenje ovih prednosti prilikom izvođenja svojih operacija. Otuda se potencijalne pretnje od ove savremene forme terorizma (kiberterorizam) uporedo sa razvojem tehnologije usložnjavaju.

Jer, kiberterorizam uključuje u sebe ljudski i tehnološki momenat. Dok, prednosti kibernetskog prostora omogućavaju teroristima da ostanu anonimni i formiraju lažne IP profile i adrese. Zbog ove kompleksnosti potrebni su izuzetni napori, napredno tehnološko znanje i osposobljenost najsavremenijim tehnologijama da bi se utvrdio identitet počinioca kiberterorizma, njegova namera ili eventualna politička i finansijska podršku koju je kao izvršilac imao. Da bismo se adekvatno branili od kiberterorista, najpre je potrebno da ih identifikujemo i dobro poznajemo njihove ključne karakteristike.

Potencijalni kiberterorista može da bude svako ko ima neprijateljske namere, dobro znanje iz oblasti informacionih tehnologija i pristup poverljivim IT informacijama. Odnosno da bismo razumeli terorizam važno je da razumemo um, odnosno psihu terorista, kao i da imamo u vidu njihove generalne karakteristike kao što su pravdoljubivost i motivisanost ideologijama, politikom, religijama, osvetom, bilo pojedinačno ili u kombinaciji. Naša predstava o teroristima kao duševno poremećenim ljudima je pogrešna. „*Na osnovu raspoloživih naučnih dokaza o vezi između nasilja i mentalnih bolesti u populaciji, nasilje većinom nije uzrokovano velikim psihijatrijskim problemima kao što su šizofrenija, bipolarni poremećaj ili depresija*“ (Swanson, 2012).

Dosadašnja istraživanja pokazala su sledeća polna, starosna i klasna obeležja terorista. Uglavnom su to muškarci. Međutim, žene i deca, takođe nisu izuzeti kao počinioci terorističkih dela. Štaviše, oni su bili izmanipulisani da se pridruže terorističkim organizacijama i budu značajni akteri. Otuda se pojavljuju deca kao vojnici (Glazer, 2006, 373-384) i osmogodišnji bombaši u Pakistanu (Mohsin, 2013) i terorističkim dejstvima na Šri Lanki - Tamilski Tigrovi (Murray, 2010). Klasna „*analiza više od 150 terorista Al-Kaide pokazala je srednju i višu srednju klasu, visoko obrazovanih, oženjenih muškaraca srednjih godina*“ (Wasielewski, 2007, 13-18). Sent Kler kao aktere kiberterorizma pominje: „*teroristička organizacije, njihove simpatizere i tražioce senzacije*“ (Saint-Claire, Steve, 2011).

Teroristička organizacije - Iako su materijali terorističkih grupa transparentni i lako se mogu pronaći na internetu, terorističke grupe su „*zatvorene*“ i bazirane na poverenju kako bi sačuvali u tajnosti svoje metode napada i pouzdane učesnike. Inače, ove grupe mogu da budu dostupne drugima, npr. preko *Cloud* platformi i proverenih kanala komunikacija (*chat rooms* i dr.). Terorističke organizacije čije aktivnosti prednjače na internetu su:

1) Al-Kaida (*Al-Qaeda*) – Mnogi pripadnici Al Kaide poseduju dobro obrazovanje u oblasti inženjerstva i tehnologije. Nakon organizovanog napada u Avganistanu, novembra 2001. godine kada su američke snage iznenada napale aktiviste Al Kaide, mnogi od njih su bili prinuđeni da pobegnu iz Kabula. Tada je pronađeno mnogo osetljivih informacija i dokumenata, koje su operativci Al Kaide ostavili za sobom, koji potvrđuju profil terorista kao dobro obrazovanih i obučenih za rad na kompjuterima i operativnim sistemima: „*Tehničke skice na arapskom, engleskom i nemačkom jeziku, studentske beležnice na arapskom, turskom, kurdskom*

i ruskom jeziku pokazale su doslednost u interesovanju i široko poznavanje električnog i hemijskog inženjeringa, atomske fizike, balistike, kompjutera i radio stanica" (Davis, 2002).

2) ISIS – Američka kompanija za kiber-sigurnost „*Fire Eie*" javno je izjavila da ISIS koristi tamnu mrežu (*dark web*)[4] za upotrebu kiberprostora u terorističke svrhe. Na taj način ISIS može da obavlja trgovinu kiber oružja/alata, što ne zahteva mnogo sredstava i stručnosti (Auwema, 2015, 82).

3) IRA (*Irish Republican Army*) – Nakon ekonomskih sankcija koje su SAD i evropske zemlje stavile na Iran, IRA je sponzorisala grupu terorista za izvođenje kiber napada kao odgovor na pomenutu situaciju (Menn, 2013).

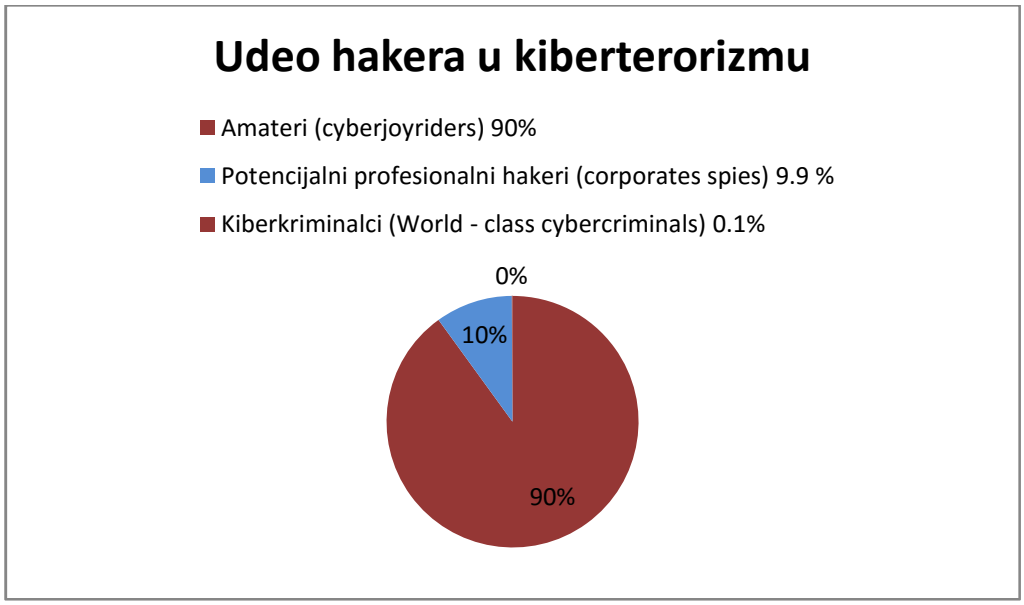
4) Tamilski tigrovi (*Liberation Tigers of Tamil Eelam*) - Najsmrtonosnija teroristicka grupa Šri Lanke, osnovana 1976. godine, zabranjena u preko trideset zemalja širom sveta. Ova teroristička grupa je bila glavni razlog za građanski rat u Šri Lanci. *Internet Black Tigers (LTTE)* su specijalizovana frakcija Tamilskih tigrova čiji je osnovni cilj da štete vladi Šri Lanke putem kiberterorističkih operacija (Vidanage, 2006, 3).

5) Popularne radikalne grupe od međunarodnog značaja, poput libanskih šiita (*Shi'ite Islamic group*), Islamska država - Hezbolah iz Libana **(***Kataib Hezbollah***)**, koriste internet sajtove u različite svrhe: za objavljivanje članaka ili planiranih predstojećih događaja, za objavljivanje nedavno snimljenih video snimaka itd. (Deutch, 1996).

Kao akteri kiberterorizma se mogu javiti i *simpatizeri* - oni kojima je ideologija terorističkih organizacija bliska, ali nisu aktivno uključeni u online terorističke delatnosti. Treća kategorija aktera su *tražioci senzacije* (*thrill seekers*) - napadači kojima primarni motiv nije politički ili ideološki, već su vođeni težnjom da dostignu slavu. Najčešće su to hakeri koji žele da proslave svoje ime (pseudonim) činjenjem kiber napada koji zahtevaju vrhunske IT veštine.

[4] *Dark web*, poznat takođe i pod nazivima *deep web, deep net, invisible web* predstavlja tamnu, skrivenu stranu interneta kojoj se može pristupiti samo kroz specijalizovane pretraživače. Koristi se uglavnom za web komunikacije koje se ne mogu presretati, otuda 57% dark web-a zauzimaju ilegalni sadržaji kao što su pornografija, nedozvoljene finansije, trgovina drogom, oružjem, krivotvorena valuta, teroristička komunikacija i još mnogo toga (Moore & Rid, 2016, 7-38).

Tabela 4. Udeo hakera u kiberterorizmu (Sproles & Byars, 1998)



Najveću pretnju po kiber bezbednost predstavljaju: hakeri (profesionalci i amateri), nezadovoljni zaposleni, kiber-kriminalci, kiber-terorističke grupe i drugi. Istraživanje Sprolesa i Bajersa (Sproles & Byars, 1998) koje je sprovedeno na uzorku od 100.000 hakera pokazalo je sledeći udeo hakera u kiberterorizmu: hakeri-amateri su odgovorni za oko 90% svih terorističkih aktivnosti na internetu, 9,9 % čine potencijalno profesionalni hakeri i 0,1 % međunarodno svetski poznati kiberkriminalci.

Teroristi uglavnom regrutovanje novih članova baziraju na propagandi svojih ideja, odnosno apelu za zaštitu ranjivih i ugroženih društvenih grupa, pozivajući se na osećaj nepravde, otuđenja i poniženja. U tome im mnogo pomaže primena „*narrowcasting*“ metode, odnosno uzak odabir ciljane subpopulacije, te i usmerenje propagande prema njenim specifičnim demografskim karakteristikama (kao što su starost ili pol), društvene ili ekonomske okolnosti (Weimann 2008). Tako se na primer, za regrutovanje maloletnika putem interneta distribuira propaganda koja može da bude u obliku dečjih priča, karikatura, popularnih muzičkih spotova ili kompjuterskih igara koji sadrže poruke kojima se promovišu i proslavljaju teroristička dela, kao što su samoubilački napadi. Dalje, neke terorističke organizacije su dizajnirale „*online*“ video igre koje bi se koristile kao sredstva za zapošljavanje i obuku i koje promovišu upotrebu nasilja.

U naučnoj javnosti preovladava shvatanje da su ciljevi terorista prvenstveno politički (verski, nacionalistički ili separatistički). Međutim, poznato je da su motivi i ciljevi promenljive kategorije, te da teroristi mogu svojim ciljevima da pripoje i ciljeve svojih finansijera. Različiti uzroci i motivi mogu da navedu pojedinca da se bavi terorizmom, kako politički, etnički, verski, tako i ideološki, ekonomski – kriza, siromaštvo, nesigurnost, socijalni - anomija, socijalna izolovanost, psihološki - karakterne crte ličnosti, određene frustracije, nagomilani stres i nezadovoljstvo postojećom životnom situacijom, ideološki, geopolitički, teritorijalni – etnoseparatistički, nacionalistički i kombinovani. Teroriste nesumnjivo karakteriše primena nasilja u ostvarenju ciljeva, kako u realnom prostoru – fizička, tako i kiberprostoru- digitalna. Pomenuta primena nasilja je upravo ono što dodatno modifikuje prvobitne motive terorista i rasplamsava dalje njihove težnje da na nasilan nelegitiman način pokušaju da promene postojeću društveno- političku stvarnost, izazovu rušenje konkretne državne vlasti ili iznude određene političke ustupke. Ono što karakteriše počinioce terorističkih kibernetskih napada je jasna usmerenost na metu, dobra organizovanost i kocentrisanost napada tako da oni udruženo imaju veće šanse da nanesu ozbiljnu štetu ciljanoj meti.

2.6. Posledice kiberterorizma

Veliki su izgledi da će kiberterorizam postati popularniji u budućnosti, naročito po pitanju bezbednosti informacionih tehnologija. Brz napredak informacionih tehnologija i porast broja visoko kvalifikovanih stručnjaka iz ove oblasti uz relativno niske troškove i jednostavno izvršenje kiber napada, stvaraju pogodno tle za napade na kompjuterske sisteme.

Savremene države oslanjaju funkcionisanje ključnih vitalnih struktura na savremene tehnologije i kompjuterske sisteme. Otuda je naveći izazov za kiberteroriste ciljanje na IT tehnologije koje podržavaju rad ključnih/kritičnih infrastruktura. Šta podrazumevamo pod kritičnom infrastrukturom? „*Skup mreža, entiteta, sistema i struktura koje mogu oštetiti održivost društvenog poretka ili javne službe kada prestanu da ispunjavaju svoje funkcije delimično ili potpuno*“ (Yagli & Dal 2014, 911). Iako je kritična nacionalna infrastruktura generalno dobro zaštićena u većini zemalja, nikada nije na odmet poboljšanje nivoa sigurnosti ovih infrastruktura i jači vid otpora protiv dela kiberterorizma. Jer, bez obzira na način na koji se kiberterorizam ispoljava, kada je glavna meta napada kritična infrastruktura, posledice mogu da budu katastrofalne.

Postoji nekoliko različitih oblika (Wilke, 1999) kiberterorizma koji stvaraju katastrofalne posledice. Tako on može da bude u vidu jednog velikog napada na kritičnu nacionalnu infrastrukturu, ili u vidu serije koordiniranih, naizgled nezavisnih napada.

Kritične infrastrukture su:

„*-Fabrike za preradu hrane*

- Farmaceutska postrojenja

- Postrojenja električne energije i prirodnog gasa

- Raskrsnice pruga i sistemi za kontrolu saobraćaja

- Sledeća generacija kontrole vazdušnog saobraćaja

- Sva moderna vojna oprema

- Komunikacije vojske i javne bezbednosti

- *Civilne komunikacije*“ (Damnjanović, 2009, 245)

Prema Noujenu „*tumačenje posledica kiberterorizma je izazov i gotovo nemoguće bez uzimanja u obzir njegovih sledećih karakteristika:*

1. Obim efekata (Scope of Effects);

2. Nepredvidljivost (Unpredictability);

3. Reverzibilnost štete (Reversible Damage);

4. Anonimnost i problem pripisivanja odgovornosti, krivice za pričinjenu štetu (Anonymity and the Problem of Attribution)“ (Nguyen, 2013, 1098-1106).

Činjenica je da kiber napad najčešće pored direktnog cilja, podrazumeva i težnju za ostvarenjem indirektnog cilja. Odnosno svrha kiberterorizma nije samo napad na određeni server, brisanje ili modifikovanje koda na kojem sistem funkcioniše, ili izmena sačuvanih podataka. Krajnji cilj je indirektan i podrazumeva efekte koje taj napad proizvodi na sisteme ili uređaje koji su pod kontrolom mete/računara i način na koji taj napad utiče na donošenje ljudskih odluka pomoću plasiranih i obrađenih informacija od strane kiberterorista. Generalno, svaki kiberteroristički napad proizvodi indirektne efekte kojima njihovi počinioci teže.

Nakon izvođenja kiberterorističkog napada lančano se stvaraju efekati koji mogu u mnogo toga da podsećaju na oružani napad, toliko da mogu da izazovu čak i smrtni ishod. Međutim, kiber napadi se značajno razlikuju od tradicionalnih vojnih napada. Kiber napadi podrazumevaju sofisticiraniju upotrebu oruđa/alata i oružja (IT tehnologije, kompjuterski sistemi). Za izvođenje tradicionalnog vojnog napada upotrebljava se oružje koje izaziva direktnu fizičku štetu, pa samim time postoji mogućnost od povređivanja po samog izvršioca, odnosno napadača. Dok se kiber napad može izvesti „iz fotelje“ daleko od ciljane mete napada prostorno i vremenski i ne predstavlja realnu fizičku opasnost od povređivanja po samog počinioca. Dok je potencijalna veličina štete takva da je samo jedan zlonamerni upadni kod dovoljan da se pričinjena šteta automatski replicira i brzo inficira druge sisteme i izbriše čitav set informacija u računaru. Dakle, kiberterorizam karakteriše velika neizvesnost posledica, potencijalno širok opseg prekida rada operativnih sistema i oštećenja, kao i visok rizik od kolateralne štete. Kao primer može da posluži Safir crv (*Sapphire worm*) koji je onemogućio rad servera u Južnoj Koreji i na međunarodnom nivou stvorio probleme tako što je ometao rad internet usluga u Tajlandu, Japanu, Filipinima, Maleziji, Indiji, diskonektovao hitan 911 servis i izazvao probleme u radu 13.000 bankomata u US (Schneier, 2003) i doprineo odlaganju kanadskih nacionalnih izbora i avio letova (Shielding, 2003). Na isti način je moguće kiber napad usmeriti na vojne resurse, te on lako može da preraste u napad na civile.

Kao „*četiri glavna cilja kiber napada koje sprovode teroristi nameću se: onemogućavanje neprijateljskih operativnih sposobnosti, uništavanje reputacije ili pogrešno predstavljanje određene organizacije, nacije ili saveza; ubeđivanje napadnutih da promene svoju pripadnost i da demonstriraju svojim sledbenicima da su sposobni da pričine značajnu štetu svojim metama*“ (Warren, 2002).

Najčešći cilj kiberterorista je onemogućavanje operativnih sposobnosti neprijatelja. Otuda kiberteroristi primenjuju one vrste kiber napada koje ozbiljno mogu da oštete ili unište funkcionisanje neprijatelja/mete i pričine značajnu štetu celoj naciji ili izazovu ekonomski kolaps ili društvena krizu. U savremenom društvu marketing i reputacija predstavljaju vitalne elemente na kojima savremene organizacije baziraju svoje aktivnosti. Otuda drugi najčešči cilj kiberterorista podrazumeva nanošenje štete uništavanjem reputacije ili pogrešnim predstavljanjem određene organizacije, nacije ili saveza. Teroristi ovaj cilj najčešće postižu širenjem lažnih glasina putem elektronskih medija (*e-mail*, veb sajtovi i dr.). Zbog velikog značaja koji mediji imaju u svakodnevnom životu, teroristi hakuju elektronske medije kako bi preneli sliku o izvedenim napadima, svojim ciljevima i motivima širom sveta i time pokazali svojim sledbenicima i široj javnosti da su sposobni da pričine značajnu štetu svojim metama, da predstavljaju ozbiljnu pretnju i šire strah. Iako se teško realizuje, nekada dela kiberterorizma imaju za cilj da naruše postojeće partnerske veze i saveze, i privole napadnute da promene „*stranu*“ kojoj su do tada bili lojalni. Šinder smatra da su najčešći akti računarskog terorizma:

„a) *elektronska komunikacija kako bi se sprovele određene terorističke aktivnosti ili regrutovali novi članovi terorističke organizacije;*

b) sabotaža vazdušnog saobraćaja, kako bi se izazvala avionska nesreća ili sabotaža elektronskih prečišćivača vode kako bi izazvali zagađenje pijaće vode;

c) upadi u bolničke i zdravstvene sisteme, kako bi se izbrisala ili promenila baza podataka pacijenata i propisane metode lečenja ili napadi na infrastrukturu za napajanje, što može izazvati smrt velikog broja ljudi koji su na respiratorima itd.“ (Shinder, 2002, 19). Vajman smatra da su efekti kiberterorizma najštetniji primenom napada na „*bot mreže*“ *i* „*SCADA sisteme*“ (Weimann, 2015, 157).

„*Botneti ili bot mreže*“ sastoje se od velikog broja kompromitovanih računara koji su zaraženi zlonamernim kodom i mogu se daljinski kontrolisati pomoću komandi poslatih putem interneta. Stotine ili hiljade ovih zaraženih računara rade udruženo kako bi ometali ili blokirali

internet saobraćaj ciljanih žrtava. *Botnet* se može koristiti u *DDoS* napadima, *proksi* i *spam* uslugama, za distribuciji *malvera* i druge organizovane kriminalne terorističke aktivnosti. *Botneti* se takođe mogu koristiti za: sakupljanje tajnih podataka ili za napade na ključnu infrastrukturu koja veliki deo svog rada bazira na internetu, kao oružje u propagandnim ili psihološkim kampanjama sa ciljem da se izazove strah, zastrašivanje ili javna sramota. *Botneti* nesumnjivo postaju glavna pretnja i oružje budućih kiberterorista, uglavnom jer mogu da se dizajniraju tako da poremete rad ciljanih računarskih sistema na različite i za teroriste delotvorne načine, i mogu čak da ih iznajme za svoje potrebe, ukoliko teroristi ne poseduju dovoljno tehničkih veština za njihovo dizajniranje (Weimann, 2015, 156).

„*SCADA - Supervisory control and data acquisition sistemi*“ (supervizorska kontrola i prikupljanje podataka) je vrsta računarskog sistema koji prati i kontroliše funkcionisanje ključnih sistema (kritične infrastrukture privatne i javne). Ovi sistemi primenom različitih alata, kao što su: programski logički kontrolori, daljinske terminalne jedinice i drugi uređaji za praćenje i automatizaciju kontrolišu: „*prečišćavanje i distribuciju vode, sakupljanje i tretman otpadnih voda, rad naftovoda i gasovoda, prenos i distribuciju električne energije, vetroelektrane, sisteme civilne odbrane, rad sirena, praćenje i kontrolu sistema grejanja, ventilacije i klimatizacije, potrošnje energije u zgradama, aerodromima, brodovima i svemirskim stanicama*“ (Weimann, 2015, 157). SCADA sistemi postoje od 1960-te, međutim nisu bili dobro umreženi. Eksponencijalni rast mreža informacionih sistema koji međusobno povezuju poslovne, administrativne i operativne sisteme, doprineo je da pristup SCADA sistemu bude najatraktivniji cilj kiberteroristima, obzirom da bi bila kakva izmena podataka koji se koriste za operativne odluke ili rad ovih programa imala katastrofalne posledice.

Kada govorimo o klasifikaciji posledica terorizma, Milašinović primećuje: „*Na unutrašnjem planu države, efekti terorizma su izuzetno složeni, latentni i neretko predstavljaju strategijski rizik po bezbednost države i građana usled:*

1. ugrožavanja života ljudi, odnosno njihovog povređivanja i smrti kao posledica terorističkih napada;

2. ugrožavanja zdravstvene bezbednosti ljudi;

3. ugrožavanja životne sredine, biljnog i životinjskog sveta;

4. destabilizacije ekonomije i ekonomskog investiranja;

5. ugrožavanja energetske bezbednosti zemlje;

6. ugrožavanja socijalne bezbednosti;

7. ugrožavanja finansijske stabilnosti države;

8. demografske destabilizacije države;

9. povećanja nacionalnog i verskog nacionalizma i tenzija;

10. ekspanzije tzv. medijskog kriminala;

11. umrežavanja terorizma i drugih vidova kriminala, od kojih je svakako najopasnija sprega sa organizovanim kriminalom i sa kriminalnim (subverzivnim) aktivnostima obaveštajnih službi neprijateljski nastrojenih država;

12. povećanja korupcije u javnom sektoru;

13. ugrožavanja funkcionalnosti pojedinih državnih resora;

14. stvaranja nepoverenja građana u državu i državne organe;

15. stvaranja nepoverenja građana i države u međunarodne organe i institucije;

16. urušavanja međunarodnih odnosa i imidža (ugleda) zemlje na međunarodnoj sceni" (Milašinović, 2011, 9-10).

Bez obzira da li je kiberteroristički akt doveo do gubitaka ljudskih života, ili samo do ekonomskih gubitaka, psihološke posledice koje dela ove vrste imaju po žrtve i širu javnost nisu zanemarljive. Generalno, terorizam je često koncipiran kao oblik psihološkog rata. Svrha svakog terorističkog napada, pa i kiber napada je da uzdrma i uznemiri javost. Direktne mete nasilja, nisu glavni ciljevi terorističkog delovanja, već one služe uglavnom kao generatori poruka. „*Komunikacija između terorista (organizacije), žrtava (ugroženih) i glavnih ciljeva (publika (e)) zasnovana na pretnjama i nasilju koristi se za manipulaciju glavnim ciljem, pretvarajući ih u cilj terora, cilj zahteva ili cilj pažnje, u zavisnosti od toga da li se prvenstveno teži zastrašivanju, prinudi ili propagandi*" (Schmid & Jongman, 2005, 28). Takođe, „*kiberterorizam se uklapa u ciljeve terorista tako što uliva strah u živote neprijatelja. Kiberterorizam može da se dogodi bez ikakvog upozorenja, a nema mnogo toga što obični civili mogu da učine da bi se zaštitili od takvih napada. Ova neizvesnost i nepostojanje kontrole nad sopstvenim svetom omogućavaju da svet vidi ovakav oblik terorizma kao užasavajuću opciju*" (Weimann, 2015, 153).

2.7. Kiberprostor

Kiberterorizam objedinjuje u sebi virtuelni kiberprostor i terorističku aktivnost. Da bi se bolje razumeo kiberterorizam, neophodno je prvo da razumemo virtuelni prostor sa svim njegovim mogućnostima. Intenzivna dinamika tehnološkog razvoja, naročito od devedesetih godina dovela je do sve veće dostupnosti računara širom sveta i porasta broja korisnika. U literaturi je u upotrebi termin kiberprostor ili njegovi sinonimi: kibernetski prostor, sajber prostor (*cyberspace*), virtuelni svet, virtuelni prostor, digitalni svet. Inače, pojam kiber (*cyber*), potiče od grče reči *kybernetes* što znači onaj koji vlada, upravlja.

Kiberprostor je sve značajniji deo infrastrukture savremenih razvijenih zemalja i obuhvata skoro sve sektore koji su značajni za funkcionisanje savremenog društva, što je uslovilo povećane rizike i sve veću potrebu za dostizanjem njegove bezbednosti. Otuda su ključna pitanja savremene bezbednosti pitanja kibernetskog prostora i njegove kiber odbrane.

Posmatrano sa semantičkog aspekta, preuzimanje i uvođenje stranih izraza iz oblasti informaciono-komunikacionih tehnologija u srpski jezik dodatno otežava tumačenje, analizu i klasifikaciju ovog fenomena. Kiberprostor koegzistira kao zasebna celina unutar realnog sveta i poseduje svoja pravila, institucije, znanje i društvenu praksu. Za njegovo funkcionisanje neophodno je mrežno povezivanje računarskih sistema - *intranet, LAN, WAN* i dr. Stoga nije teško zaključiti da kiberprostor nije isto što i internet, odnosno on predstavlja širi pojam od interneta. Internet podrazumeva fizičku dimenziju, odnosno tehnološka sredstva koja su povezana tako da čine funkcionalnu infrastrukturu, dakle sačinjen je od fizički opipljivih elemenata. Dok, kibernetski prostor predstavlja složeniju pojavu i podrazumeva kako fizičku infrastrukturu, čiji je sadržaj lako uočljiv, kao što je softver i ljudsku aktivnost koja čini internet, *World Wide Web* mogućim, odnosno i ne-fizičku dimenziju. Dakle, to je nematerijalni (*online*) prostor koji nastaje upotrebom digitalne tehnologije pomoću koje se obavlja online komunikacija, u „*svetu za sebe*“, koji je fundamentalno odvojen od realnog (stvarnog) sveta, koji egzistira u „*offline modu*”. Mnogi autori, među njima i Vajnstok (Weinstock, 2000) ukazuju da ovaj vid komunikacije sve više postaje deo „*offline*” sveta. Međutim, pomenuta digitalna komunikacija se značajno razlikuje od „*offline*” komunikacije.

Izraz „*cyberspace*“ pojavio se prvi put u SAD. Američko ministarstvo odbrane (2012) ga definiše kao: „*globalno područje u okviru informacionog okruženja koje je sačinjeno od međuzavisne mreže infrastrukture informacionih tehnologija, uključujući internet, telekomunikacione mreže, računarske sisteme i ugrađene procesore i kontrolere*“ (Scaparrotti, 2014, II9, 5a). U Rečniku kompjuterskih termina navedeno je da kibernetski prostor „*predstavlja okruženje virtuelne realnosti u kome osobe komuniciraju pomoću povezanih računara*“ (Tasić & Bauer, 2003, 125). U „*Strategiji za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine*“ je navedeno da se „*pod „sajber prostorom” podrazumeva ili vrsta „zajednice” sačinjene od mreže računara u kojoj se elementi tradicionalnog društva nalaze u obliku bajtova i bitova*“ ili „*prostor koji kreiraju kompjuterske mreže*” (Službeni glasnik br. 71/18). Dakle, to je virtelni prostor koji je sačinjen od isprepletanih računarskih mreža iz celog sveta kojima se povezuju krajnji korisnici i time omogućava njihova nesmetana komunikacija bilo putem audio, video, glasovnih, e-mail ili šifrovanih poruka. To je „*nova forma mentalne dimenzije ljudske egzistencije unutar koje nastaje simulirana realnost kao posledica interakcije između ljudskog i artificijelnog interfejsa. Predstavlja alternativnu prostornu dimenziju unutar koje se uspostavlja veza između različitih personalnih računara, računarskih mreža, različitih virtuelnih zajednica i pojedinaca*“ (Mimica & Bogdanović, 2007, 60).

Kiberprostor je kompleksan fenomen koji podrazumeva veliki broj korisnika, ali i širok dijapazon aktivnosti kako ofanzivnih, tako i defanzivnih kao što su na primer: manipulacija protivnikom ili njegovim potencijalnim odlukama, ciljanje na određeni informacioni medijum (na primer bežičnu pristupnu tačku), prenošenje neke poruke (šifrovana poruka u informacionoj dimenziji), stvaranje kiber-persona (onlajn identitet koji olakšava komunikaciju, odlučivanje i uticanje na javnost u kognitivnoj dimenziji) i dr. Mnoge mreže su dizajnirane sa specifičnom svrhom, te su kao takve u određenoj meri izolovane od interneta koji predstavlja samo jedan deo kibernetskog prostora.

Različiti akteri deluju unutar kibernetskog prostora. Dogan navodi dve grupe aktera: „*timove mamaca (troll army) - sponzorisani su od strane države, poseduju lažne identitete koje koriste kao učesnici u blogovima, internet forumima i na društvenim mrežama u cilju propagande, kreiranja percepcije javnog mnjenja, podrivanja disidentskih struktura i slično; timovi za kreiranje grupnog mišljenja (swarm stream teams) - ciljno orijentisana grupa ljudi*

koja se služi kiber prostorom da agresivno širi viralne (virusne) video sadržaje kojima razbijaju poruke protivnika ili određenih medija“ (Duggan, 2015, 14).

Strukturalno posmatrano, kibernetski prostor čine tri sloja. Prvi je fizički vidljiv i opipljiv deo, koji čine njegova infrastruktura, mrežni i prenosni uređaji podrške. Drugi deo je softverski i odnosi se na deo koji su ljudi načinili kao programski sistem podrške i instrukcija kako bi kibernetski prostor funkcionisao. Treći sloj su informacije koje nastaju kao rezultat interakcije prva dva dela, odnosno tehničke podrške i ljudske intervencije - mašina i ljudskih programa, instrukcija kojima se podaci obrađuju i kreiraju u informacije koje se potom prenose brzo i efikasno dalje bez obzira na geografsku udaljenost.

Teroristi se služe „*online*“ platformama u različite svrhe:

„*1) psihološki rat;*

2) propaganda;

3) online indoktrinacija;

4) regrutacija i mobilizacija;

5) pretraživanje podataka;

6) virtualna obuka;

7) planiranje i koordinacija , i

8) prikupljanje sredstava“ (Weimann, 2015, 24).

3. SAVREMEN DRUŠTVENO-POLITIČKI KONTEKST

Savremen društveno – politički kontekst počiva na principima globalizacije. Globalizacija je dovela do raspada ranijih formi društava koje su bile državno orjentisane. Mnogi autori primat daju ekonomskim aspektima globalizacije i smatraju da su ostali aspekti jedino njihov nus-efekat ili da su u službi ekonomske globalizacije. Ključne ekonomske promene koje je iznedrila globalizacija su: davanje prevlasti slobodnom tržištu i ograničavanje uloge države na neophodan minimum, liberalizacija trgovinskih tokova, međunarodna mobilnost kapitala, radne snage, informacija, tehnologije i ideja i dr. Naučno-tehnološki razvoj i inovacije u oblasti informaciono-komunikacionih tehnologija (ICT) omogućili su globalno umrežavanje, laku dostupnost i brzu razmenu informacija bez obzira na realnu prostornu udaljenost. S kulturološkog aspekta globalizacija je uvela pluralističke vrednosti i otvorenost prema stranim kulturnim sadržajima, međutim „*pluralitet dovodi do kritičnih tenzija*“ (Smelser, 2003: 108).

Tranzicija nerazvijenih zemalja uglavnom postsocijalističkih se ostvaruje dobrovoljnim zaduživanjem kod međunarodnih fondova (MMF, Svetska banka i dr.), što dovodi do osiromašenja naroda i omogućava strogu kontrolu država dužnika. U navedenim uslovima društva u tranziciji se orjentišu na ostvarenje profita, što dalje uzrokuje procvat sive ekonomije, korupcije, organizovanog kriminala i nelegalnog kapitala. Postojeća situacija se prelama sa makro na mikro nivo i dovodi do „*korodiranja karaktera*“ (Sennett, 1998) usled opadanja poverenja, lojalnosti, radne etike i posvećenosti.

Umrežavanje društva omogućilo je brz prenos informacija širom sveta (Castells, 2000), toliko da je „*posredi produbljivanje i ubrzavanje svetske međuzavisnosti u svim društvenim aspektima*“ (Held, 2003, 48). Informacione tehnologije predstavljaju najznačajnija sredstva informisanja, time što pružaju brojne mogućnosti za izražavanje stavova različite vrste - promovisanje ideja, apela, nezadovoljstva postojećim sistemima moći, političkih ideja i dr. Naš savremeni zapadni svet je umotan slikama, znacima i simbolima (Miller et al., 2008). Tehnološki razvoj nije doneo promene samo u načinu informisanja, nego je znatno izmenio funkcionisanje celokupnog društva, njegovih ključnih nacionalnih i međunarodnih struktura i izmenio je način poslovanja i življenja. Primenu savremenih telekomunikacija u sistemu poslovanja najbolje ilustruje rad od kuće koji „*omogućava pojedincu manje vremena provedenog na putovanja i više vremena za porodicu, a poslodavcu veću produktivnost, manje troškove zbog uštede prostora*“ (Baruch, 2000, 38).

Zbog široke upotrebe koje savremene informacione tehnologije imaju (odašilju poruke širokom auditorijumu, proizvode efekte najširih razmera) potrebno je da informaciono-komunikacione tehnologije budu predmet razmatranja različitih nauka kako bi se mogućnosti za njihove različite zloupotrebe svele na minimum i postigle što efikasnije prakse i regulacije.

3.1. Globalizacija

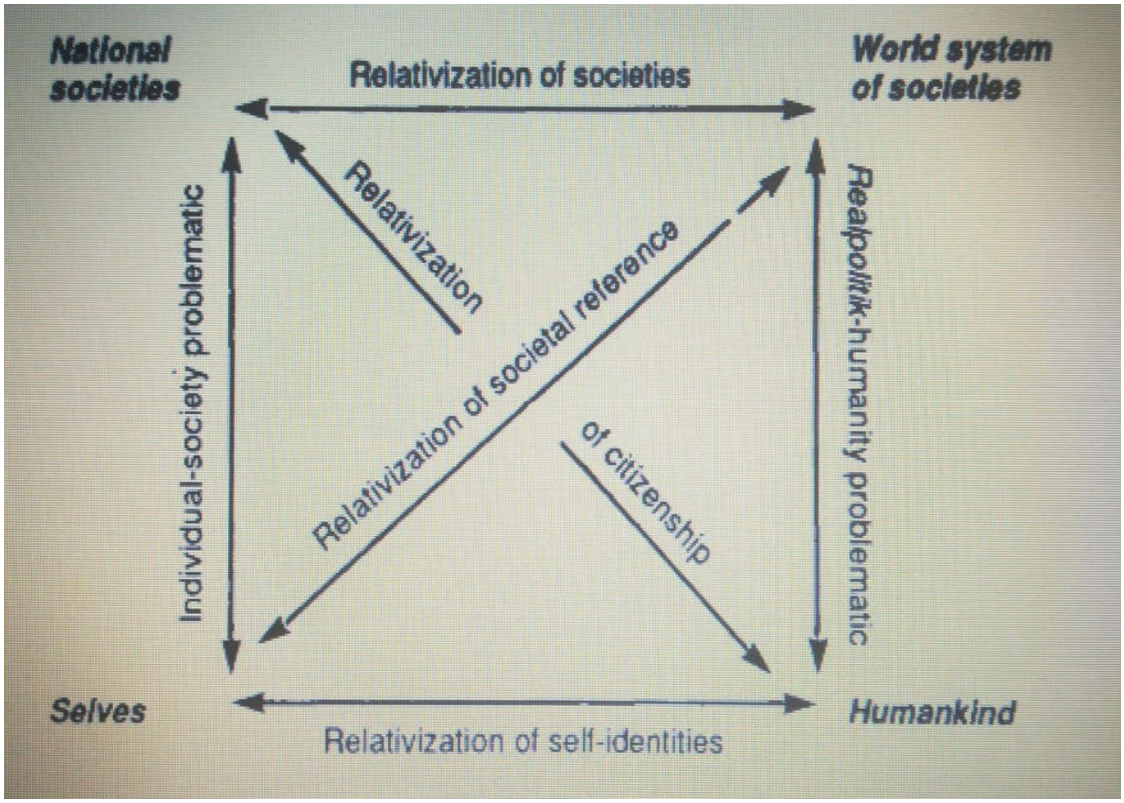
Termin globalizacija je aktuelan termin koji je široko razmatran u brojnim raspravama savremenih mislilaca. Šta globalizacija zapravo znači? Poznato je da globalizacija zahvata savremeno društvo u celosti, kao i sve njegove sisteme (društveni, politički, ekonomski, kulturni i dr.). Upravo zbog svoje složenosti, dinamičnosti i sveobuhvatnosti, ovaj fenomen nije lako definisati.

U savremenoj literaturi postoji nekoliko različitih načina definisanja i izučavanja globalizacije:

1. u zavisnosti od teorijskog pristupa razlikujemo skeptike, hiperglobaliste i transformacioniste (Held, 2003; Bauman, 1998). Prvi pravac razmišljanja čine *skeptici*, koji sumnjaju u postojanje celokupnog procesa i vide „*globalizaciju kao mit*“ (Volerstin, 2003), ili ne poriču njeno postojanje, ali smatraju da je mit to da ovaj proces nema alternativu i predstavlja „*novi vid svetske dominacije*“ (Burdije, 1999, 39). Tako neki autori definišu globalizaciju kao da ona „*nije ništa drugo do 'rekolonizacija' u novom ruhu*“ (Neeraj, 2001, 6-7). Drugi pristup razmišljanja čine hiperglobalisti koji naglašavaju efekte globalizacije u svim društvenim sferama (bilo pozitivne bilo negativne). Otuda globalizaciju vide kao:„*integraciju svetske ekonomije*” (Gilpin, 2001, 364), „*razvoj globalnih finansijskih tržišta, rast transnacionalnih korporacija i njihova sve veća dominacija nad nacionalnim ekonomijama*“ (Soros, 2003, 13). Treći pristup čine autori koji se pojmom globalizacije služe da objasne transformaciju društvenih promena krajem XX i početkom XXI veka – transformacionalisti. Za njih je karakteristično to što globalizaciju vide kao „*istorijsku transformaciju*“ (Albrow, 1996, 88) koja je dovela do promena „*u do sada neviđenom stepenu*“ (Freidman, 1999, 7) i do te mere intenzivirala društvene odnose širom sveta „*na način da se lokalni događaji uobličuju na osnovu događaja koji se dešavaju miljama daleko i obratno*“ (Giddens 1990, 21); u ekonomiji uticala na „*način sticanja prihoda i egzistencije*“ i omogućila „*širenje slobodnog tržišta kapitalizma do svake zemlje na svetu*“ (Freidman, 1999, 8); „*u politici gubitak stepena lokalne kontrole, a u kulturi gubitak dostignuća kolektiviteta*“ (Mittelman, 2000, 6).

2. u zavisnosti od nivoa analize možemo da razlikujemo makroglobalizaciju, mezoglobalizaciju i mikroglobalizaciju, odnosno glokalizaciju. Jer, „*nisu samo društva koja zaostaju, nego su sva društva uključena u proces „modernizacije“ koji se tiče praktično svih*“ (Robertson, 2001, 12).

Slika 3. Globalno polje (Robertson, 2001, 27)



3. Kao što primećuje Jejts (Yeates, 2001) među savremenim misliocima postoje dijametralno suprotna mišljenja o fenomenu globalizacije. Otuda podela na pobornike (globalofoličare) i kritičare globalizacije (antiglobaliste = globalofobičare i alterglobaliste). Pristalice globalizacije navode njene prednosti i smatraju je rešenjem za mnoge socijalne probleme. Ukazuju da globalizacija stvara sloj vrhunskih menadžera i naučne elite, državnih funkcionera i političko-vojne elite, dok smanjenje inflacije i ubrzani tehnološki napredak dovode do rasta produktivnosti i BDP-a (Derdorff & Stern, 2001). Kritičari se pozivaju na nedostatke kao što su: „*globalno uništavanje životne sredine, ekspanzivno osvajanje manje razvijenih nacija zapadnim socio-kulturnim modelima i sve jači socio-ekonomski pritisci da se prilagodi kompeticiji na svetskom nivou*“ (Hengsbach, 1997, 182-195). Oni globalizaciju smatraju glavnim

uzrokom brojnih socijalnih problema kao što su: siromaštvo (Katz, 2004), rastući jaz između onih koji imaju i onih koji nemaju (Gidens, 2003, 598-599; Žoa i Šuler, 2005, 256-259), nezaposlenost (Carter, Schwartz, Norris, 2008), migracije (Silvey, 2009), prenaseljenost gradova usled masovnog napuštanja sela, upotreba droge, razaranje porodice (Milić, 2001), organizovani kriminal, trgovina ljudima i dr.

4. Različiti autori nude različite modele globalizacije. Tako Džon Grej i Emanuel Tod razlikuju dva modela globalizacije: asimetrični - ovaj model globalizacije je antagonistički i neoimperijalni (Gray, 1998) i asocijativni - ovaj model je neantagonistički, socijaldemokratski (Todd, 2003). Lesli Skler takođe govori o dva modela globalizacije: kapitalističkom i socijalističkom (Sklair, 2013).

Možemo reći da je globalni poredak isprepletan sistem moći. Autori nude različite definicije globalizacije u zavisnosti od toga šta im je u fokusu. Odnosno, u zavisnosti od toga da li se globalizacija poima kao proces - „*Nezadrživ i nepovratan proces integracije kultura, tržišta i državnih zajednica, koji je dostigao nezabeležen nivo*“ (Vuletić, 2006, 11) ili projekat uticajnih grupa koje žele da uspostave svetsku dominaciju i dalje širenje kapitalizma kroz ekonomsku liberalizaciju i političku deregulaciju. Lesli Skler predlaže „*globalno sistemsku teoriju*“ (Sklair, 2001) i pridaje veliki značaj inovacijama iz druge polovine XX veka (tehnološke, ekonomske, političke, kulturno-ideološke).

3.2. Posledice globalizacije koje pogoduju širenju kiberterorizma – makro nivo

Gidens ukazuje da „*dinamika savremenog društva po svojoj širini i snazi preobražaja ipak prevazilazi sve ranije dinamike*“ (Giddens, 1998, 16; Giddens, 2005, 25, 32 i dr.). Dok ga brzina kojom se odvijaju savremene promene podseća na „*vožnju kočijama koje vuče zmaj u kasu*“ (Gidens, 1998, 58).

Globalizacija je nesumnjivo olakšala način življenja, ali ne za sve svetske zemlje i njihove stanovnike podjednako. Pojedinci ili društvene grupe susreću se sa različitim poblemima koji onemogućavaju, otežavaju ili ugrožavaju njihove mogućnosti da ostvare svoja prava ili zadovolje fundamentalne ljudske potrebe.

Jedan od njih je siromaštvo. Svetska banka, Međunarodni monetarni fond, Svetska trgovinska organizacija i druge globalne institucije nameću svoju moć tako što nude finansijsku pomoć u vidu kredita zemljama koje su u razvoju. Međutim, u praksi je potvrđeno da su na taj način mnoge domaće ekonomije upale u „*dužničko ropstvo*“. Jer, nisu svi principi primenljivi na istovetan način kod različitih nacionalnih ekonomija. Otuda, Soros ukazuje da MMF „*ne raspolaže metodologijom za razlikovanje između zdravih i nezdravih ekonomskih politika*” (Soros, 2003, 89). Dalje, delom ili u celosti demokratski principi se ne primenjuju i ne poštuju u praksi. Bogati imaju različite mogućnosti da se izbore za politike koje im odgovaraju bilo lobiranjem ili korupcijom i na taj način očuvaju ili povećaju postojeće stanje nejednakosti (Li, Squire, Zou, 1998).

Multikulturalnost i tolerancija se promovišu kao globalne vrednosti, međutim javno ispoljavanje etničkih, verskih i rasnih obeležja nije poželjno i neretko nailazi na političku osudu kao rasizam ili neki drugi vid diskriminacije. „*Tehnološke inovacije stvorile su mogućnosti za kiber konflikte i revolucionarne borbe; pojava dronova- bespilotnih letelica, istovremeno razvija mogućnosti nadzora, dok u nekim slučajevima onemogućava ili ugrožava mogućnosti za otvorene sukobe u obliku protesta i neslaganja*“ (Wagner-Pacifici & Hall, 2012, 195).

Savremeni kapitalisti širom sveta pojedine sektore proizvodnje izmeštaju u druge zone svetske ekonomije koje su isplativije zbog jeftine radne snage i drugih uslova poslovanja. Na taj način migranti iz ruralnih predela po prvi put ulaze na tržište rada i obavljaju poslove koji im pružaju povoljnije uslove i višu zaradu od pređašnje koju su primali

za poljoprivredne poslove. Dok su usled „*ubrzane deruralizacije*“ (Volerstin, 2003, 105) istovremeno socijalno isključeni i nesposobni da odbrane svoje interese.

Globalizacijske promene prelamaju se i na klasnu strukturu, koja se takođe transformiše (Gorc, 1982, Basan et al, 2005, 230). Otuda se „*konflikti između društvenih grupa menjaju, sve češće gube klasni karakter i fokusiraju se na identitete druge vrste, poput religijskih*“ (Hantington, 2000). Kriza države blagostanja, kao i kriza političkih, ekonomskih i socijalnih institucija stvaraju nezadovoljstvo i nesigurnost. Otuda, Sasen smatra da su globalni kapital i nova iseljenička radna snaga dva glavna suprostavljena aktera u globalizacijskim procesima (Sasen, 2005, 197).

Nesumnjivo je „*savremeno društvo prevashodno rizično*“ (Bek, 2001, 29). Postojeća društvena situacija na makro nivou zbog brojnih problema može da izazove odbojnost prema kapitalističkom razvoju, nacional-šovinizam ili verski fanatizam, separatističke težnje, što uz laku dostupnost tehnoloških inovacija čini kiberterorizam aktuelnim oblikom terorizma.

3.2.1. Tehnološka revolucija i umrežavanje društva

Jedna od najznačajnijih promena koje su se dogodile tokom XX-tog veka je razvoj informacione tehnologije i njena široka primena u gotovo svim segmentima društva. Društvo se transformisalo iz industrijskog u informaciono tako da primarni resursi postaju znanje i informacije, a ne kao u prethodnim društvima materija i energija. Tehnološke tvorevine kao što su: računari, računarske mreže, internet, *Twitter*, *Facebook, YouTube,* pametni telefoni i ostalo, prihvaćeni su velikom brzinom toliko da predstavljaju neizostavni deo svakodnevnice bez čije primene su poslovanje i privatni život gotovo nezamislivi.

Iako je društvo globalizovano, nisu svi svetski regioni podjednako uključeni u informacionu revoluciju zbog razlika kao što su: stepen razvoja, ekonomska stabilnost, tehnološke mogućnosti i dr. Iako tehnologija nije još uvek u potpunosti zahvatila sve aspekte čovekovog življenja, neupitno je da ona oblikuje život savremenog pojedinca.

Savremeno društvo predstavlja „*sistem mreža znanja i informacija*“ (Castells, 2000). Opšte je poznato da su mreže otvoreni sistemi, koje karakteriše fluidnost, promenljivost, dinamičnost, kao i velika mogućnost razvoja. Tehnološki progres omogućio je da komunikacija bude multidimenzionalna i da se odvija u različitim pravcima prostorno i vremenski neograničeno. Ovo podrazumeva da društva nisu više vezana za svoj geografski položaj, državu ili naciju, već jednostavno postoje u kibernetski prostoru kroz sisteme komunikacija.

Internet značajno otvara vrata alternativnim sadržajima i nudi mogućnosti za mobilizaciju i osnaživanje društveno isključenih i manje privilegovanih pojedinaca i grupa. Zbog složenosti i dvosmislenosti novih tehnologija pravno-ekonomske, društvene i bezbednosne nauke su pred velikim izazovom. Sasen ukazuje da je nužno da kibernetski prostor pojmimo kao „*daleko konkretniji prostor za društvene borbe od nacionalno političkog sistema*“, navodeći dalje kako bi to moglo da „*olakša pojavu novih tipova političkih subjekata, koji postoje izvan formalnog političkog sistema*“ (Sassen, 2002, 382). Jer, savremene tehnologije olakšavaju pristup pojedincu da pretraži i lako pronađe društvenu grupu, politički subjekt ili pokret koji je u skladu sa njegovim interesovanjima i stavovima, nezavisno od lokalnih raspoloživih sadržaja. Na taj način su „*nove tehnologije poboljšale komunikaciju i poverenje u društvene pokrete i mobilizaciju članova*“ (Della Porta, 2012, 49).

Dakle, kiberaktivizam predstavlja novu vrstu aktivizma koji podrazumeva upotrebu novih tehnologija za podsticanje rasprava na one teme koje su politički diskutabilne i problematične, jer nailaze na otpor u realnom svetu. Žene su se vremenom sve više služile internetom u političke svrhe, da prikažu kontradikcije između „*muških*“ i „*ženskih*“ poslova, eksploatacione radne uslove kako bi na taj način povećale mogućnosti za svoje oslobađanje i emancipaciju od rodnog ugnjetavanja (Khamis, 2015; Everett, 2004; Schuster, 2013).

Zbog velikog dijapazona mogućnosti koje pružaju, savremene IT tehnologije, postale su značajno sredstvo za vršenje kriminalnih dela i njihovo međusobno organizovanje. Veza između terorizma i interneta je višestruka. Savremeni teroristi se uglavnom služe internetom da ostvare međusobnu komunikaciju i promovišu svoje ideje ili pošalju poruke mržnje i pošalju sliku učinjenih dela nasilja kod što većeg broja ljudi. Upotrebu interneta od strane terorista možemo podeliti u dve kategorije:

1) „*komunikativna upotreba interneta – podrazumeva širenje propagande, kampanje psihološkog ratovanja, internu komunikaciju i radikalizovanje regruta širenjem poruka mržnje;*

2) instrumentalna upotreba interneta - podrazumeva online edukacije terorista, „virtuelne kampove“ za obuku budućih napadača“ (Weimann, 2015, 24).

Dakle, ni počinioci međunarodnog kriminala (terorizam ili organizovani kriminal), takođe nisu ostali imuni na primenu savremenih informacionih tehnologija (IT). Nekadašnje kriminalne organizacije su bile strogo hijerarhijski uređene. Informaciona revolucija iznedrila je nove forme organizovanog kriminala i terorističke organizacije koje su fleksibilne, mrežne strukture sa nekoliko centara moći i karakteriše ih velika mobilnost članova. Na taj način pojedine kriminalne aktivnosti dobijaju globalne razmere (Selley, 2003).

Opšte gledano informaciona tehnologija je jedan od najzačajnijih elemenata koji na makro nivou oblikuju društvene tokove zbog:

- raznolike primene u gotovo u svim sferama društvenog postojanja
- uticaja koji trenutno vrši
- budućih promena koje će njena upotreba neminovno iznedriti
- eventualnih izazova i problema izazvanih njenom primenom.

Dakle, veoma je važno bavljenje ovom problematikom iz različitih uglova - politikološkog, sociološkog, ekonomskog, kulturološkog, pravnog i bezbednosnog.

Jer, dinamika razvoja informacionih tehnologija, sve veći broj visoko kvalifikovanih stručnjaka iz ove oblasti, relativno niski troškovi i brojne mogućnosti za izvršenje kiber napada, nesumnjivo ukazuju da su veliki izgledi da će kiberterorizam da postane popularnija pretnja u budućnosti. Jedino dobro poznavanje i razumevanje savremene situacije može da dovede do adekvatnog reagovanja nadležnih organa i pravnog sistema, efikasnog otkrivanja i dokazivanje krivičnih dela koja spadaju u ovaj oblik kriminaliteta.

3.2.2. Jaz između bogatih i siromašnih

Brojna istraživanja (Dollar & Kraay, 2001; Ferreira, 1999) su potvrdila da globalizacija smanjuje siromaštvo i da je u pozitivnoj sprezi s rastom. Međutim, neka istraživanja navode da je to smanjenje siromaštva vrlo skromno u odnosu na ostvarene stope rasta (Vandemoortele, 2002).

Tabela 5. Prosečna godišnja stopa rasta u periodu 1987-2013. godine (Piketty, 2015, 467)

bogatstvo najbogatijih	6,8 %
svetski bruto društveni proizvod	3,3 %
prosečno bogatstvo odraslih stanovnika sveta	2,1 %
prosečni prihodi odraslih stanovnika sveta	1,4 %

Nužno je tumačiti svaki dohodak zasebno, odnosno udeo koji ostvaruju siromašni, pripadnici srednjeg sloja i bogati u ukupnom dohotku. Iako, generalno globalizacija donosi korist, ona šteti najugroženijima i najsiromašnijima (Lundberg & Squire, 2000).

Tabela 6. Ukupna nejednakost dohodaka u vremenu i prostoru (Piketty, 2015, 264)

	mala nejednakost (u Skandinaviji 70-80.)	umerena (Evropa 2010)	velika (Evropa 1910, SAD 2010.)
1% najbogatijih	7	10	20
sledećih 9%	18	25	30
sledećih 40%	45	40	30
polovina društva koja je najsiromašnija	30	25	20

Jaz između bogatih i siromašnih može se tumačiti sa globalnog aspekta i na nivou jedne države. Objašnjenje i razumevanje savremenih ekonomskih tokova je gotovo nemoguće bez razumevanja principa libelarne ekonomije i multinacionalnih kompanija.

Multinacionalne kompanije su značajan društveni akter i uživaju veliku moć u savremenom društvu: 1. ekonomsku – imaju značajnu ulogu u svetskoj ekonomiji, 2. političku – njihovo rukovodstvo predstavlja deo vladajućih struktura „*elite vlasti*" uključujući i političku elitu, 3. kulturno-ideološku – imaju snažan uticaj na kulturu i širenje ideologije konzumerizma i dobru saradnju sa medijima i lobistima.

Kako bismo bolje razumeli funkcionisanje multinacionalnih kompanija neophodno je da poznajemo osnovne principe rada na kojima ove kompanije baziraju svoje poslovanje. „*Pravila korporacijskog ponašanja su: 1. imperativ profita, 2. imperativ rasta; 3. konkurencija i agresivnost; 4. amoralnost; 5. dehumanizacija; 6. hijerarhija; 7. brojivost, linearnost i segmentacija; 8. eksploatacija; 9. efemernost i pokretljivost; 10. nesklad sa prirodom; 11. homogenizacija*" (Mander, 2003, 315). Dakle, primarni ciljevi multinacionalnih kompanija su ostvarenje profita i rasta. Ovi ciljevi su „*iznad dobrobiti zajednice, zdravlja radnika, zdravlja stanovništva, mira, zaštite sredine ili državne bezbednosti*" (Mander, 2003, 316). Multinacionalne kompanije mogu lako da izmeštaju svoje poslovanje s jednog na drugo mesto, karakteriše ih velika prostorna i vremenska mobilnost, decentralizovanost što znatno olakšava eksploataciju ljudskih i prirodnih resursa. Zbog pomenute moći ove kompanije nanose štetu nacionalnim ekonomijama, uživaju brojne privilegije kao što su poreske olakšice, ugrožavaju državni suverenitet tako što kao globalni investitori diktiraju odgovarajuće uslove domaćim proizvođačima i vladi, ugrožavaju prava radnika i sindikalnu zaštitu i dr.

Nesumnjivo su multinacionalne kompanije važan globalni društveni akter, čiji rad potpomažu principi neoliberalne ekonomije. Otuda ove globalne institucije poseduju moć da investiraju po sopstvenom izboru i na taj način pospešuju globalnu nejednakost i siromaštvo, tako što ulažu u željene regione sveta, dok druge izbegavaju. Zemlje možemo da podelimo u tri kategorije: „*bogate zemlje, nosioce globalizacije i neglobalizovane zemlje*" (Dollar & Kraay, 2001). Moćne transnacionalne korporacije zbog svojih interesa najčešće biraju ekonomski slabe i nerazvijene zemlje, odnosno nacionalne ekonomije u kojima mogu da dominiraju i diktiraju uslove. Istovremeno s druge strane multinacionalne kompanije u potrazi za povoljnijim uslovima poslovanja, resursima i jeftinom radnom snagom prenose svoje poslovanje u zemlje periferije (otvaraju se nova radna mesta, obuke radnika i dr.). Međutim, to pogoduje postojećem poretku moći, obzirom da u praksi pravila poslovanja nisu ujednačena u razvijenim i nerazvijenim zemljama (neujednačena dnevna nadnica radnika, uslovi rada, prava radnika i dr.).

Na taj način se održava siromaštvo već siromašnih i još više produbljuje jaz između onih koji imaju moć i diktiraju uslove i onih koji tu moć nemaju. To potvrđuje i poznata „*teorija pređenog puta*“ (Mahoney, 2000).

Siromaštvo se najčešće poima kao materijalna deprivacija – lišenost, nedostatak ili uskraćenost novčanih sredstava za normalan život. Reč je o multidimenzionalnom fenomenu. Šta generalno znači biti siromašan? „*Za pojedince, porodice i skupine može se reći da su siromašni, ako im nedostaju resursi da bi nabavili hranu, učestvovali u aktivnostima i obezbedili životne uslove i potrepštine koje su uobičajene ili barem široko odobravane ili prihvaćene u društvu kojem pripadaju*” (Townsend, 1979, 31). Ono što je karakteristično za siromaštvo je subjektivni osećaj nezadovoljstva koji nastaje zbog diskrepancije između realnih potreba, očekivanja i stvarnih mogućnosti za njihovo realizovanje. Neki autori vide siromaštvo i isključenost kao sinonime (Abrahamson, 1995), dok drugi ističu razlike imeđu materijalne i socijalne deprivacije (Townsend, 1987). U literaturi siromaštvo se svodi na jednu dimenziju - finansijsku (materijalnu), dok je isključenost multidimenzionalna i pored nedostatka finansijskih sredstava podrazumeva i depriviranost u ostvarivanju prava i raznih životnih mogućnosti kao što su: stanovanje, obrazovanje, političko odlučivanje, socijalne veze, zaposlenje i dr.

Globalizacija uopšteno uz globalnu ekonomsku krizu suzila je mogućnosti nacionalnih ekonomija da joj se odupru. Takva situacija proizvodi negativne posledice kao što su: smanjenje izvoza, pad produktivnosti, nesigurnost radnog mesta, nezaposlenost, smanjenje dohodka i penzija i druge probleme. Pojedinci popuštaju pod pritiscima. Na taj način postojeće stanje pogoduje širenju alternativnih oblika ispoljavanja nezadovoljstva i pokušaja da se postojeći poredak promeni.

3.3 Posledice globalizacije koje pogoduju širenju kiberterorizma – mikro nivo

Globalizacija utiče na gotovo svakoga, odvija se upravo „*ovde*" i snažno utiče kako na javnu, tako i na privatnu društvenu sferu - intimni i lični aspekt života svakog pojedinca. Iako mnogi autori primat daju ekonomskim posledicama globalizacije, nisu zanemarljivi njeni uticaji na: kulturu, pojedinca, identitet, stavove - etičke, psihološke, ekološke i dr. Dakle, reč je o kompleksnom, sveprožimajućem, polivalentnom i protivrečnom fenomenu, koji predstavlja značajan izazov za celokupno čovečanstvo uopšte.

Savremena globalizacija otvara brojna pitanja i postavlja brojne izazove. Jer, dovodi u pitanje nekadašnje osnove i menja čovekovo shvatanje i znanje, komunikaciju, moralnost, utiče na identitet, podrazumeva iskorak iz domena vlastite kulture, dok brzina promena otežava adaptaciju čoveka na novonastalu situaciju. Istinska globalna kultura prema Tomlinsonu (Tomilson, 1999) ne može da postoji bez stvarnog prihvatanja kosmopolitskih vrednosti. Vrednosti u savremenom društvu su uzdrmane i nestabilne, što dalje stvara unutrašnji konflikt pojedinca. To se dalje odražava na sve sfere njegovog delovanja. Pojedinac je na međi da bira između najmanje dva tipa ličnosti: „*lokalnog*" i „*kosmopolitskog*" (Merton, 1957).

Dakle, principi liberalizma na kojima globalizacija počiva iznedrili su brojne promene. Pojedinci popuštaju pod ovim pritiskom, dok velika brzina kojom se promene odvijaju znatno umanjuje mogućnost predviđanja. To izaziva kod pojedinca osećaj nesigurnosti, strah, otpor, nepoverenje, doživljaj stranog kao nametanje i svojevrsnu agresiju prema svemu stranom, što dovodi do pojave ekstremnih reakcija bilo da su u pitanju pojedinci (stranci), njihov kapital ili kultura.

Dakle, globalizacija pored brojnih olakšica i prednosti stvara i „*duboku krizu morala i sistema vrednosti. Tri su osnovna etička izazova koja su dovela do globalne krize:*

1) ogromna pohlepa izražena kroz sumanutu trku za profitom;

2) odsustvo empatije i elementarnog osećaja za drugog čoveka;

3) etos rasipništva koji je tako modeliran da podstiče na zaduživanje, sticanje i trošenje" (Ljajić, Meta, Mladenović, 2016, 45).

Na koji način obični ljudi doživljavaju proces globalizacije? Da li je poistovećuju sa modernizacijom, zapadizacijom i amerikanizacijom? Različita istraživanja su se bavila ovom tematikom. Istraživanje sprovedeno u Hong Hongu čija je svrha bila da prikaže način na koji ljudi vide modernizaciju i zapadizaciju pokazalo je da modernizaciju vide kao proces usavršavanja, odnosno prikupljanja i primenu naučnog znanja, kako u upravljanju, tako i u obrazovanju. Dok, zapadizaciju vide kao proces asimilacije zapadnih sistema vrednosti (socijalnih, moralnih i političkih), kao i ljudskih prava i sloboda sa lokalnim kulturnim sistemima i dotadašnjim vrednostima (Fu & Chiu, 2007).

Da globalizacija istovremeno naglašava razlike i ujedno stvara sličnosti, ujedinjuje i odvaja primećuju Leher i Boli (Lechner & Boli, 2003). Čiu i saradnici (Chiu et al, 2011) navode: „*strah, zavist, bes, izolovanje, odbacivanje, agresija, javljanje pobude da se brani integritet vlastite kulture*“, kao odbacujuće reakcije na globalnu kulturu. Ove emocionalne reakcije i strah od kulturalne kontaminacije se prema navodima Čenga (Cheng, 2010) najčešće javljaju u nezapadnim kulturama. Negativne reakcije na posledice globalizacije su najčešće kod ljudi iz nezapadnih i nerazvijenih zemalja, te su oni zbog dotadašnjih istorijskih iskustava i kulture sećanja podozrivi prema zapadnjačkim uticajima i vide razvijene zemlje kao izvoznike kapitalizma.

Redefinicija prostora (Bauman, 2003) i „*njegovo univerzalno otvaranje kao toposa novog tipa suverenosti*“ (Hardt i Negri, 2003, 146), „*sabijanje prostora i vremena*” (Gidens, 1985, Robertson, 1992) omogućavaju brz protok informacijai lako mešanje kultura. Tako s jedne strane imamo tehnološki progres i brojne olakšice koje on sa sobom nosi, dok s druge strane raste stres kod ljudi, slabe društveni odnosi (porodični, partnerski i prijateljski), menja se način komunikacije, prisutna je otuđenost i kriza identiteta, raste broj fizičkih i mentalnih oboljenja izazvanih stresom, nekretanjem i drugim faktorima koji proizilaze iz savremenog načina života.

U takvim uslovima terorističke organizacije mogu da predstavljaju vid socijalne sigurnosti, zajedništva i podrške socijalno isključenima, protivnicima društvenog poretka, otuđenima, obespravljenima i dr. Naročito, jer počivaju na nezadovoljstvu i kritici novonastale situacije i neguju osećaj empatije i pripadnosti sa žrtvama savremenog poretka i apeluju na nužnost promene u savremenom globalnom društvu.

Terorističke organizacije su uglavnom bazirane na poverenju svojih članova, koji kroz međusobnu komunikaciju i praktikujući različite terorističke aktivnosti razvijaju osećaj pripadništva što dalje učvršćuje odanost njihovim zajedničkim ciljevima i vrednostima. Nasuprot tome savremeni svet karakteriše sve veća otuđenost pojedinca. Usled upotrebe raznih sredstava informisanja i komunikacije (*fejs*, *twitter* i dr.) održavanje socijalnih veza i komunikacija postaje površnije. Takva situacija ostavlja prostora za kiber terorizam kao primamljivu i lako pristupačnu formu terorizma.

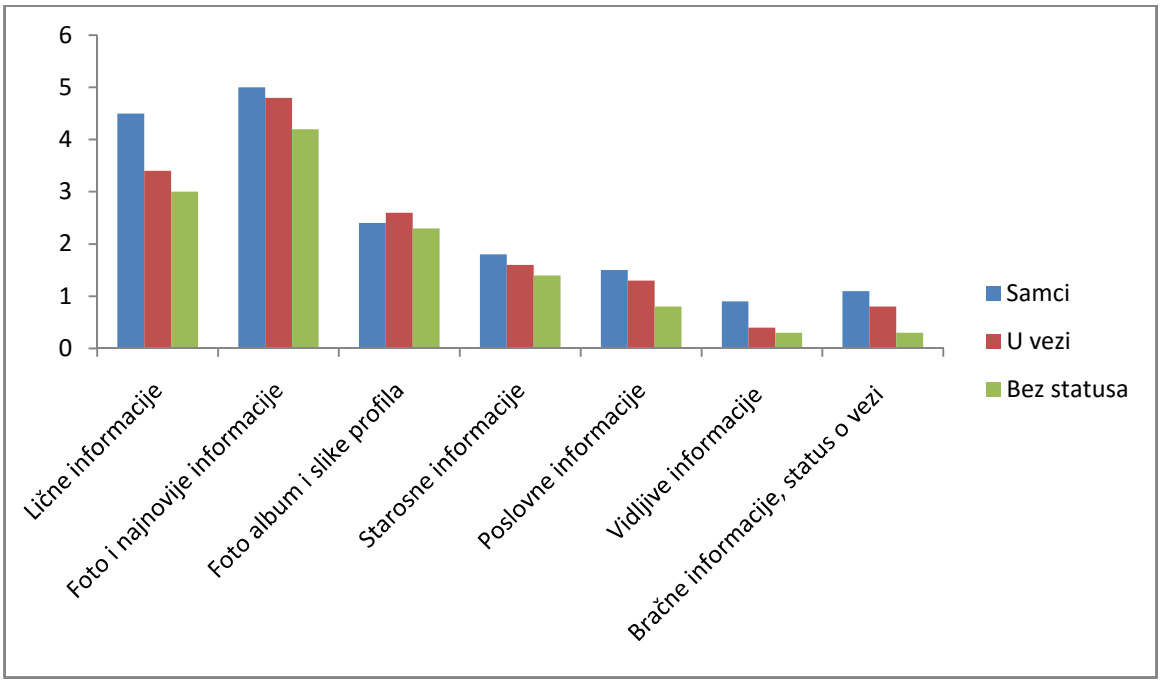
3.3.1 Virtuelne zajednice

Iako nastaju u virtuelnom prostoru, virtuelne zajednice su istinite kao i one koje postoje u fizičkom prostoru „*face-to-face*“. Jer, u njima ljudi takođe mogu da manipulišu određenim informacijama, da ih dobiju ili pruže, vode debatu, pregovaraju ili kritikuju fizičku realnost. Interakcije u virtuelnom prostoru podrazumevaju stvaranje novih oblika identiteta, za čiju koordinaciju sa drugim učesnicima je neophodna upotreba interneta.

Elektronska komunikacija je relativno novi oblik komunikacije, koji karakteriše jednostavan i brz prenos informacija, bilo putem računara, bežičnih *wireless* uređaja, mobilnih telefona i dr. To proizvodi nove vrste društvenih mobilizacija koje nisu specifično vezane za lokalno. Svako ko ima pristup internetu, može da pristupi informacijama sa bilo kojeg mesta. Postoje različite veb stranice, blogovi i grupe za ćaskanje (onlajn diskusije) u kojima ljudi mogu da pronađu ili objave željene informacije.

Kako usluge na internetu funkcionišu? Na primer, Tviter (*Twitter*) je jedna vrsta usluge na internetu u kojoj: „*(1) korisnici imaju javni profil u kojem emituju kratke javne poruke ili ih ažuriraju, usmeravaju na određene korisnike ili ne, (2) poruke postaju javno agregirane između korisnika, i (3) korisnici mogu da odluče čije poruke žele da primaju, ali ne i nužno ko može da prati njihove poruke; ovo se razlikuje od većine društvenih mreža gde je praćenje (following) jednih prema drugima dvosmerno (tj. uzajamno)*“ (Murthy, 2012, 1061). Korisnici društvenih mreža konzumiraju internet usluge na osnovu svojih interesovanja, što ih najčešće dovodi u interakciju sa ljudima koje ne poznaju. Tviter (*Twitter*) i Fejsbuk (*Facebook*) su javni profili čiji korisnici mogu da objavljuju (postuju) svoje statuse gotovo svakodnevno, što postaje važan deo njihovog identiteta (Murthy, 2012; Boon & Sinclair, 2009). Na taj način naizgled banalan *tweet* postaje važno sredstvo pomoću kojeg pojedinac gradi i potvrđuje svoj identitet na društvenim mrežama.

Tabela 7. Prisustvo ličnih informacija na Facebook profilu (Nosko, 2010, 415)



Dakle, veb usluge pružaju korisnicima da formiraju i ažuriraju javni ili polu-javni profil unutar određenog sistema putem kojeg korisnici mogu da se povezuju sa drugim korisnicima i na taj način formiraju virtuelne zajednice. Virtuelne zajednice predstavljaju novu društvenu formu koja se razlikuje od klasičnih samim time jer ne podrazumeva direktne kontakte „*licem u lice*“, poznanstvo i prisutnost, već se ostvaruje kroz upotrebu savremenih informacionih tehnologija.

Razvoj tehnologija stvorio je novu vrstu moći koja je bazirana isključivo na tehnološkim veštinama i znanju. Postojeća moć se realizuje pomoću interneta i remeti dosadašnji poredak moći koji pogoduje tradicionalnim elitama. Razvoj savremene tehnologije omogućava svakome pristup informacijama, ne jedino elitama. Ali, takođe otvara mogućnosti za kriminalce i kriminalna dela novog tipa, kao što su kiberkriminal i kiberterorizam. „*Njihova devijantnost, podržana moćnom tehnologijom, može imati vrlo ozbiljne i obimne posledice po društvo. Dakle, sviđalo se to nekom ili ne, oni postaju respektabilni članovi kluba kriminalaca sa belom-kragnom. Rađa se nova elita pod nazivom kiber-elita. Ono što se nikako ne bi smelo prevideti je visoka verovatnoća objedinjavanja, radi zajedničkog delovanja, ove novonastajuće elite sa devijantnim delom klasične moćne elite*“ (Petrović & Stojanović, 2016, 13).

3.3.2 Kiberkultura

U savremenim uslovima društvene transformacije i uključivanja svih sfera društvenog postojanja u globalne procese razvoja, kolektivni oblici kulturne identifikacije predstavljaju značajne odbrambene mehanizme prilagođavanja na novonastalu situaciju. Postoji mnogo definicija kulture. Jedna od njih definiše je kao „*društveno nasleđe koje pojedinac dobija od svoje grupe*“; „*način mišljenja, osećanja i verovanja*“ i „*apstrakt ponašanja*“ (Gerc, 1998, 11). Generacijsko prenošenje kulturnih dobara i vrednosti na članove zajednice je jedna od osnovnih funkcija kulture. Iako se kultura prevashodno odnosi na društveno nasleđene i naučene obrasce mišljenja određene grupe ljudi, zajednice ili društva, to nipošto ne znači da kultura ne sadrži komponentu individualnosti.

Pripadnici različitih društvenih grupa razvijaju svoje posebne vrste kulture, što je u literaturi poznato pod nazivom potkultura ili subkultura. „*Jedan poseban, relativno zatvoren segment opšte kulture, čiji pripadnici dele zajednička uverenja, običaje i vrednosti, a često i način oblačenja, ishrane, ponašanja i moralne norme*” (Videnović, 2015), a razlikuje se i „*izdvaja*“ od kulture šire zajednice kojoj ta grupa pripada nazivamo subkultura. Uz ovaj termin često se koristi i termin kontrakultura, obzirom da pripadnici određene subkulture dominantne vrednosti neke zajednice ili odbacuju (ne u celosti), ili tumače na sebi svojstven način. Iako subkulturu vezujemo isključivo za kulturne sadržaje određene društvene grupe, sloja ili sredine, ona ne predstavlja izolovanost, nego kulturnu šarolikost. Subkultura se „*može analitički raščlaniti i definisati na sledeći način: a) u odnosu na univerzalnu kulturu, potkultura predstavlja relativno zaokrugljenu, samosvojnu i identitarnu celinu; b) nju čine vrednosti, pravila i norme koje članovi grupe usvajaju i praktikuju na duže vreme, slede i produžavaju; v) potkulture reprezentuju osobenosti socijalnih grupa, slojeva i njihovih položaja; d) potkulturne grupe su kreatori i vlasnici različitih stilova*“ (Božilović, 2004, 53-54).

Upotrebom savremene tehnologije akteri u kibernetskom prostoru teže da se potvrde u alternativnoj stvarnosti te stvaraju virtuelne zajednice i svoju kulturu koja predstavlja novi vid subkulture – kiberkultura. U realno postojećoj stvarnosti osetljivi su na pravila koja postoje i uslove poretka, te nastoje da prenesu šifre odnosa iz virtuelne sredine koja ih prihvata na kolektive i institucije sa kojima dolaze u dodir.

U virtuelnom svetu im je omogućeno samostalno oblikovanje životnog stila i uloga, jer im virtuelni svet pruža brojne mogućnosti, kao što su odabir identiteta, virtuelnog okruženja i onih sa kojima žele da komuniciraju. „*Dok se pitaju šta žele, učesnici potkultura simbolički obeležavaju polje delovanja, a samom pojavom na određenom mestu oni izražavaju razlike u sklonostima. Povezivanjem sa izabranom potkulturnom grupom, mladići i devojke teže da se izdvoje od primarnih društvenih zajednica kojima pripadaju i da se udalje od uloga koje su im namenjene. Napuštajući mesto represivnih očekivanja, bar privremeno, neutrališu važenje strogih zahteva i otpisuju značaj poretka koji ih odbija*“ (Marić, 1998, 160).

Razvoj globalne ekonomije uslovio je migracije radne snagekoje su najčešći uzrok multikulturalnih dodira, dok je kibernetski prostor omogućio kontakte bez stvarnog fizičkog kretanja ili preseljenja. Uticaj medijaje takođe velik. Učestali kulturni dodiri uzrokovani globalizacijom bude svest o kulturnim razlikama i stvaraju izazove, jer dovode u pitanje dotadašnje kulturne sisteme i vrednosti, „*identifikaciju sa lokalnom kulturom*“ (Tong, et al, 2011) i stvaraju „*strah za egzistenciju*“ (Torelli et al, 2011). Pomenuti kulturni dodiri mogu da uzrokuju kako pozitivne, tako i negativne individualne reakcije. Odbijanje prihvatanja stranih kulturnih sadržajaje posledica negativnih reakcijakoje nastaju usled mešanja kultura. Pozitivne reakcije najčešće nastaju ukoliko multikulturalna iskustva i mobilnost nastaju kao rezultat usavršavanja i razvojapojedinca, određene društvene grupe ili institucije i one vode sintezi/kulturnoj asimilaciji, koja znači usvajanje pojedinih elemenata iz strane kulture.

Mnogo toga što definišemo kao deo kiber subkulture se sastoji u ličnom ili političkom blogiranju, aktivizmu društvenih medija na platformama kao što su *Facebook*, *Twitter*, *Instagram* i dr. (Kahn i Kellner, 2004). Blogovi su posebno dizajnirane mreže za vođenje dijaloga i debata, razmenu alternativnih informacija, demokratsko samoizražavanje i političku kritiku i sl. Dela Porta (Della Porta, 2012, 49) je takođe tvrdila da su nove tehnologije poboljšale komunikacijsko poverenje kod društvenih pokreta, koji ih uglavnom koriste za mobilizaciju istomišljenika.

3.3.3. Kriza identiteta

Kako savremeni trendovi i izazovi novog globalnog poretka utiču na „*homosociologikusa*“? Kako doživljava, razume i shvata društvene procese i odnose u koje je svakodnevno uključen? Kakvo je njegovo psihološko funkcionisanje? Početkom 21.veka razmatranje društvenih uslova i razumevanje savremenog „*homosociologikusa*“ nije izvodljivo lokalno već samo globalno (Bek, 2002, 17-44).

Brisanje barijera između globalnog i lokalnog najbolje ilustruje termin „*globalitet*“ (Yergin, 2002) koji služi da označi stanje globalne realnosti i konkurentske odnose, koji nastaju usled strukturnog pomeranja tokova trgovine. Jer, međunarodne gigantske kompanije konkurišu zajedno sa lokalnim za: partnere, kapital, potrošače, dobavljače, kapacitete i sisteme distribucije. Ruši se dosadašnja hijerarhija ekonomskih snaga i uticaja na lokalnom i globalnom nivou, stvara se nova preraspodela svetskog bogatstva, što se dalje odražava i na promene u kulturnoj sferi gubitkom kulturnih identiteta i homogenizacijom kultura. Globalno decentralizovano poslovno okruženje karakteriše pojava novih pravila poslovanja i upravljanja, inkorporiranje stranih uticaja i modifikacija lokalnog. Primena savremenih tehnologija i društvenih mreža za razmenu informacija u različite svrhe, kako poslovne tako i privatne u mnogome utiče na kvalitet života savremenog pojedinca. Stvoreni su novi uslovi i izazovi za integraciju individualnog i globalnog. To dalje dovodi u pitanje nekadašnje postavke identiteta i vodi njegovom redefinisanju.

Identitet je predmet razmatranja onda kada ga dovodimo u pitanje, tj. kada je u krizi. Šta identitet predstavlja za pojedinca? „*Pojmom identiteta izriče se osnovni ljudski smisao, a sva ostala varijabilna određenja nisu drugo do njegove akcidencije*“ (Kalanj, 2010, 119). Postoji nekoliko vrsta identiteta: društveni, politički, kulturni, religiozni, nacionalni, teritorijalni, itd.

Kao što Apadurai primećuje „*centralni problem globalnih interakcija je tenzija koja nastaje između homogenizacije i heterogenizacije*“ (Appaduruai, 2000). Obzirom da globalizacija značajno utiče na psihičko funkcionisanje ljudi, a naročito na transformaciju identiteta u 21.veku, njene efekte na identitet možemo da prikažemo Arnetovom (Arnett, 2002) podelom aspekata identiteta:

1. „*bikulturalni identitet*“ - predstavlja kombinaciju lokalnog i globalnog identiteta, koji dalje rezultira stvaranjem složene hibridne forme identiteta,

2. „*konfuzni identitet*“– karakteriše otuđenost, osećaj marginalizovanosti i ne pripadanje nijednoj kulturi,

3. „*identitet samoodabrane kulture*“- podrazumeva individualni odabir i/ili pridruživanje odabranoj kulturi kolega disidenata (Arnett, 2002). Iako je Arnet tumačio efekte globalizacije prevashodno na adolescentima, njegova podela je primenljiva zbog opšteg uticaja koji globalizacija ima na identitet pojedinca bez obzira na starosno doba. Poslednji aspekt identiteta možemo da nazovemo „*pomaljajuća odraslost*“ (Arnett, 2002) i on predstavlja prihvatanje situacije i pronalaženje sebe. Istraživanja su pokazala da „*prihvatanje stranih ili globalnih vrednosti ne znači nužno i žrtvovanje lokalnog kulturnog identiteta*“ (Tong, 2011; Morris, 2011). Lokalne zajednice nastaju kao rezultat dugogodišnjeg kolektivnog delovanja generacija putem kojih se prenose znanja i iskustva i čuvaju u vidu kolektivnog pamćenja. Otuda lokalne zajednice predstavljaju jedinstvenu osnovu za formiranje kolektivnog identiteta koji daje smisao delovanju prevashodno na temelju kulturnih pretpostavki u odnosu na druge izvore smisla. Kolektivni identiteti nesumnjivo pružaju svojevrstan odgovor na izazove globalizacije i predstavljaju moćno sredstvo za „*određivanje i lociranje pojedinačnih 'ja' u svetu, kroz prizmu kolektivne ličnosti i njene osobene kulture. Upravo nam zajednička, jedinstvena kultura omogućava da saznamo ko smo mi u savremenom svetu. Ponovo otkrivajući tu kulturu, otkrivamo sami sebe, autentično lično ja*” (Smit, 1998, 34). Međutim, kao što Kastels primećuje „*ti su identiteti, u većini slučajeva, odbrambene reakcije na nametanje globalnoga nereda i promena koje se brzo odigravaju i koje se ne mogu nadzirati. Oni grade skloništa, ali ne i nebesa*” (Castells, 2002, 73). Pojedinci koji se nalaze u stanju konfuzije identiteta, ili nikako ne mogu da se identifikuju ni sa jednim, uglavnom su marginalizovani pojedinci, sa niskim nivoima lokalne i globalne identifikacije (Norasakkunkit & Uchida, 2011).

Imaginacija je ključ za razumevanje savremenog globalnog poretka (Appadurai, 2000). Informacione tehnologije omogućile su prevazilaženje fizičkih i nacionalnih granica i krstarenje kiberprostorom i „*nova sredstva za izgradnju zamišljenih sebe i zamišljenih svetova*“ (Appadurai, 2000, 3) proizvode mnoštvo zamišljenih identiteta i zajednica. Postovanje (objavljivanje na internetu) svakodnevnih događaja, raspoloženja i razmišljanja nas u određenom smislu promoviše. *Twitter, Facebook* i drugi online profili deo su publiciteta.

Jer, kao što je istraživanje pokazalo, broj pratilaca ili prijatelja, kao i ono što objavimo na društvenim mrežama predstavljaju promociju sebe „*reklamu*“ (Livingstone, 2008), što znatno utiče na to kako se mi percipiramo. Iako je Livingstonovo istraživanje uglavnom usmereno na istraživanje uticaja društvenih mreža na mlade, takođe i drugi deo populacije - odrasli koriste društvene mreže i na taj način formiraju „*online*“ identitete koji ih promovišu u privatne i poslovne svrhe. To dalje otvara pitanja bezbednosti od različitih formi kibernasilja i zloupotreba informacionih tehnologija.

3.3.4. Alijenacija

Alijenacija postaje sve prisutniji problem u savremenom društvu. Različiti faktori koji tome doprinose su:

- ekonomski – Dosadašnja istraživanja su pokazala da ekonomski razvoj ima pozitivne posledice na ostvarivanje materijalnih ciljeva, ali da „*istovremeno slabi osećaj zajedništva i stvara hladnije, manje humane društvene sredine*“ (Fu, H. -Y., & Chiu, 2007, 636–653). Do sličnog nalaza su došli Jang i saradnici (Yang et all, 2011, 677-695). Autori Tisakloglou i Papadopoulos razlikuju četiri dimenzije deprivacije: „*objektivno siromaštvo, socijalne veze, uslovi stanovanja i potrošnja dobara*“ (Tsakloglou & Papadopoulos, 2002).

- socijalni – Nepotpuna socijalizacija je najčešći uzrok ovog tipa alijenacije. Takođe, pojedinci se različito prilagođavaju savremenim društvenim tokovima. U okviru jednog društva različiti pojedinci dramatično različito doživljavaju globalizaciju (Norasakkunkit & Uchida, 2011, 774-786) koja nesumnivo ostavlja snažne posledice na socijalne odnose. Ugrožena je osnovna baza ljudskog društva - porodica koja se suočava sa brojnim izazovima, što rezultira povećanim brojem razvoda i samohranih roditelja. Socijalna isključenost nije stvar izbora, već posledica ograničavanja koja dovodi do delimične ili u celosti neuključenosti u nematerijalne aspekte životnog standarda - socijalne veze.

- psihološki - Kriza identiteta pojedinca, psihički poremećaji.

- tehnološki - Tehnološki razvoj doprineo je da kontakti licem u lice postanu sve ređi, a poznanstva virtuelna. Nastaje novi vid društvenih zajednica i kiber kulture, koje pojedinci ne mogu sebi da pruže bilo zbog neznanja rada na računaru ili finansijskih nemogućnosti, te na taj način bivaju isključeni iz ovih novih društvenih formi. Ili sa druge strane prekomerna upotreba društvenih mreža dovodi do socijalne isključenosti toliko da ona prelazi u zavisnost od informacionih tehnologija.

- kulturni – Odbijanje stranih kulturnih sadržaja ili nepotpuna identifikacija sa kulturom zajednice kojoj pojedinac pripada. Sklonost ka određenim subkulturama, kontrakulturama.

- politički – Alijenacija nastaje usled nezadovoljstva postojećim društvenim poretkom i odnosima moći, kada pojedinac smatra da postojeći društveni svet i politička situacija nisu vredni učestvovanja. Politička alijenacija je „*dobrovoljan izbor pojedinca, koji nastaje usled njegovog stava prema društvenom sistemu da sistem ne pruža aktivnosti ili ciljeve koje on vrednuje*“ (Olsen 1969, 291-92). Studije pokazuju da demokratske političke institucije uživaju najslabiju podršku od strane onih koji su marginalizovani u društvu kojem pripadaju, jer stanje nemoći u kojem se nalaze predstavlja važan uslov koji ih navodi na pružanje otpora prema lokalnim pitanjima i vlasti. Zato su marginalizovani u društvu skloniji da glasaju za radikalne populističke stranke, pre nego za one koje su „podupirači" postojeće političke i ekonomske situacije i globalizacijskih težnji (Gibson, McAllister & Swenson, 2002; Lubbers, Gijberts & Scheepers, 2002).

Alijenacija (otuđenost) je multidimenzionalan fenomen. Svi predhodno navedeni faktori ne isključuju jedan drugog, već su tesno međusobno povezani uzročno –posledičnim vezama.

4. KIBERNETIČKI KRIMINALITET

4.1. Internet, pogodnosti i zloupotreba

Internet je revolucionarni izum koji je značajno promenio čovečanstvo. Zbog brojnih pogodnosti koje nudi predstavlja najefikasniju savremenu metodu komunikacije. Omogućava brzu i jednostavnu manipulaciju podacima različite vrste (audio i video) i nudi širok dijapazon ideja i informacija. Internet nesumnjivo pruža brojne olakšice. Vajmen kao „*osnovne prednosti interneta navodi: jednostavan pristup, malo ili nimalo regulacije, cenzure ili drugih oblika kontrole od strane vlasti, potencijalno ogromnu publiku raštrkanu širom sveta, anonimnost komunikacije, brz protok informacija, jeftin razvoj i održavanje prisustva na mreži, multimedijalno okruženje (mogućnost da se kombinuje tekst, slika audio i video i da se dozvoli korisnicima da „skidaju" filmove, pesme, knjige, postere i tako dalje), mogućnost da se uobličava izveštavanje u tradicionalnim masovnim medijima, koji sve više koriste Internet kao izvor svojih informacija*" (Weiman u: Damnjanović, 2009, 238-239).

Zbog sve većih mogućnosti koje internet nudi, ljudi postaju sve više zavisni, te raste i potencijal za njegovu zloupotrebu. Jer, korisnici interneta uglavnom ne poseduju dovoljno znanja da bi koristili brojne usluge koje internet pruža bezopasno. Štaviše, „*korisnici interneta su uglavnom nedovoljno upoznati sa funkcionisanjem računara, i vrlo često nisu spremni i voljni da preduzmu mere zaštite za koje oni smatraju da su suviše skupe, previše tehnički zahtevne ili da je potrebno utrošiti previše vremena na njihovu upotrebu*" (Abrams, Podell & Jajodia, 1995, 117).

Brz protok informacija na internetu omogućava brzo širenje kompjuterskih virusa, crva, trojanaca i drugih zlonamernih softvera, što uz generalno neznanje korisnika interneta o postojećim merama zaštite, čini da internet bude izvor mnogih problema i izazova. Internet sam po sebi nije uzročnik kriminala, ali je „*jednostavno moćno sredstvo komunikacije koje ima potencijal da pojača i ubrza kriminal*" (Williams, 2008). Tehnološka revolucija je uticala na kriminogeno okruženje tako što ga je transformisala i stvorila novi vid kriminala u kiberprostoru (Britz, 2013, 3, 75-76). Većina prevara na internetu su u stvari samo usavršene verzije ranijih, klasičnih prevara, u koje je internet doneo novine. Najčešći oblici zloupotrebe interneta su:

1) hakovanje – Nelegalni upad u kompjuterske sisteme. Može se reći da je najzastupljenije krivično delo koje se vrši putem interneta.

Motivi za hakovanje mogu da budu kako lični, tako i politički. Hakeri najčešće rade pripremne radnje i pristupaju zaštićenim (tajnim) podacima razbijanjem lozinki ili upotrebom za to predviđenih hardvera ili softvera. Dakle, hakovanje je samo uvertira za druga krivična dela kao što su neovlašćena manipulacija podacima ili špijunaža.

2) nezakonito prikupljanje podataka - Napadi na baze podataka iz veb aplikacija kojima se pribavljaju poverljive informacije, kao što su „*Cross-site scripting – XSS*“ (Vernotte et al, 2014) i „*SQL injection*“ (Halford, 2006).

3) krivično delo presretanja podataka –Ometanje transfera podataka, informacija i njihovo snimanje, bilo da se komunikacija odvija putem Interneta, bežičnog ili *wifi* (*e-mail*, *chat*, i dr.) ili fiksne linije. Meta napada je komunikaciona infrastruktura.

4) ometanje podataka – Ove vrste napada uglavnom su usmerene na ometanje i brisanje podataka koji su čuvani u kompjuterskim sistemima. Najčešće se izvode pomoću *Trojan Horse* softvera, crva (*Warms*) i dr.

5) internet reketiranje (ometanje rada sistema)– Napadači prete *DoS* napadom (*Denial-of-service attack*) i ucenjuju kompanije koje ostvaruju svoje poslovanje elektronskim putem, kao što su: elektronsko bankarstvo i e-prodavnice, pružaoci e-usluga i kockanja putem interneta i dr. Najčešće virusima i programiranim mrežama kompjutera za izvođenje organizovanih *DoS* napada ometaju poslovanje tih kompanija, napadaju vebsajtove i onemogućavaju njihove usluge, napadaju servere ili računarski sistem.

6) falsifikovanje – internet i kompjuterske alatke: iseci (*cut*), zalepi (*paste*) ili kopiraj (*copy*), omogućile su da se željeni deo teksta ili dokumenta iseca ili kopira sa njegove originalne verzije i lepi (*paste*) na lažni dokument. Što je ozbiljnost falsifikata veća, zahteva i veću umešnost i poznavanje rada na računaru.

7) pranje novca – „*Nelegalno prikrivanje nezakonitog profita od strane pojedinaca, malih preduzeća, korporacija, kriminalnih sindikata, korumpiranih zvaničnika, pa čak i korumpiranih vlada*“ (Britz, 2013, 106). Savremene informacione tehnologije i globalno finansijsko tržište omogućile su teže praćenje tokova novca i njegove lakše zloupotrebe. Pravna regulativa u vezi sa bankarskim poslovanjem nije ujednačena svuda u svetu. Tako su u nekim zemljama banke zakonom zaštitile svoje poslovanje tzv. bankarskom tajnom, dok su u drugim zemljama banke dužne da podnose redovne izveštaje o svom poslovanju.

Takva situacija otvara prostora da pojedinci peru novac tako što ga anonimno deponuju u zemlju sa pravnom regulativom koja im pogoduje, a potom odatle mogu da ga prebace za upotrebu u bilo koju drugu zemlju.

8) internet investicione prevare – Ni investitori nisu ostali imuni na prednosti koje internet pruža. Jednostavno i brzo pristupanje različitim investicionim izvorima, kao i neverovatno laka trgovina hartijama od vrednosti učinile su da internet bude prihvaćen kao važan alat za investitore. Međutim, investiranje samo po sebi nosi određenu dozu rizika, koji su se sa primenom interneta u ovoj oblasti uvećali. To potvrđuje veliki broj i različite vrste investicionih prevara (e-investicioni bilteni, investicioni veb sajtovi o lažnim fondovima, *spam* pošta i dr.).

9) prekršaji na internetu vezani za sadržaj – Podrazumeva promovisanje sadržaja koji je zakonom zabranjen u većini zemalja, kao što su: dečja pornografija, sadržaj koji podstiče ksenofobijui vređanje na etničkoj, rasnoj, religijskoj ili polnoj osnovi i dr.

Kao što je prethodno navedeno zloupotrebe interneta se mogu javiti u različitim oblicima. Možemo ih sistematizovati u dve glavne kategorije: „*upad u sisteme i DoS napade*“ (Nguyen, 2013, 1093). „*Upad*“ podrazumeva napad na računarske sisteme koji se oslanja na propuste, odnosno „*rupe*“ u sistemu koje napadači koriste kao priliku za upad u određeni sistem kako bi pristupili njegovim resursima i isporučili željenu alatku (virus ili *malver*). Malver je „*kod ili softver koji je posebno dizajniran da ošteti, naruši, ukrade ili uopšte nanese štetu ili nelegitimno utiče na podatke, hostove ili mreže*“ (Nguyen, 2013, 1094). Napadači primenjuju *DoS* napad da onemoguće pružanje usluga određenog sistema.

Teroristi se takođe služe internetom u različite svrhe. Vajman smatra da „*aktivnosti terorista na internetu možemo da klasifikujemo u osam grupa: 1. psihološki rat, 2. publicitet i propaganda, 3. traženje informacija, 4. prikupljanje fondova, 5. regrutovanje i mobilizacija, 6. umrežavanje 7. deljenje informacija, 8. planiranje i koordinacija*“ (Weimann u: Damnjanović, 2009, 239). Dakle, na internetu se mogu pronaći razni sadržaji o teroristima: teroristički vebsajtovi, snimci terorističkih napada, čak i e-obuke terorista i dr.

4.2. Kiberkriminal

U naučnoj javnosti, još uvek nije ustanovljena jedinstvena definicija pojma kiberkriminala. Na kongresu Ujedinjenih nacija predložena je sledeća definicija kiberkriminala: „*Kriminal koji se odnosi na bilo kakav oblik kriminala koji se može izvršavati posredstvom računarskih sistema i mreža, u računarskim sistemima i mrežama ili protiv računarskih sistema i mreža*“ (Gercke, 2012, 11-12). Ova definicija sadrži određenje kiberkriminala u užem i širem smislu. Tako se kiberkriminal u užem smislu odnosi na kompjuterski (računarski kriminal) kojim se ugrožava bezbednost kompjuterskih sistema i podataka, dok u širem smislu kiberkriminal podrazumeva sve kriminalne radnje koje su sprovedene upotrebom kompjutera (računarskih sistema), uključujući i ilegalnu distribuciju informacija i drugih sadržaja.

Kiber kriminal podrazumeva posebnu vrstu kriminalnih radnji kojima se ugrožava bezbednost kibernetskog prostora u celini, ili pojedinih njegovih delova na različite načine i upotrebom različitih sredstava unutar računarskih sistema kako bi počinioci pribavili protivpravnu korist za sebe ili učinili štetu nekom fizičkom ili pravnom licu. Za ovu vrstu krivičnih dela u upotrebi je nekoliko različitih naziva: „*kompjuterski kriminalitet*“ (Gercke, 2012, 11), „*sajberkriminal*“ (Clay, 2007, 4), „*visokotehnološki kriminal*“ (Službeni glasnik Republike Srbije“ broj 61/05), „*computer abuse -zloupotreba kompjutera, crime by computer - delikti uz pomoć kompjutera, computer fraud - kompjuterska prevara, informatički kriminalitet, sajber kriminalitet, tehno kriminalitet*“ (Jovašević, 2011, 639).

Uporedo sa ekspanzijom automatizovanih informaciono-tehnoloških sistema, rastu i bezbednosni rizici. Odnosno upotreba kompjuterskih tehnologija omogućila je da ranije poznata tradicionalna krivična dela kao što su razne vrste prevara, falsifikovanja i pronevere novca i krađe poprime novi oblik i način izvršenja. To iziskuje stvaranje nove regulative i mera kažnjavanja za pomenuto protivpravno ponašanje. Otuda je pojmu opšteg kriminaliteta neophodno dodati i „*kompjuterski kriminal kao obeležje progresivnog kriminaliteta*“ (Đokić & Živanović, 2005, 305-318). Kiberkriminal obuhvata: „*krađu intelektualne svojine, kršenje prava zaštite patenta, tajne trgovine, kršenje zakona o autorskim pravima, napade protiv računara kojima se namerno utiče na obradu podataka*“ (Clay, 2007, CRS-4).

Mogućnosti zloupotrebe informacionih tehnologija su velike: „*Računar ili uređaj može da bude zastupnik zločina, pomoćno sredstvo za izvršenje krivičnog dela ili meta zločina; zločin se može dogoditi na samom računaru, ili na ne-virtualnoj lokaciji*“ (Gordon & Ford, 2006, 14).

Zato se termin kiber kriminal koristi za pokrivanje širokog spektra kriminalnih postupaka, odnosno ne obuhvata samo napade koji se mogu izvesti upotrebom telekomunikacionih mreža, nego i napade na same informacione sisteme, kompjutere, kao što su: špijunaže, otkrivanje i presretanje tajnih podataka i njihovo neovlašćeno kopiranje, ometanje obrade podataka, krađu intelektualne svojine, autorskih prava ili patenata, distribuciju različitog sadržaja (virusa, dečje pornografije i dr.), prevare putem interneta i mejlova, mešanje u online finansijske usluge i brojne druge.

Prema Izveštaju Saveta Evrope o organizovanom kriminalu iz 2005. godine navedene kategorije dela evidentirane su kao kiberkriminal:

1) „*krivična dela protiv poverljivosti*”, integriteta i raspoloživosti, odnosno dostupnosti podataka i računarskih sistema (tzv. CIA prekršaji). To uključuje ilegalni pristup računarskim sistemima hakovanje kompjutera, prisluškivanje, prevare korisnika interneta (npr. špijunaža, krađa lozinke, pecanje), računarske špijunaže (uključujući upotrebu Trojanskih konja i drugih tehnika), kompjuterska sabotaža i iznuđivanje (npr. virusi i crvi, napad u vidu poricanja usluge, spamovanje ili bombardovanje e-pošte);

2) „*tradicionalna krivična dela izvršena pomoću računara*“ (u rasponu klasičnih prevara kao što su: manipulacije računima ili bilansima kompanija, online manipulacije, aukcijske prevare i onlajn prevare porudžbina, nezakonita upotreba bankomata, zloupotreba kreditnih kartica, falsifikovanje i drugi oblici prevara i napada manipulacijom kontrolnih sistema ili bolničkih računara);

3) „*krivična dela u vezi sa sadržajem kao što su dečja pornografiju, rasizam i ksenofobija*“, traženje, podsticanje i pružanje uputstava za ponašanje koje podstiče zločine od ubistva do silovanja, mučenja, sabotaže i terorizma. Ova kategorija uključuje i kiber uznemiravanja, klevetu i širenje lažnih informacije preko interneta i internet kockanje;

4) „*krivična dela vezana za kršenje autorskih i srodnih prava*“ kao što su neovlašćeno reprodukovanje i korišćenje računarskih programa, audio/video i drugih oblika digitalnih radova, ili podataka iz banki i knjiga (Savet Evrope, 2005, 40).

Ono što neko kriminalno delo određuje kao kiberkriminal je to što je „*izvršeno korišćenjem kiber tehnologije u kiber domenu*“ (Tavani, 2003, 103). Dakle, kada je u pitanju kiberkriminal značaj informaciono-komunikacione tehnologije, odnosno računarske mreže je višestruk. Kompjuterski (računarski) kriminalitet je specifičan vid kriminaliteta koji se javlja u različitim oblicima u zavisnosti od njegovih osobenosti, kao što su struktura, način na koji se ova vrsta kriminaliteta ispoljava i sredstava koja se upotrebljavaju prilikom njegovog izvršenja i karakteristika učinioca.

Obzirom da kiber kriminal, sa stanovišta pravnih nauka podrazumeva delikte koji su inkriminisani zakonima, Fišer predlaže upotrebu šireg pojma „*kiber pretnje*“ (Fischer, 2005) da obuhvati kako inkriminisane radnje, tako i one koje još uvek nisu proglašene krivičnim delima u važećim krivičnim zakonicima. Kiber pretnje su „*zlonamerna upotreba tehnologija koje pripadaju kibernetskom prostoru kao instrumenata pretnje, ali i kao ciljeva od strane velikog broja aktera– kriminalaca, terorista, organizacija i država*“ (Fischer, 2005, 6).

Ključna odrednica ovog kriminaliteta je tesna povezanost sa tehnologijom, iz koje proizilazi i njegova dinamičnost i šarolikost pojavnih oblika. Međutim, ipak možemo izdvojiti njegove osnovne karakteristike: „*1) objekt zaštite je bezbednost računarskih podataka ili informacionog sistema u celini ili njegovog pojedinog dela (segmenta), 2) poseban, specifičan karakter i priroda protivpravnih delatnosti pojedinaca, 3) posebna znanja i specijalizacija na strani učinioca ovih krivičnih dela koja isključuje mogućnost da se svako, bilo koje lice nađe u ovoj ulozi, 4) poseban način i sredstvo preduzimanja radnje izvršenja - uz pomoć ili upotrebom (zloupotrebom) računara, 5) namera učinioca kao subjektivni elemenat u vreme preduzimanja radnje koja se ogleda u nameri pribavljanja za sebe ili drugog koristi ili nanošenja štete drugom fizičkom ili pravnom licu*“ (Petrović & Jovašević, 2006, 211-214).

Izvršioci računarskih (kompjuterskih) krivičnih dela su lica kojima su informacione tehnologije fizički dostupne. Međutim, potrebno je da poseduju stručno znanje i praktične veštine iz oblasti računarskih tehnologija. Odnosno, fizički kontakt počinioca sa žrtvom nije nužan. Otuda su njihovi izvršioci uglavnom specifična kategorija, nenasilni i nedelikventni. Sve se odigrava u jednom virtuelnom prostoru, kiber (*cyber*) prostor, koji je „*veštačka tvorevina koja zahteva visoku tehničku opremljenost, dobru informacionu infrastrukturu koja je ničija i svačija svojina, u kome paralelno koegzistiraju virtuelno i realno i kod koga je komunikacija kolektivna*“ (Matijašević-Obradović, 2014, 279-298).

Stoga specifičnost računarskih (kompjuterskih) krivičnih dela proizilazi i iz same činjenice da se ona vrše unutar kiber (*cyber*) prostora, prikriveno - pod tajnim (virtuelnim) identitetom, neretko uz postojanje vremenske razlike između momenta kada je izvršena kriminalna radnja i trenutka kada je nastupila posledica takvog *online* postupanja. Kompjuterski kriminalitet se ispoljava u različitim oblicima u zavisi od sledećih elemenata:

1) osnovne mete (cilja) kiber napada – da li je fizičko ili pravno lice, da li je težnja da se nanese šteta mreži u celosti ili jednom njenom određenom delu, da se ometaju pojedine funkcije, izvrši upad i dr.;

2) oruđa kojim se kiber kriminalci služe zarad postizanja svojih ciljeva;

3) okruženja u kojem se realizuju kiber napadi;

4) dokaza – odnosno upotrebljenih tehnoloških sredstava i interneta za njegovo izvršenje je ono što svrstava učinjena kriminalna dela u kiberkriminal i pomaže njegovo otkrivanje i dokazivanje.

5) težina posledica i visine načinjene štete.

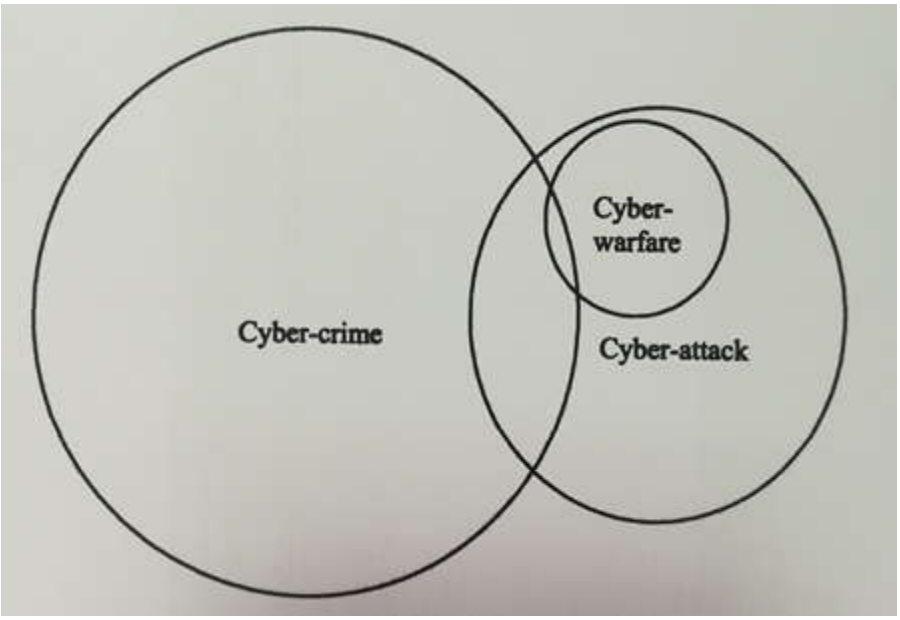
Tabela 8. Oblici kompjuterskog kriminala (Babić, 2009, 67-239)

Oblici kompjuterskog kriminala	
1. Tradicionalni	2. Neotradicionalni
1.1. Prenos podataka	2.1. Hakovanje
1.2.Virusi	2.2.Dečja pornografija
1.3.Trojanski konj (*Trojan Horse*)	2.3. Kiberterorizam
1.4.Seckanje (*Salami-Techniques*)	2.4.Kiber rat
1.5.Superzappping	2.5. Prisluškivanje i kompjuterska špijunaža
1.6. Stepenice (*Trap Doors*)	2.6. Neovlašćeno korišćenje usluga
1.7.Logičke (programske) bombe	2.7. Neovlašćeno kopiranje i reprodukcija kompjuterskih programa
1.8. Asinhroni napadi (*Asynchronous Attacks*)	2.8.Neovlašeno menjanje podataka i/ili programa (kompjuterska prevara krivotvorenje isprava i overavanje neistinitog sadržaja)
1.9. Strvinarenje (*Scavenging*)	2.9.Kompjuterska prevara
1.10. Curenje podataka (*Data Leakage*)	2.10. Kompjuterski falsifikati
1.11. Krpljenje i prerušavanje (*Piggybacking & Impersonating*)	2.11.Krivotvorenje kreditnih kartica
1.12. "Ožičavanje", prisluškivanje (*WireTapping*)	2.12.Kompjuterska ucena i iznuda
1.13. Simulacija kažnjivih dela kao njihova pripremna faza	2.13.Neovlašćeno uklanjanje ili uništavanje podataka i /ili, programske i tehnološke podrške (kompjuterska sabotaža)
	2.14.Kompjuterska krađa
	2.15.Organizovani hakerski kriminal

4.3. Distinkcija kiberkriminal – kiberterorizam

„*Kiber pretnje, kiber incidenti i kiber vandalizam poput oštećenja sajtova nisu terorizam. Sama zabrinutost u vezi kiber terorizma potiče od kombinacije straha, neznanja ili o tome što se na globalnom nivou nisu suštinski definisali, taksativno nabrojali akti koji se mogu okarakterisati kao takvi*“ (Jonev, 2016, 2).

Slika 4. Relacija između kiber aktivnosti (Hathaway, 2012, 833)



Po čemu se razlikuju kiberkriminal i kiberterorizam? „*Generalno, oni se razlikuju na osnovu cilja aktivnosti. Kiberkriminal se uglavnom odnosi na zločine koji su počinjeni upotrebom informacionih tehnologija, naročito interneta za ostvarenje lične koristi, a kiberterorizam se odnosi na zločine koji podrazumevaju upotrebu informacionih tehnologija u političke svrhe*“ (Fischer, 2005, CRS-10).

Dakle, ključna razlika između kibervandalizma, kiberkriminala i kiberterorizma je motiv. Može se reći da kibervandali gotovo da i nemaju neki naročiti motiv, osim što teže osećaju zadovoljstva zbog neovlašćenog upada u neki informacioni sistem koji je teško probiti, jer je dobro obezbeđen. Dok su klasični kiberkriminalci vođeni motivima lične prirode, odnosno željom da ostvare korist (imovinsku ili neimovinsku) sebi ili nekom drugom, ili da nanesu štetu drugom licu ili nekoj instituciji zbog ličnih motiva. Kiberteroristi su vođeni političko-ideološkim motivima.

„*Tri vrste motivacija koje određuju delovanje određenih terorističkih grupa:*

1) Racionalna motivacija određuje ponašanje terorista u smeru da pre svega razmišljaju o svojim ciljevima i mogućnostima, analizirajući ih kroz prizmu „cene" koju moraju da plate i mogućeg dobitka.

2) Psihološka motivacija za sprovođenje terorističkih akata proizilazi iz ličnog nezadovoljstva teroriste sopstvenim životom i dostignućima.

3) Kulturna motivacija unutar terorističkih grupa snažno utiče na jedinstvo i oblikovanje ciljeva i vrednosti unutar terorističkih grupa. Kultura oblikuje vrednosti i motiviše ljude određene zajednice na način koji deluje nerazuman za posmatrače sa strane" (Jazić, 2010, 122-123).

Iako je najveći broj učinjenih terorističkih akata bio u znaku verskog fanatizma, „*osnovni cilj većine terorističkih grupa je nezavisnost i država*" (Jazić, 2010, 115). Nije nepoznato da određeni teroristički pokreti uživaju podršku neke države zbog filozofskih stavova koje zastupaju, a koji toj državi odgovaraju. Neretko su države finansirale terorističke operacije „*radi ostvarenja sopstvenih spoljnopolitičkih ciljeva ili na unutrašnjem planu radi jačanja sopstvene politike*" (Lutz & Brenda, 2004, 14-16). Tada govorimo o državnom terorizmu, odnosno kiber ratu (Stytz, 2006) kada teroristi primenjuju savremene informacione tehnologije radi postizanja viših ciljeva kojima se utiče na spoljno - političko ili unutardržavno stanje. „*Kiberteroristi obično imaju nameru da direktno ili indirektno demorališu civilno stanovništvo, što ga razlikuje od kiberrata koji nije direktno usmeren protiv civila*" (Brenner, 2007, 388).

Takođe je jedna od upečatljivih razlika između kiberkriminala i kiberterorizma ta što počinioci dela kiberkriminala nastoje da ostanu anonimni, neotkriveni, dok kiberteroristi kao i teroristi uglavnom žele publicitet i da izazovu strah što većih razmera. „*Načini na koje teroristi nastoje da ostvare željeni nivo publiciteta su:*

1) planiranje akcija koje treba da imaju veliki značaj u vestima;

2) sprovođenje aktivnosti koje treba da osnaže sopstvenu propagandu i regrutovanje;

3) odabir najpogodnijeg vremena i lokacije za privlačenje publicitita prilikom sprovođenja akcija;

4) izdavanje proglasa;

5) održavanje kontakata sa štampom i davanje izjava;

6) priznavanje odgovornosti za određene akcije

7) slanje poruka kroz značenje i simboliku mete ili akata“ *(Paletz & Schmid, 1992, 32).*

4.4. Veza između kiberterorizma i organizovanog kriminala

Globalizacija i naučne i tehnološke inovacije omogućili su da organizovani kriminal poprimi međunarodne dimenzije. Organizovani kriminal je kompleksna kriminološka pojava, koja se javlja u različitim oblicima od države do države. To značajno otežava definisanje ovog pojma, kao i činjenica da se organizovani kriminal različito tumači u nacionalnim zakonodavstvima.

„*Organizovani kriminal predstavlja dobro organizovanu kriminalnu organizaciju, sa strogom hijerarhijom, disciplinom, odgovornošću, lojalnošću i podelom zadataka, čiji je cilj ostvarivanje što većeg profita i legalizacija nezakonito stečene imovine, zahvaljujući postignutom stepenu društvenog ugleda, bilo na osnovu prodora u strukture vlasti ili uspostavljenih veza sa organima vlasti, državnim organima, legalnim poslovnim privrednim subjektima i uticajnim političkim partijama i strankama*“ (Bošković, 1998, 9). Abadinski smatra da je za razumevanje organizovanog kriminala neophodno pojmiti „*organizaciju grupe i njeno delovanje, koji po njemu predstavljaju suštinske delove ovog savremenog fenomena, pa tako navodi da je organizacija voljna da upotrebi nasilje ili da se služi podmićivanjem, radi ostvarivanja svojih ciljeva ili obezbeđenja discipline*“ (Abadinsky u Škulić, 2003, 38-39). Škulić navodi opšte uslove koji moraju da budu ispunjeni za postojanje organizovane kriminalne grupe: „*1) brojčani sastav – grupu moraju činiti najmanje tri lica; 2) odgovarajući vremenski kontinuitet – grupa mora postojati određeno vreme; 3) kriminalna ciljna usmerenost – grupa mora delovati sporazumno u cilju vršenja jednog ili više krivičnih dela za koje je propisana kazna zatvora od četiri godine ili teža kazna, te; 4) generalna svrha kriminalnog delovanja – grupa čini krivična dela radi: a) neposrednog ili posrednog sticanja finansijske ili druge koristi ili b) radi ostvarivanja i zadržavanja uticaja na privredne ili druge važne državne strukture*“ (Škulić, 2014, 2-3).

Sve do pojave narko terorizma pojmovi organizovanog kriminala i terorizma su tumačeni odvojeno. Šeli i Melcer na primeru dve studije slučaja krijumčarenja cigareta navode zajedničke karakteristike terorizma i organizovanog kriminala: „*finansiranje na nezakonit način, imaju sličnu organizacionu strukturu, služe se korupcijom i namenski organizuju svoje poslovanje u oblastima sa slabom kontrolom od strane državnih službi, koriste prednosti savremene tehnologije, iste tehnike za pranje i transfer novca, neretko i iste izvršioce*“ (Shelley & Melzer,

2008). Šmid takođe navodi nekoliko sličnosti između terorizma i organizovanog kriminala: „*racionalno obrazloženje, primena tehnika zastrašivanja, pretnje fizičkim nasiljem i upotreba sličnih taktika*“ (Schmid, 1996).

Uprkos sličnostima između terorizma i organizovanog kriminala i „*bez obzira na to što se u određenim situacijama isti subjekti bave i terorizmom i organizovanim kriminalom, „linija“ između ova dva vida kriminalnih delatnosti, kao i vičnosti, umišljaja i krivične odgovornosti izvršilaca krivičnih dela, jasna je i nedvosmislena*“ (Mijalković u: Šikman, 2011, 51). Iako organizovani kriminal, kao i međunarodni terorizam karakteriše mrežna struktura i ostale prethodno navedene sličnosti: „*Da bi određena grupa predstavljala organizovani kriminal mora da zadovolji određene kriterijume kao što su: neideološki karakter, hijerarhijska ustrojenost, ograničeno ili ekskluzivno članstvo, trajan karakter, upotreba nasilja i podmićivanja, zastupljenost specijalizacije članstva i podele rada, posedovanje monopola i da se funkcionisanje zasniva na eksplicitnim, internim pravilima*“ (Abadinsky, 2003, 2-3). Upravo su neki od pomenutih kriterijuma ono što razlikuje organizovani kriminal od terorizma.

Terorizam, takođe ima međunarodni karakter, ali ono po čemu se razlikuje od organizovanog kriminala je njegov ideološko-politički karakter. Dok je primarni cilj organizovanog kriminala „*sticanje profita i moći pojedinačno ili u celini*“ (Savona, Adamoli, Di Nicola & Zoffi, 1998, 6) odnosno sticanje koristi na nezakonit način. Jer je „*organizovani kriminalitet neideološko udruženje jednog broja lica, koje među sobom ostvaruju vrlo bliske društvene interakcije, organizovano u hijerarhijskoj osnovi, od najmanje tri nivoa-ranga, a sa ciljem obezbeđenja profita i moći, zahvaljujući učešću u nezakonitim i zakonitim aktivnostima*“ (Abadinsky, 1994, 38). Kriminalne grupe koje pripadaju organizovanom kriminalu sprovode međunarodne aktivnosti kojima krše međunarodne regulative i prevazilaze nacionalne granice, što znatno smanjuje eksternu kontrolu nad njihovim aktivnostima i otežava njihovo otkrivanje od strane bezbednosnih službi.

Dodirna tačka između terorizma i organizovanog kriminala je kao što navode Mijalković i Bošković (Mijalković & Bošković, 2009) finansiranje terorizma, odnosno „*prljavi novac*“. Kada je reč o organizovanom kriminalu „*najveća dobit se ostvaruje trgovinom narkoticima, pranjem novca, trgovinom oružjem ili organizovanim krađama*“ (Petrović, 1998, 37-39).

Terorističke organizacije su u tesnoj vezi sa ostalim kriminalnim delovanjem, jer na taj način pribavljaju materijalna sredstva koja su im neophodna za realizaciju planiranih terorističkih aktivnosti. Dakle, teroristi vrše najteža krivična dela kako bi pribavili korist za sebe ili organizaciju kojoj pripadaju i time nanose štetu pojedincima – bogatim civilima i pravnim licima (banke, kompanije, menjačnice, pošta, zlatare i dr.), nude usluge reketiranja, bave se krijumčarenjem ljudi i droge i slično. Teroristi se vodi različitim interesima ekonomskim, pravnim i dr. Ali, nesumnjivo ono što određuje ovaj oblik međunarodnog organizovanog kriminaliteta je to što je on prevashodno politički obojen. „*Kriminalna organizacija da bi mogla da opstane nužno mora da koristi nasilje ili neka druga sredstva poput zastrašivanja, kao i da uspostavi spregu sa državnim, političkim, ekonomskim i finansijskim subjektima, bilo korupcijom, ucenom, iznudom ili nekim drugim načinom*“ (Bošković, 1998, 53). Terorizam je uglavnom u sprezi sa nekom državom, njenim organima ili uživa zaštitu neke političke partije kojoj pomaže da se domogne ili održi na vlasti, a čiji se interesi zasnivaju na iredentističkim i separatističkim težnjama.

Povećana upotreba digitalnih uređaja i eksponencijalni rast snage i mogućnosti koje primena računara pružaju ukazuju da će većina budućih zločina da sadrži kiber komponentu. To se odražava i na organizovani kriminal. Savremena tehnološka dostignuća predstavljaju osnovna sredstva za ostvarenje komunikacije i organizovanje kriminalnih aktivnosti, a nekada su i osnovna sredstva za njihovo izvršenje.

Tabela 9. Procenjena distribucija učinjenih krivičnih dela koje sadrže kiber komponentu (Davis, 2012, 277).

Prekršaj	%
Prevara / falsifikovanje / krađa	79.3
Krivična pretnja	8.5
Online zloupotreba maloletnika / dečja pornografija	4.9
Kiber napadi / kiber *squatting*	1.9
Ostalo	1.8
Nasilni kriminal	1.3
Krijumčarenje droge	1.0

Napomena: Zbog zaokruživanja odgovori anketiranih ne sadrže ukupno 100 %

Otuda Koreja i Bovling (Correia & Bowling, 1999) navode da je XXI vek početak nove ere izazova za pronalaženje i sprovođenje adekvatnih zakona.

Tabela 10. Procentualno prikazani problemi koji otežavaju istragu krivičnih dela sa kiber komponentom (Davis, 2012, 278).

Problem	1	2	3	4	5	Prosek
Nemogućnost praćenja komunikacija na internetu	8,8	8,0	16,0	26,4	40,8	3,82
Oskudna obuka	9,5	8,7	24,4	26,0	30,7	3,60
Javna apatija / nedostatak svesti	10,3	12,7	31,7	27,8	17,5	3,29
Pitanja nadležnosti	15,9	19,8	24,6	16,7	23,0	3.11
Nedostaci razmene informacija / obaveštajnih podataka	9,6	27,2	25,6	23,2	14.4	3.06
Nedostatak tehničke stručnosti zbog smene zaposlenih	32.5	17.5	16.7	15.9	17.5	2.68
Nedostatak standardnih operativnih procedura	21.8	21.0	34.7	13.7	8.9	2.67
Napomena:	1- u potpunosti se ne slažem, 5- u potpunosti se slažem					

Pored prethodno navedenih karakteristika koje doprinose da se dela računarskog kriminaliteta teško otkrivaju i dokazuju, efikasno suprostavljanje kiberkriminalu otežava:

1) tamna brojka - od ukupnog broja učinjenih delikata u kibernetskom prostoru samo mali procent se prijavljuje, odnosno evidentira kod nadležnih organa;

2) nedovoljna informisanost i poznavanje ove vrste kriminala;

3) relativno nov pojam;

4) informaciono-komunikaciona tehnologija i njen razvoj nisu podjednako dostupni u svim državama (razvijene zemlje imaju bolje mogućnosti i pristup najsavremenijim tehnološkim inovacijama)

5) kiberkriminal izmiče strogom teritorijalnom određenju, jer nije usko vezan za teritoriju, kao tradicionalni oblici kriminala, odnosno odlikuje ga transnacionalnost;

6) prostorna prikrivenost – otežano prostorno određenje obzirom da se kiberkriminal dešava u *online* okruženju (kibernetskom prostoru), lako prevazilazi prostorne granice i kao takav kiberkriminal je teško uhvatljiv i uočljiv;

7) vremenska prikrivenost – mogućnost vršenja krivičnog dela velikom brzinom. Od momenta izvršenja krivičnog dela do ispoljavanja posledica po žrtvu (fizičko ili pravno lice) može i ne mora da postoji vremenska distanca;

8) prikrivenost zbog različitih motiva – na primer očuvanje reputacije je najčešći motiv prikrivanja kiberkriminalnih radnji kod privrednih subjekata koji posluju putem elektronskog bankarstva, trgovine i sl.

Funkcionisanje i održavanje složenih kriminalnih sistema, kao što su organizovani kriminal i terorizam praktično je nemoguće bez podrške informacione tehnologije koja je ujedno značajno sredstvo za izvršenje i otkrivanje kriminalnih dela. Prethodno navedene otežavajuće okolnosti za otkrivanje kriminalnih dela koja sadrže kiber komponentnu i ostale pogodnosti koje savremene tehnologije pružaju, sasvim očekivano čine da veze između organizovanog i kiberkriminala u budućnosti rapidno rastu.

5. BORBA PROTIV KIBERTERORIZMA

5.1. Tri faze odbrane od kiberterorizma

Nisu sve države, institucije i organizacije podjednako digitalizovane, što znatno utiče na verovatnoću napada. Velike kompanije su češće mete napada jer za svoje svakodnevno poslovanje koriste velike računarske mreže, pa samim time ostavljaju više prostora za napad. Jer, što je sistem kompleksniji, onda je potencijalno ranjiviji.

Bezbednost i odbrana računarskih sistema su pitanja od prioritetnog značaja, obzirom da se savremeno društvo umnogome oslanja na rad i podršku informaciono-komunikacionih infrastruktura. Pitanje kiber bezbednosti kao što primećuju mnogi autori (Kizza, 2009, 45-46; Solange, 2009, 3) uglavnom podrazumeva zaštitu resursa (materijalnih i/ili nematerijalnih) od eventualnih opasnosti. Međutim, ovo pitanje se sve više odnosi na očuvanje života ljudi i održavanje međunarodnog mira, jer se posledice napada nastalog u kibernetskom prostoru lako prenose u realnost i direktno utiču kako na živote ljudi, tako i na stanje u pojedinim državama i međunarodne odnose. Dakle, razmere potencijalne štete variraju od: kratkotrajne obustave svakodnevnih aktivnosti, pričinjavanja značajne ekonomske štete, kolapsa (u saobraćaju, trgovini, na berzi) pa sve do katastrofa sa velikim brojem ljudskih žrtava.

Pričinjena šteta zavisi od nekoliko faktora: samog napadača - njegovih ciljeva i motiva, sposobnosti i resursa (znanja, alata) kojima raspolaže, kao i od postojećeg sistema odbrane mete napada. Obzirom da na karakteristike napadača ne možemo da utičemo, ono što ima presudnu ulogu je snažna i efikasna odbrana. Međutim, „*Kratka ocena naših ukupnih sposobnosti da se bavimo teroristima koji koriste kibernetski prostor bi zaključili da smo u većini potencijalnih ciljeva tehnološki i proceduralno slabi u svakom pogledu tri faze kiber odbrane od kvalifikovanih, strpljivih i postojanih napadača koje verovatno neće biti lako zaustaviti*“ (Goodman, 2007, 50). Imajući u vidu veliku brzinu kojom se tehnologija razvija i nove inovacije primenjuju, pred službama kiber zaštite i odbrane je težak zadatak da te promene isprate i održe isti tempo razvoja. Kada govorimo o odbrani od kiberterorizma Gudmen se zalaže za „*tri faze odbrane:*

1) *Prevencija*;

2) *Upravljanje incidentom, ublažavanje napada, ograničenje štete*;

3) *Upravljanje posledicama*“ (Goodman, 2007, 46).

Odbrana od kiberterorizma je problematična. Praćenje aktivnosti u kibernetskom prostoru je otežano zbog široko omogućenog pristupa velikom broju korisnika. Unutar računarskih sistema korisnici se međusobno masovno povezuju zbog najraznovrsnijih potreba i motiva. Pitanje zaštite računarskih mreža je takođe problematično, obzirom da su tehnike zaštite i sredstva korak iza napada i teško mogu da prate dinamiku inovacija napadača. Napadači svoje napade uglavnom baziraju na otkrivanju „*rupa u sistemu*“. Sledeći problem su insajderi, odnosno saučesnici u kriminalnim aktivnostima koji su omogućili pristup potencijalnim zloupotrebama pa su samim time delom odgovorni za pričinjenu štetu. Takođe, unutarorganizacijska mobilnost i saradnja sa spoljnim saradnicima otežavaju odbranu i praćenje aktivnosti u ovom segmentu. Još jedna otežavajuća okolnost je ta što teroristi u kibernetskom prostoru lako mogu da sakriju svoj stvarni identitet formiranjem lažnog online profila; zahvaljujući tome imaju mogućnost da se infiltriraju među ostale sve do momenta izvršenja napada. Obzirom da ova vrsta kriminala ostaje velikim delom neprijavljena, nedovoljno sredstava se izdvaja za rešavanje potencijalnih pretnji i problema. Pomenute poteškoće treba da podstaknu razvoj novih mera odbrane od kiberterorizma.

5.1.1. Prevencija

Može se reći da je prevencija samo jedna od faza odbrane, ali veoma značajna obzirom da predstavlja prvi korak u odbrani od kiberterorizma. Mnogi informaciono-tehnološki sistemi dizajnirani su tako da na što bolji način pruže traženu uslugu / proizvod svojim korisnicima, dok njihovoj zaštiti nije posvećena posebna pažnja. Kiberterorizam za razliku od ostalih oblika kiberkriminala ima za cilj da pričini štetu što je moguće većih razmera. Usled velike dinamike razvoja tehnoloških dostignuća i inovacija, sa aspekta bezbednosti i odbrane gotovo da je nemoguće pratiti razvoj savremenih tehnologija i ići u korak sa njima ne bi li se pružile adekvatne mere zaštite.

Razni autori prednost daju metodu predviđanja kiber napada, te navode da u tome značajno mogu da posluže ključni podaci, kao što su:

„1) *Motivacija, omogućava predviđanje najverovatnijeg cilja kiber napada;*

2) Mogućnost za izvršenje, omogućava determinisanje najverovatnije vrste kiber napada;

3) *Vreme, predviđanje tačnog vremena kada bi se desio kiber napad*“ (Yuji & Munkhdorj, 2017, 110).

Dejvis takođe smatra da su „*prevencija i svest ključni elementi u smanjenju prevalencije devijantnih akata, naročito u borbi protiv kompjuterskog kriminala*“ (Davis, 2012, 278). Dok, Klajn predlaže „*holističku strategiju prevencije*“ (Klein, 2018) koja uključuje sva sredstva, odnosno integriše vojni i ne-vojni pristup. Dakle, sveobuhvatna strategija prevencije podrazumeva da se vojne i ne-vojne aktivnosti sprovode udruženo u cilju prevencije kiberterorizma „*odvraćanjem* i *odgovaranjem*“ potencijalnog protivnika da izvrši delo kiberterorizma (Klein, 2018, 29).

„*Odvraćanje (Deterrence)*“ – „*Uprkos ograničenjima da se utiče na donošenje odluka potencijalnih napadača i njihovih lidera, odvraćanje ostaje održiv koncept za prevenciju kiberterorizma*“ (Klein, 2018, 30). Mnoge terorističke organizacije, uključujući Al-Kaidu i Islamsku državu karakteriše strateško i racionalno funkcionisanje. Zbog toga je odvraćanje još uvek relevantno kada govorimo o strategijama odbrane od kiberterorizma.

Sve dok se principi vojne nužnosti i zakonska regulativa pažljivo razmatraju, i vojni i ne-vojni odgovori su održive opcije. Na uspešnost strategije odvraćanja umnogome utiče percepcija potencijalnog neprijatelja. Odvraćanje je jače ukoliko postoji verodostojna pretnja sile i neprihvatljive posledice po napadače koje im sleduju nakon bilo kakve vrste kiber napada. Dakle, održavanje stalnih i agresivnih operacija protiv dela kiberterorizma je preduslov dobre prevencije. Na primer, ukoliko Islamska država ili rukovodstvo Al-Kaide smatraju da će, nakon čina terorizma biti izloženi sistematičnim vojnim ili ne-vojnim intervencijama koje prete da ugroze njihov opstanak i bazu moći, takva percepcija ih odvraća od kibernapada koji su pretnja po život.

U svojoj osnovi, strategija odvraćanja od kiberterorizma je uticaj na neprijatelja i njegovo uveravanje da štetnost posledica nakon izvršenja kibernapada nadvladava potencijalne koristi. Tokom vremena upotrebljavaju se različite vrste odvraćanja. Iako postoje brojne podvrste, izdvajaju se dve glavne strategije odvraćanja: „*odvraćanje kaznom i odvraćanje odbijanjem*“ (Iasiello, 2018, 36).

„*Odvraćanje kaznom*“ - uveravanje napadača o značaju kazne i odmazde za učinjen napad. Ovakav scenario odmazdu ne ograničava na specifične akcije, odnosno podrazumeva uključivanje i drugih sredstava kao što su kinetičke i ekonomske sankcije. Kao dobar primer može da posluži doktrina Hladnog rata u kojoj je pretnja upotrebe nuklearnog oružja sprečila nameru protivnika da upotrebi slično oružje. Ovaj princip, odvraćanje kaznom možemo da primenimo u kibernetskom prostoru, gde odmazda ima oblik digitalnih postupaka kao što su kibernapad koji je usmeren protiv potencijalnih počinioca kiberterorizma, ili preduzetnički udar koji izaziva kolaps i onesposobljava funkcionisanje neprijateljske mreže. Veruje se da su SAD stajale iza napada Stuksnet virusom (*Stuksnet*) koji je bio usmeren na iranske nuklearne programe koji su se bavili istraživanjem uranijuma. Virus je izazvao značajan zastoj u radu i razvoju. Navedeni događaj je dobar primer „*strategije odvraćanja kaznom*“ u pomenutom slučaju SAD protiv Irana.

„*Odvraćanje odbijanjem*“ je manje konfliktna strategija koja se zasniva na pokušajima da se potencijalni napadači ubede da će uprkos uloženim naporima ostati uskraćeni za koristi koje očekuju od napada. Ova strategija predstavlja tradicionalno defanzivnu formu, koja kada se primenjuje u kibernetskom prostoru podrazumeva obeshrabrivanje ili frustriranje neprijatelja upotrebom robusne, proaktivne i skupe odbrane, tako da odnos uloženog i dobiti za napadača

imaju negativnu računicu. Primena ove strategije zahteva snažnu fokusiranost i posvećenost vlade, velika materijalna ulaganja i saradnju sa privatnim sektorom kako bi se osigurali sistemi i mreže i stavili pod njenu kontrolu. Korišćenje naprednih bezbednosnih praksi i usvajanje pouzdanih komponenti hardvera i softvera iziskuju velika ulaganja i kontinuirano praćenje tehnološkog razvoja. Uspešnost strategije odvraćanja od kiberterorizma zavisi od nekoliko faktora: „*komunikacija, signalizacija, pripisivanje i proporcionalnost*“ (Iasiello, 2018, 37-41). Ukoliko neki od pomenutih faktora nije ispunjen postoji rizik da neprijateljstvo eskalira državnim sukobom zbog nesporazuma ili pogrešnog tumačenja.

Efikasna komunikacija sa međunarodnom zajednicom, a naročito protivnicima, je jedan od preduslova i pitanje kredibiliteta jedne države nacije, koja mora da poznaje granice, odnosno „*crvene linije*“ koje se ne prelaze, kao i u kojim slučajevima ih je potrebno preći. Dakle, efektivna komunikacija zahteva postojanje konsenzusa o operativnim normama ponašanja u kibernetskom prostoru za šta je potrebno uložiti veliki napor. Sjedinjene Američke Države i Kina nisu uspele da pronađu zajednički jezik u strateškom i ekonomskom dijalogu u julu 2013. godine. SAD zbog fokusa na tehnologije i mreže automatizovanih mašina preferiraju korišćenje termina „*cybersecurity*“- kiber bezbednost, dok zemlje poput Kine i Rusije preferiraju korišćenje šireg pojma „*information security*“- bezbednost informacija (Farnsworth, 2011). Kina i Rusija se zalažu za širu interpretaciju koja uključuje i tehnologije i informacije koje postoje i razmenjuju se na mreži, kako bi povećali kontrolu sadržaja i informacija kojima njihovo građanstvo ima pristup, dok SAD podržavaju politiku slobode interneta. Bez zajedničkog jezika, dve strane ostaju u neslaganju i ne uspevaju da postignu konsenzus o tome kako bi internet trebalo koristiti na odgovarajući najbezbedniji način. Slabosti u komuniciranju otežavaju slanje jasnih poruka u kibernetskom prostoru što može da poveća tenzije.

Signalizacija se primenjuje duže vreme u oblasti međunarodne politike, pregovorima u ratu, krizi, kao i međunarodnim ekonomskim pregovorima (Walsh, 2007, 441). Bez obzira kada se primenjuje, u miru ili ratu, ključni element bilo koje strategije kiberodvraćanja uključuje sposobnost da se namere pravilno prikažu i odašilju do željenog prijemnika. Bez mogućnosti signaliziranja povećava se rizik pogrešnog shvatanja ili tumačenja, što strategiju „*odvraćanja kaznom*“ može da učini neefikasnom. Na primer, pre izvršenja strategije „*odvraćanje kaznom*“, država koja se brani mora jasno da signalizira svoje nezadovoljstvo agresoru tako da ga on pravilno tumači i razume da potencijalni troškovi za preduzimanje određenog kibernapada

daleko prevazilaze potencijale prednosti. Dalje, da bi signalizacija bila efikasna država mora da ima uspostavljeno radno telo koje verodostojno sprovodi uspešnu i destruktivnu kiberodmazdu. Ukoliko protivnik ne veruje u kredibilitet države, signalizacija ne može da bude uspešna. Kao i komunikacija, signalizacija u kibernetskom prostoru može lako da se pogrešno interpretira, ignoriše ili čak ne primeti od strane agresora. Signalizacija može da se sprovodi otvoreno, prikriveno ili putem diplomatskih, ekonomskih ili vojnih kanala.

Pripisivanje odgovornosti u kiberprostoru je izuzetno teško jer kiberprostor pruža mogućnosti svojim korisnicima da prikriveno deluju. „*Spektar odgovornosti države -spectrum of state responsibility*“ (Healey, 2012) je specijalno dizajnirana alatka koja služi da pomogne analitičarima da pripišu odgovornost za određeni kibernapad sa preciznošću i transparentnošću na osnovu deset kategorija, gde je svaka od njih obeležena različitim stepenom odgovornosti. Da bi se identifikovali agresori u kiberprostoru, tehnička analiza nije dovoljna s obzirom na činjenicu da mnogi neprijateljski akteri sprovode istu taktiku, tehnike i procedure, koriste iste alate, ili se bave sličnim operacijama za sprovođenje zlonamernih aktivnosti. Dakle, „*iako su tehnički podaci korisni za određivanje nivoa veština i TTP-a (tehnološke taktike, tehnike i procedure) kiber napadača, oni su delimično delotvorni za pripisivanje, jer ne uzimaju u obzir ponašanje, osobine, namere, motivacije ili želje aktera, niti pružaju predviđanje budućih napada i ciljeva*“ (Iasiello, 2012, 5). Jasielo navodi ograničenja pomenute tehnike pripisivanje dela kiberterorizma počiniocima: „*pripisivanje sa zakašnjenjem*, *neuspelo pripisivanje* i *odsustvo pripisivanja*“ (Iasiello, 2012, 5-6).

„*Pripisivanje sa zakašnjenjem - Tehnička analiza zahteva vreme. Potrebno je da se utvrdi da li je incident stvarno zlonameran, zatim da se identifikuje računar sa kojeg je proistekla maliciozna aktivnost (poznato je da počinioci koriste botnete - mrežu kompromitovanih računara koje kontroliše počinioc). Pomenuta procedura traje, odlaže se na neko vreme kako bi se prikupili svi podaci, što ostavlja prostora napadaču da može da pobegne, odnosno nestane pre nego što mu se pripiše zločin.*

Neuspelo pripisivanje - Zbog ograničenih sposobnosti tehničke opreme, ljudske greške ili stučnosti počinioca, tehnička analiza nije uvek u mogućnosti da obezbedi uspešnu identifikaciju počinioca.

Odsustvo pripisivanja - Brojni razlozi mogu da dovedu do pogrešne identifikacije

lokacije ili identiteta počinioca: neispravan softver, neispravni podaci, nejasni ili pogrešno tumačeni podaci“ (Iasiello, 2012, 5-6).

Proporcionalnost u kibernetskom prostoru - pričinjena šteta kiberterorističkim napadom treba da bude srazmerna kazni. Praktično je teško to postići iz raznih razloga. Kada nacionalna država deluje nezavisno od jedne ugledne međunarodne organizacije kao što su Ujedinjene nacije, rizikuje da ugrozi diplomatske, čak i ekonomske odnose. Zbog toga je potrebno da pre donošenja odluke o odmazdi, koja može da bude kibernetičkog ili ne-kibernetičkog oblika, dobro proceni posledice i potencijalnu štetu i projektuje ponašanje međunarodne zajednice.

„*Odgovaranje* (*Dissuasion*)“ – „*Osim odvraćanja drugi deo holističke strategije prevencije je odgovaranje, odnosno nastojanje da se utiče na rukovodstvo potencijalnih neprijatelja tako što se obeshrabruju inicijative vojnih nadmetanja*“ (Klein, 2018, 30). Postupak odgovaranja je delotvoran pre nego što se pretnja manifestuje. Jer, odgovaranje uključuje „*aktivnosti oblikovanja*“, koje su tipično ne-vojne po svom obimu i sprovode se u miru, odnosno jedino izvan potencijalne opasnosti od vojne akcije. Strategija koja uključuje odvraćanje usmerena je na prikazivanje kibernapada kao beskorisnog.

Bosler i Holt su sproveli istraživanje da predstave percepciju policije o njihovoj trenutnoj sposobnosti da odgovore na dela kiberkriminala i prikažu predloge za poboljšanje društvenog odgovora na kiberkriminal. Navode:

1) „*korisnici interneta treba da budu pažljiviji kada koriste internet,*

2) *teže kazne za kiberkriminalce*

3) *teža krivična gonjenja za kiberkriminalce*

4) *jasnije zakonodavstvo protiv kibernetičkog kriminala bi povećalo uspešnost gonjenja i istrage*

5) *specijalni forenzički alati i tehnologije*

6) *povećanje sredstava za obuku agencija koje su u službi zakona*

7) stvaranje bolje saradnje između države i saveznika po pitanju kiberkriminala

8) *rad sa provajderima (npr. AOL) kako bi se nadgledao internet*

9) *bolja edukacija javnosti u vezi sa kiberkriminalom*

10) *saradnja sa poslovnom zajednicom radi poboljšanja izveštavanja i istraživanja kriminala*

11) *namenski strukturirane lokalne jedinice za kibernetički kriminal*

12) *bolje metode za otkrivanje kibernetičkog kriminala*

13) *više računarskih obuka za službenike*

14) *povećanje menadžmenta kako bi se razvilo praćenje na reginalnom nivou*

15) *rad sa građanima*“ (Bossler & Holt, 2012, 175).

Pomenuti predlozi primenljivi su i kada je u pitanju prevencija kiberterorizma. Dakle, potrebno je da se javni i privatni sektor zajedno angažuju i sarađuju na ostvarivanju kiber bezbednosti, udruženo primenom različitih metoda odbrane. Odnosno, potrebno je da se kompanije iz privatnog sektora koje tesno sarađuju sa državnim vitalnim strukturama, kao što su privatne bezbednosne agencije, fondacije za ostvarivanje građanskih prava i dr. značajnije uključe i informišu o pretnjama od kiberterorizma, kao i o drugim vrstama kiberkriminala. Kao primer dobre prakse može da posluži Holandija. Na primer, organizacija *Nederland ICT* okuplja nešto više od 550 informaciono-komunikaciono tehnoloških kompanija, među kojima su neke od vodećih u Holandiji (*Microsoft*, *Google Holandija*, *UPC*, *CGI Holandija*, *KPN IT Solutions*) i poseduje svoju savetodavnu grupu eksperata koja se bavi problemima i razvojem kiber sigurnosti.

Dobra prevencija podrazumeva:

- usaglašavanje propisa i kažnjavanja dela kiberterorizma na međunarodnom nivou
- razvoj istraživačkih jedinica za kibernetički kriminal na lokalnom nivou
- dobra koordinacija privatnog i javnog sektora
- primena određenih standarda, postupaka i procedura radi bolje bezbednosti sistema
- preduzimanje određenih mera zaštite (redizajniranje postojećih sistema, fizičko ili kiber presretanje napada, prisluškivanje, postavljanje senzora i dr.)
- primena različitih tehnika (*firewalls* i *password* kao filteri za korisnike kojima je dozvoljen pristup, tajni ili javni ključ za šifrovanje, različiti sistemi za otkrivanje upada i dr.)
- planiranje (finansijsko, edukacija, istraživački projekti za iznalaženje novih tehnologija odbrane i zaštite).

5.1.2. Suočavanje sa kiberterorističkim napadom

Da bi informaciono-komunikacione strukture funkcionisale neophodno je postojanje dva ključna elementa: fizički – oprema (mašina) i ljudski element – koji sprovodi nekoliko tehnoloških postupaka i zadatih naredbi koje se ispisuju programskim jezikom uz upotrebu odgovarajućih programerskih alata. Dakle, računarski sistemi funkcionišu automatizovano, tako što ga pravilno zadata funkcija pokreće ili zbunjuje - nanosi štetu ili unosi u njega neispravan kod za „*loše*“ funkcionisanje.

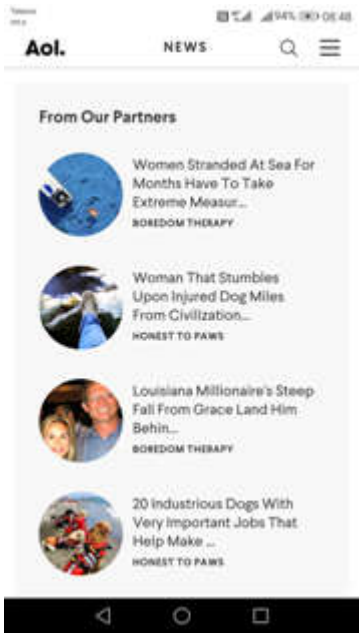
Kako bi se opasnost po računarske sisteme svela na minimum najpre je neophodno stvoriti zaštitu, odnosno neku vrstu barijere, pomoću koje će se organičiti ili onemogućiti pristup „*spoljnim*“ neautorizovanim korisnicima da manipulišu podacima i izvode malverzacije. To se najčešće postiže postavljanjem određenog sistemima lozinki (*password*) ili *firewall* kojima se ograničava pristup na autorizovane korisnike. Takođe, od velike važnosti je postavljanje senzora koji služe da pravovremeno detektuju napad i upozore da je napad otpočeo. Prema navodima Džančevski i Kolarika (Janczewski & Colarik, 2008, 274-276) zbog velike količine podataka, nemoguće je kontrolisati celokupan protok informacija, zato je važno postaviti sisteme za nadgledanje na odgovarajuće mesto. Ovi sistemi pomoću kojih se nadgleda internet saobraćaj mogu da obavljaju različite funkcije (prikupljanje podataka, snimanje, njihovo filtriranje i alarmiranje u slučaju napada).

Kibernapad se najčešće otkriva metodama koji prate signale i detektuju anomalije. Dok se odbrana, odnosno određeni sistem protivmera u ovakvim slučajevima primenjuje protiv predstojećeg kibernapada jedino u slučaju njegovog detektovanja. Tehnike otkrivanja kibernapada i kontramere se usavršavaju u skladu sa do sada poznatim, odnosno otkrivenim metodama za izvođenje kibernapada. Postojeći sistemi zbog svojih ograničenja, nisu više u mogućnosti da otkriju sve kibernapade sa visokim stepenom preciznosti i tačnosti. Zato u većini slučajeva administratori sistema ni ne primete da su bili izloženi napadu ili pokušaju napada. Dakle, kibernapad postaje otkriven, tek kada je pričinjena značajna šteta koja ne može da prođe neopaženo. Upravo zbog toga sistemi odbrane nisu dovoljno pripremljeni na predstojeće napade kiberterorista.

Napadači najčešće koriste *feed*-ove - vrsta javnih domena koji podrazumevaju više tehničkih aspekata za razliku od uobičajenih društvenih podataka, vesti. To je određeni sled

sadržaja koji se često ažurira na računaru ili mobilnom telefonu kroz koji možemo da se „*krećemo*“. Sadržaj se prikazuje u sličnim blokovima koji slede jedan drugog. Kao primer može da posluži izgled mreže na računaru koji se pretvara u *feed* ili izgled pregledavanja na mobilnom uređaju.

Slika 5. Primer *feeda* koji sadrži tekst i slike (Aol News, 8.11.2018)



Brojni autori predlažu upotrebu *fedd*-ova za predviđanje mogućih kibernapada ili određene vrste napada (Holm, Ekstedt &Andersson, 2012, 825-837; Bollen, Mao & Zeng, 2011, 1-8). *Twitter feed*-ovi mogu da budu dobar izvor za prikupljanje informacija o kibernapadima. Bolen i saradnici pretpostavljaju da se neke promene koje su usmerene protiv žrtve napada u kibernetskom prostoru dešavaju neposredno pre izvršenja samog napada. Otuda predlažu sledeće postupke za njegovo predviđanje:

„*1. Prikupljanje arhive kiberincidenata koji su se dogodili u prošlosti korišćenjem feed-ova“*

2. Prikupiti izvore ranjivosti koji su eksploatisani u incidentima. Sakupljanje društvenih izvora (članci, vesti, tvit-ovi) koji se odnose na svaku žrtvu u arhivi.

3. Detektovati obrasce koji se ponavljaju posmatrano iz uglova ugroženosti. Otkrivanje nekog obrazca upoređivanjem društvenih izvora sa žrtvom, koji su objavljeni neposredno pre napada pomoću feed-a i onih koji su objavljeni u drugim periodima.

4. Obučiti model za učenje mašina na uzorku otkrivenom u prethodnom koraku

5. Unos dnevnih društvenih sadržaja u obučeni model i provera da li se šablon pojavljuje u dnevnim izvorima. Otkriveni uzorak u petom koraku će biti rezultat predviđanja“ (Bollen, Mao & Zeng, 2011, 119). Za predviđanje kibernapada može da posluži i potencijalna motivacija za njegovo izvršenje (Munkhdorj & Yuji, 2017).

Zarad postizanja sigurnosti administratori mreže treba da automatizuju analizu dnevnika kako bi prepoznali napade koji su u toku ili trendove koji ukazuju na pokušaje upada. Na primer, niz neuspelih pokušaja prijavljivanja može da ukaže na to da neko pokušava da pogodi lozinku i dobije neovlašćeni pristup mreži. Administratori mreže su zaduženi za njenu bezbednost, te je većina njih dobro upoznata sa rizicima i preduzimaju čvrstih mera kako bi sprečili napade na njihove mreže i računare.

Gudmen (Goodman, 2007, 49) smatra da organizacije treba da kreiraju sopstvene sigurnosne politike i planove odbrane koje pokrivaju širok spektar mogućih kibernapada koji predstavljaju potencijalni rizik za organizaciju. Takođe smatra da su veoma korisne praktične vežbe, ali ih organizacije uglavnom izbegavaju jer su skupe i uznemiravajuće jer su mnogi informacioni sistemi delikatni, pa se njihovi vlasnici plaše da će nešto poći naopako.

5.1.3. Saniranje posledica – ublažavanje i ograničavanje

Suočavanje sa kiberterorističkim napadom ne znači samo pomenute mere zaštite i njegovo otkrivanje, nego i upravljanje posledicama napada, tako da se one: što je moguće više ublaže i ograniče, pričinjena šteta svede na minimum, zaštite resursi i informacije, povrati što veći broj podataka (*backup*, *recovery* funkcije) i prikupi što je moguće više informacija o izvršenom napadu (revizorske funkcije) kako bi se otkrili počinioci i predupredili napadi te vrste u budućnosti.

Nakon kiberterorističkog napada u ovoj fazi odbrane postoje dve primarne procedure odbrane: „*oporavak (recovery) i odgovor response (response)*“ (Goodman, 2007, 50).

„*Postupci koji spadaju pod oporavak:*

- *uklanjanje ili zatvaranje neprijateljskih entiteta*
- *procena štete šta je slomljeno ili izmenjeno, a šta nije*
- *automatski procesi za procenu i brzu i efikasnu racionalizaciju onoga što je ostalo*
- *utvrđivanje prioritetnih funkcija koje treba da se rekonstruišu*
- *vraćanje na stanje pre napada bez uništenja dokaza*“ (Goodman, 2007, 50).

Dobro planirani i pažljivo izvršeni napadi, kao što su korumpiranje podataka ili zlonamerni kod su najveći izazovi za oporavak. Jer, organizacija može duži vremenski period da bude izložena zamaskiranom, netransparentnom napadu, što znatno otežava *back up* i pronalaženje odgovarajuće rezervne kopije podataka, i otkrivanje svih štetnih transakcija. Oporavak se odnosi na pasivni oblik odbrane, jer podrazumeva rekonstituciju oštećenog IT sistema napadom, kako bi se organizacija što pre je moguće osposobila za uobičajeno funkcionisanje. Dok, odgovor (*response*) podrazumeva aktivni oblik odbrane. Jer se odnosi na identifikaciju i kažnjavanje počinioca kiberterorističkog napada, i potpunije informisanje o opasnostima na osnovu pređašnjeg iskustva zarad efikasnije odbrane i zaštite od pomenute vrste napada u budućnosti.

Odgovor (*response*) podrazumeva sledeće postupke:

- „*pronalaženje pravog krivca: snažni precizni tragovi i forenzički alati, neka vrsta "otiska prsta"*

- izmerena odmazda: pravni principi i proporcionalne odmazde

-asimetrije: šta učiniti o napadačima sa malo IT sredstava ili ranjivosti?

-eskalacija: procena štete kako bi odlučili da li želimo da pošaljemo jaku poruku“ (Goodman, 2007, 50).

5.2. Mere odbrane od kiberterorizma

Kiberterrorizam treba istraživati kao i bilo koji drugi slučaj koji uključuje digitalne dokaze. Odnosno, kako bi prikupljeni digitalni dokazni materijali bili prihvatljivi na sudu moraju da zadovoljavaju određene forenzičke standarde i protokole, koji se primenjuju za identifikaciju, pribavljanje, raspolaganje i ispitivanje elektronskih dokaza kako na nacionalnom, tako i na međunarodnom nivou. Ovo je naročito važno, jer istraživanje i rešavanje slučajeva kiberterorizma podrazumeva pored angažovanja državnih (nacionalnih) sudova i uključivanje tribunala i međunarodnih sudova i institucija.

Kiberteroristi se služe različitim tehnikama kako bi zamaskirali svoj identitet i ostali anonimni. Pomoću proksi servera sakrivaju *IP* adrese. Takođe sakrivaju korake kojim je napad izveden i služe se falsifikovanim *IP* adresama. Pomenute radnje im obezbeđuju značajnije nivoe anonimnosti, koji otežavaju ulazak u trag počiniocima kiberterorizma. Nivo veština počinioca se ne može lako proceniti, obzirom da datoteke koje su odabrane zbog svoje ranjivosti za izvođenje kibernapada ne zahtevaju upotrebu složenih hakerskih veština i alata za njihovu eksploataciju. Tehnička analiza ima svoja ograničenja i ne može da prodre dublje tako da pruži odgovore na pitanja: zašto je napadač odabrao specifični računar; koji je nivo rizika pretpostavio pre izvršenja napada i dr. Sa ovom tvrdnjom se slaže i Jasielo koji navodi da: „*Trenutno uspostavljena analitička metodologija: Proces analitičke hijerarhije (AHP), Analiza konkurentnih hipoteza i Delphi tehnike, nije adekvatna za adresiranje suptilnih nijansi kiber problema*“ (Iasiello, 2012, 4).

Šta proces analitičke hijerarhije *(AHP)* podrazumeva? „*Proces analitičke hijerarhije (AHP)*“ (Iasiello, 2012) - struktuirana tehnika koja se primenjuje za donošenje složenih odluka, metodologija je suviše statična i zahteva variranje alternativa u fiksnu, ponderisanu hijerarhiju. Kiber scenariji su više dinamičniji i ne mogu lako da se uklope u sistem rangiranja. Štaviše, proces analitičke hijerarhije se fokusira na „efekte“ kiberaktivnosti analizirajući hipoteze o tome šta je tačno ili šta je verovatno da će se dogoditi, a ne na motivima nakon kiber događaja.

„*Analiza konkurentnih hipoteza (ACH)*“ (Iasiello, 2012) - zasniva se na identifikaciji i analizi alternativnih hipoteza, a ne samo na jedan „*najverovatniji*“ zaključak. Međutim, kao i proces analitičke hijerarhije, analiza konkurentnih hipoteza nije u stanju da uzme u obzir dinamičnu prirodu kibernetskog prostora i dešavanja u njemu, te on ostaje siva površina. Jer,

osnovna struktura analize konkurentnih hipoteza-a ne uzima u obzir šta je „iza“ dokaza o izvršenom kiber napadu, nego služi samo za pronalaženje dokaza. Takođe, ova analiza zahteva analitički prevelik broj hipoteza, te je skoro nemoguće odrediti broj kiberaktera koji su zaslužni za svaki pokušaj ili uspešno sproveden upad u mrežu.

„*Delphi tehnika (DT)*“ (Iasiello, 2012) - fokusirana prognoza, koja može da pomogne prediktivnim analizama; nije održivi alat istraživanja, već služi kao podrška studijama sa bolje uspostavljenim i pouzdanijim metodama. Krajnje gledano, analitičari su primorani da je u svojim analizama primjenjuju prilikom upotrebe metode „*instinkta*“ za iznošenje pretpostavki na osnovu obimnih dokaza (Iasiello, 2012, 4-5).

Kako bi kiberodbrana bila što uspešnija Beriša i Barišić smatraju da je potrebno da se formira „*jedan centralni autoritet koji bi koordinirao odgovorom na nacionalnom nivou. U načelu nacionalni tim za odgovor na incident čini grupa eksperata za informacionu bezbednost koji proučavaju ranjivosti računarskih sistema*“ (Beriša & Barišić, 2016, 7), odnosno tzv. „*Tim za odgovor na incident (Computer Incident Response Team – CIRT, Computer Emergency Response Team – CERT)*“ (Beriša & Barišić, 2016, 7).

U odbrani od kiberterorizma upotreba kompjutera je neminovna, međutim potrebno je pokrenuti dublje mehanizme odbrane kao što su: sistemski pristup problemu, edukacija - kreiranje politike koja široko pokriva problem kiberterorizma, integracija međunarodnihi nacionalnih mera odbrane i standarda, potrebno je da se veća pažnja posvećuje „porukama“ koje se online emituju i dr.

Dakle, potrebno je da odbrana od kiberterorizma bude što je moguće sveobuhvatnija i slojevita. Jer, „*aktivna kiber odbrana podrazumeva proaktivne mere za suzbijanje neposrednih efekata kiber-incidenta, dok je pasivna odbrana usmerena na proizvodnju kiber sredstava koji pružaju efikasan otpor kiber napadima*“ (Farwell & Rohozinski, 2012, 109).

5.2.1. Aktivne mere odbrane od kiberterorizma

Aktivnu kiberodbranu Rozencvajg definiše kao „*sinhronizovanu pravovremenu sposobost da se otkriju, analiziraju i smanje pretnje. [Aktivna kiberodbrana] radi na brzini mreže, koristeći senzore, softver i inteligenciju da otkrije i zaustavi štetne aktivnosti pre nego što dopru do mreža i sistema*“ (Rosenzweig u: Dewar, 2014, 9).

Aktivna odbrana podrazumeva uključivanje ljudskog elementa u sam proces, odnosno analitičare koji: nadgledaju i primjenjuju svoje znanje kada su izloženi pretnjama unutar mreže, pronalaze adekvatne odgovore i usavršavaju se kako bi se što je moguće efikasnije izborili sa pretnjama od kiberterorizma, prate dnevnike aktivnosti koji automatizovano prikupljaju informacije koje im pomažu da detektuju napade ili pokušaje upada u sistem. Na primer ukoliko je sistem zaštićen lozinkama, niz neuspelih pokušaja prijavljivanja može da ukaže na pokušaj nekoga da pogodi lozinku i dobije neovlašćeni pristup mreži. Pomenuti analitičari kiber bezbednosti najčešće su specijalizovani za određenu oblast ili domen (testiranje, praćenje incidenta i reagovanje, analiza malvera, upravljanje rizikom i prikupljenim informacijama o opasnostima i dr.).

U širem smislu, prema navodima Vonga aktivna kiber odbrana uključuje:

„1) *eksploataciju*,

2) *kontranapad*;

3) *preduhitrujući napad (preemptive attack)*;

4) *preventivni napad (preventive attack)*“ (Wong, 2011, 19)

Prvi postupak aktivne kiberodbrane podrazumeva eksploataciju računarskih sistema koji su mete kibernapada. Pasivne mere odbrane mogu tokom kibernapada ili nakon njegovog izvršenja da otkriju *IP* adrese direktno sa kojih je pokrenut napad. Međutim, napadači sve više usavršavaju tehnike napada. Savremeni napadi su sve sofisticiraniji i nastaju kao konačni rezultat lančanih reakcija koje su proizvod umreženih hakovanih kompjutera, što značajno otežava da se utvrdi pravo poreklo napada i uđe u trag prvobitnom izvoru napada. Zato Belenкi i Ansari predlažu „*IP traceback*“ (Belenky & Ansari, 2003, 162). Međutim, ova tehnika još uvek nije zaživela zbog: neekonomičnosti - treba da se implementira na što je moguće više *ISP*-a da bi rezultati bili što precizniji i tačniji, problema sa kompatibilnošću i performansama. Revizijom kiber napada se celokupan postupak kojim je izvršen napad vraća unazad sve dok se ne otkrije

poslednja *IP* adresa računara sa kojeg je napad proistekao. Potom forenzičari identifikuju vlasnika računara, tako što „*istražuju dokumente sačuvane na računaru, vebistoriju, keš datoteke, e-poštu itd.*“ (Keith, Bejtlich & Rose, 2008, 205-300). Dakle, eksploatacija podrazumeva detaljnu analizu kiber napada.

Kontranapad je vrsta aktivne kiber odbrane koja podrazumeva suprotstavljanje napadaču ekvivalentnim kiber napadom. To ne samo da odbija trenutni napad, nego sprečava napadača da pokrene dalje napade. Na primer, u januaru 2000. godine na samitu Svetske trgovinske organizacije (*STO*) server je bio meta *DoS* napada od strane aktivističke grupe *E-hippies* čije je sedište u Velikoj Britaniji. Međutim, kompanija *Conkion Inc.* je bila u stanju da prati *IP* adrese sa kojih je proistekao napad na *STO* server i umesto da ga filtrira, dolazni napad je preusmerio nazad na server napadača i onemogućio ga na nekoliko sati.

Preduhitrujući napad kao i kontranapad spadaju u „*hack-back aktivnosti*“ (Boebert, 2010, 48-49). Preduhitrujući napad je „*preduzimanje sile protiv napada za koji se veruje da je neizbežan na osnovu dokaza da je neprijateljska akcija počela ili će uskoro početi*“ (Wong, 2011, 25). Dakle, ova vrsta aktivne odbrane podrazumeva reakciju na osnovu pretpostavljenog scenarija, odnosno „*sprovođenje napada na mrežu ili sistem u očekivanju da će taj sistem izvršiti napad na vaš*“ (Wong, 2011, 25). Preduhitrujući napad ima za cilj da oslabi i onesposobi neprijatelja tako da on ne može da sprovede planiranu ofanzivu. „*Svest potencijalnih napadača o takvom „kiber patroliranju“ samo po sebi deluje kao odvraćanje*“ (Boebert, 2010, 49) od njihove namere, jer su izloženi dodatnim sigurnosnim izazovima, pa samim time i neizvesnošću u pogledu stepena do kog su oni sami ugroženi.

Preventivni napad je sličan prethodno pomenutom preduhitrujućem napadu. Razlikuju se, po tome što preventivni napad podrazumeva „*upotrebu sile protiv očekivanog napada koja je zasnovana na proceni postojećih ili potencijalnih sredstava koje će napadač koristiti za napad u budućnosti ili da izazove druge vrste štete*“ (Sofaer, 2010, 9).

Prethodno navedeni postupci aktivne kiberodbrane zasnovani su na poznatoj i validnoj tehnologiji koju koriste i sami napadači, te ne postoje značajnije tehničke prepreke za njihovu primenu. Eventualne prepreke koje se mogu javiti su zakonske i političke prirode. Tako je pravno pitanje vlasništva nad napadnutom / oštećenom mašinom diskutabilno. Može se tvrditi da pravo nad mašinom koja postoji na internetu nasleđuje vlasnik fizičkog hardvera. Međutim, kiberteroristi mogu da koriste ukradenu mašinu za izvršenje zločina.

Ograničenja pomenutih mera aktivne kiberodbrane su vrlo kontroverzna, jer se njihovim sprovođenjem mogu prekršiti određeni međunarodni zakoni. Otuda Dening navodi „*etičke i legalne principe sprovođenja aktivne kiber odbrane:*

1. vlast

2. imunitet treće strane

3. nužnost

4. proporcionalnost

5. ljudsko učešće

6. građanske slobode“ (Denning, 2014, 111).

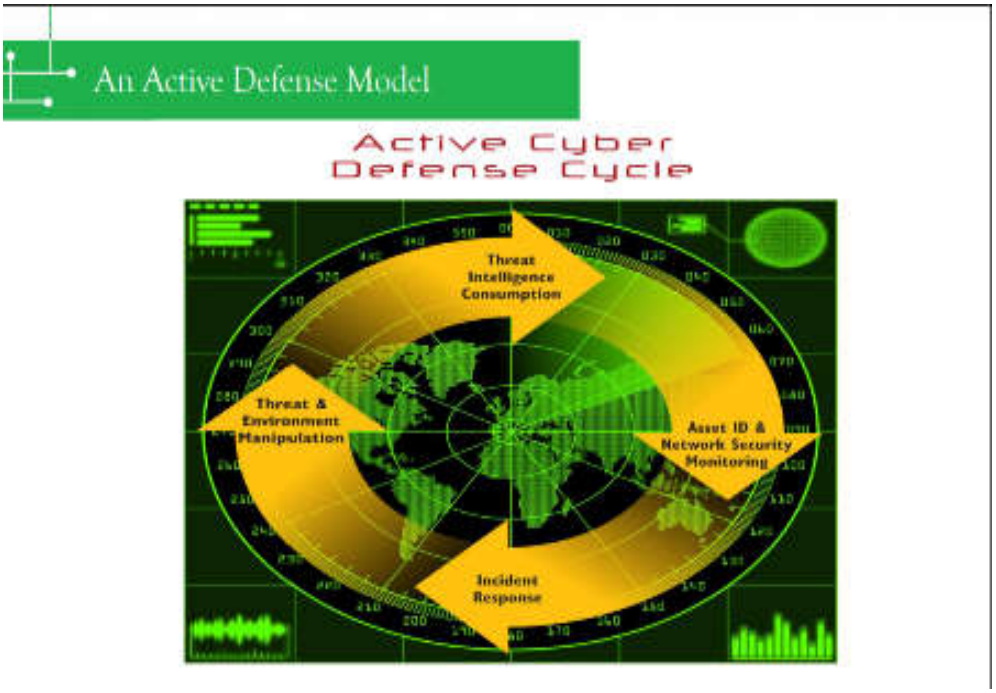
Prvi princip „*vlast*“ podrazumeva da aktivnu kiber odbranu mogu da sprovode samo organi koji su za to ovlašćeni, odnosno prihvaćeni od strane vlasti da rade u skladu sa zakonom. Drugi princip, „*imunitet treće strane*“ podrazumeva zaštitu trećeg lica. Odnosno, aktivna kiberodbrana ne sme da ugrozi one koji su žrtve kibernapada. Treći princip „*nužnost*“ znači da se mere aktivne kiberodbrane sprovode jedino kada je to neophodno, u slučajevima nužnosti. Četvrti princip „*proporcionalnost*“ znači da aktivnu kiberodbranu ne treba sprovoditi ukoliko pričinjena šteta i ostvarena korist nisu proporcionalne. Bilo koja vrsta aktivne kiberodbrane, čak i automatizovani oblici u određenoj fazi zahtevaju povremeno angažovanje ljudi. Peti princip „*ljudsko učešće*“, podrazumeva ograničavanje ljudskog faktora, jer nije poželjno, ni praktično uključiti ljude u sve faze aktivne kiberodbrane. Šesti princip „*građanske slobode*“ je usmeren na poštovanje građanskih prava korisnika mreža, onih koji su mete ili žrtve napada, ali i osumnjičenih (Denning, 2014, 111-112).

Inače, „*aktivnu kiber odbranu čine četiri karakteristike: obim efekta, stepen saradnje, vrste efekata, stepen automatizacije*“ (Denning, 2014, 109). Prva karakteristika, obim efekta razlikuje internu i eksternu odbranu. Interna odbrana je ona čiji su efekti ograničeni na mrežu koja je predmet odbrane. Dok, eksterna odbrana podrazumeva efekte koji prevazilaze mrežu. Druga karakteristika, stepen saradnje, pravi razliku između aktivne kiberodbrane koje su kooperativne, odnosno odvijaju se u skladu sa odobrenjem i saglasnošću za sprovođenje pojedinih mera aktivne odbrane i one koje to nisu. Dalje, na osnovu vrste efekata razlikujemo četiri tipa aktivne kiberodbrane u zavisnosti od: 1. deljenja, podrazumeva aktivnosti kojima se distribuiraju informacije o napadu (*IP* adrese sa kojih je napad izvršen i dr.), 2. prikupljanja, podrazumeva aktivnosti koje su usmerene za pribavljanje što većeg broja informacija o pretnji i

njenim efektima, 3. blokiranja efekata neprijateljskih aktivnosti, 4. preventivnih efekata kojima se onemogućavaju izvori koji se koriste za napad. Stepen automatizacije - poslednja četvrta karakteristika aktivne kiberodbrane se odnosi na to u kojoj meri je neophodno uključivanje ljudskog faktora, odnosno koji je stepen njegovog angažovanja.

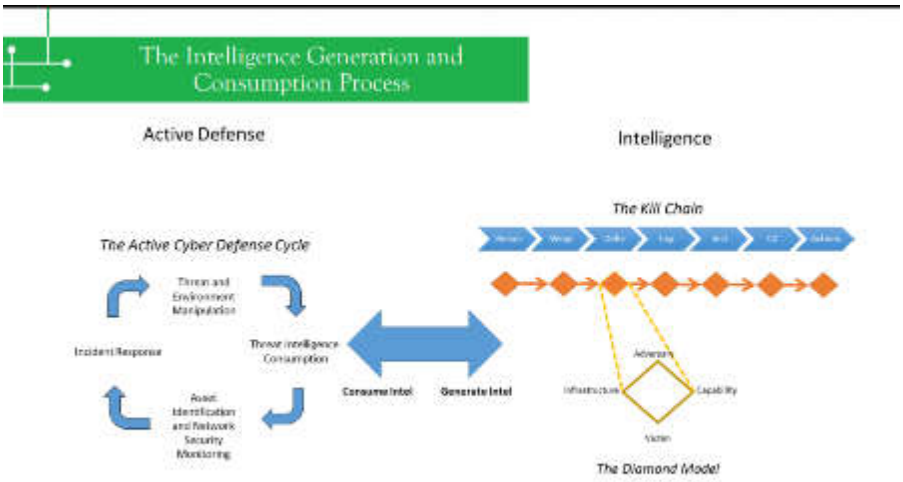
Robert Li pominje ciklus aktivne kiberodbrane, koji se sastoji iz četiri faze: „*1. pretnja, 2. identifikacija promena i nadgledanje bezbednosti mreže, 3. reagovanje na incident, 4. pretnja i rukovanje okruženjem*“ (Lee, 2015).

Slika 6. Ciklus aktivne kiber odbrane (Mandt & Lee, 2016, slajd 13)



Prva faza ciklusa aktivne kiberodbrane je „*pretnja*“ koja služi za identifikovanje realnih opasnosti kojima je izložena organizacija. To podrazumeva prikupljanje obaveštajnih informacija o misiji i okruženju organizacije. Kompanija ili organizacija može da prikuplja informacije o određenom kiberincidentu „*lokalno i udaljeno*“ (Lachow, 2013, 5-6). Lokalno prikupljanje informacija podrazumeva upotrebu raznih tehnika aktivne kiberodbrane unutar svojih granica. Dok, udaljeno prikupljanje informacija podrazumeva da određena kompanija ili organizacija sarađuje sa drugim organizacijama i ima pristup njihovom serveru što joj omogućava da prikuplja informacije van svojih granica.

Slika 7. Prva faza ciklusa aktivne kiberodbrane - pretnja (Mandt & Lee, 2016, slajd 14)



Druga faza ciklusa posvećena je identifikovanju promena kako bismo uvideli ozbiljnost pretnje i pokrenuli adekvatan odgovor. Treća faza, podrazumeva adekvatno „*reagovanje na incident*“ (Mandt & Lee, 2016) u zavisnosti od obima pretnje, kao i praćenje primenjene procedure reagovanja kako bi se iskorenila opasnost. Četvrta poslednja faza aktivne kiber odbrane podrazumeva izmene na mreži, odnosno njeno usavršavanje tako da bude otporna i sigurnija na dotadašnje pretnje kojima je bila izložena.

5.2.2. Pasivne mere odbrane od kiberterorizma

Svi korisnici interneta, bilo da je u pitanju pojedinac ili organizacija trebalo bi da primenjuju pasivne mere odbrane (set odbrambenih sistema). Jer, one pružaju konstantnu zaštitu ili uvid u pretnje od kiberterorizma pomoću alatki uz minimalne potrebe za stalnim nadzorom i intervencijom ljudi. Načešće su to sistemi koji zahtevaju periodično održavanje i krpljenje (*patching*) kao što su: zaštitni zidovi i različiti sistemi zaštite koji služe za otkrivanje (*IDS*) ili sprečavanje upada (*IPS*), sprečavanje propuštanja podataka (*DLP*), antivirusni softver, *malvare* sistemi, filteri za *spam* i dr.

Šta podrazumeva pasivna kiberodbrana? „*Pasivna kiberodbrana obuhvata kriptografiju i steganografiju (analogno upotrebi kamuflaže i prikrivanja aviona), sigurnosni inženjering i verifikaciju, konfiguraciju nadzora i upravljanja, procenu ranjivosti i ublažavanje, procenu rizika, rezervno kopiranje i oporavak (back up) izgubljenih podataka, edukaciju i obuku korisnika*“ (Denning, 2014, 109). Dakle, uključuje: „*firewalls, kibernetsku 'higijenu' koja trenira i edukuje radnu snagu kako bi se zaštitili od grešaka ili prekršaja koji mogu da dovedu do kiber upada, senzornu tehnologiju koja služi za detekcij 'honey pots' ili mamce koji služe za diverziju i upravljanje rizikom kibernetskog prostora kroz kolektivnu odbranu, pametno partnerstvo, informatičku obuku, veću svesnost o situaciji i uspostavljanje sigurnih, otpornih mrežnih okruženja*“ (Farwell & Rohozinski, 2012, 109). Iz prethodnog možemo zakjučiti da pasivna kiberodbrana podrazumeva splet kompleksnih mehanizama odbrane. Međutim, brojni mehanizmi koje pasivna odbrana uključuje su suštinski pasivni, ali postaju aktivni onda kada ugrade elemente za onesposobljavanje otkrivenih pretnji.

Pasivnu kiberodbranu već neko vreme primenjuju organizacije koje vode računa o bezbednosti svog poslovanja. Međutim kako su kibernapadi vremenom postajali sve ozbiljniji i složeniji, a posledice sve teže, oslanjanje na pasivne sisteme odbrane postalo je nedovoljno za kontinuirano praćenje i analizu sistema i podataka. Aktivna odbrana omogućava organizaciji da adekvatno i brzo reaguje na bezbednosne rizike i minimizira štetne posledice i gubitke.

5.3. Nove strategije koje se primenjuju u borbi protiv kiberterorizma

Kako bismo usavršili odbranu od kiberterorizma potrebno je konstantno usavršavanje postojećih i potraga za novim strategijama i idejama. U potrazi za novim idejama, Jasielo je ispitao mogućnosti primene dosadašnjih modela državne odbrane na kiber domen. Ispitao je: „*strategiju za nuklearno odvraćanje (Nuclear Deterrence), strategiju odvraćanja od terorizma (Terrorism Deterrence), strategiju odvraćanja od pretnji neprijateljskih država (Rogue States)*“ (Iasiello, 2018, 41-45).

„*Nuklearno odvraćanje (Nuclear Deterrence)*“ - U svojoj osnovi ova strategija ima za cilj da spreči upotrebu nuklearnog oružja, te se primenjuje jedino na države koje raspolažu nuklearnim naoružanjem. Početkom sedamdesetih godina, za vreme hladnog rata između SAD i Sovjetskog Saveza ova strategija se pokazala kao vrlo uspešna. Strategija nuklearno odvraćanje se zasniva na teoriji „*mutually assured destruction*“ (Payne & Walton, 2002, 169), odnosno sigurnom uzajamnom uništenju zemalja koje se usude da pokrenu upotrebu nuklearnog oružja. Otuda su SAD i Sovjetski Savez uprkos brojnim nesuglasicama i zaoštrenim odnosima, odlučili da ne koriste nuklearno oružje i rizikuju početak nuklearnog rata koji bi imao razorne posledice globalnih razmera. Malvenon i Retrej primećuju sličnosti koje postoje između između kiber i nuklearnog sukoba:

„1. *Oba deluju na sva tri nivoa vojnih operacija: strateški, operativno i taktički, i njihovi efekti imaju potencijal u rasponu od malih do populacionih razmera.*

2. Oba imaju kapacitet da stvore velike, čak i egzistencijalno, destruktivne efekte.

3. Oba se mogu sprovoditi između nacionalnih država, između nacije-države i nedržavnih aktera, ili između hibrida koji uključuju nacionalne države i ne-državne zastupnike.

4. Nuklearni i kiber konflikt može da predstavlja odlučujući poraz neprijatelja, time što on negira potrebu za konvencionalnim ratovanjem.

5. Oba mogu namerno ili nenamerno da uzrokuju kaskadne efekte izvan okvira prvobitnog cilja napada“ (Mulvenon & Rattray, 2012, 18).

Pored sličnosti postoje i razlike između kiber i nuklearnog sukoba:

„1. *Nacionalne države uglavnom ne preuzimaju odgovornost za preduzete neprijateljske akcije u kiberprostoru.*

2. Nije bilo zastrašivanja time šta može da učini kiber napad; incidenti poput STUKSNET-a i malvera koji je uništio 30.000 hard drajvera naftne kompanije u Saudijskoj Arabiji su doveli do značajnih poremećaja, ali nisu bili dovoljni da ozbiljno utiču na operacije u nuklearnom pogonu ili naftnoj kompaniji.

3. Izuzetno teško je identifikovati počinioca u kiberprostoru; što ne može da bude precizno kao što je identifikacija nacionalne države koja je pokrenula nuklearno oružje i,

4. Razvoj nuklearnog oružja se može pratiti, za razliku od njega ne postoji slična transparentnost za proizvodnju kiber oružja u državi, niti nadzorna međunarodna agencija koja prati takve razvoje" (Iasiello, 2013, 398). Pomenute razlike između kiber i nuklearnog sukoba ukazuju da strategija za nuklearno odvraćanje nije primenjiva u kiberprostoru (Iasiello, 2018, 42).

„*Strategija odvraćanja od terorizma (Terrorism Deterrence)*" - Ova strategija se pokazala uspešnom u nekoliko slučajeva. Na primer, kada teroristička organizacija preuzima atribute nacionalne države, odnosno kada poseduje imovinu koja se odmazdom može oštetiti, tada može da se utiče na vođstvo terorista tako da ono ograniči svoju politiku i delovanje zarad očuvanja resursa koje organizacija poseduje. Ubistvo terorističkog lidera najvišeg ranga, takođe može efikasno da odvrati teroriste od planiranih aktivnosti, ali samo na određeno vreme dok se ponovo ne organizuju. Kako bi strategija odvraćanja bila uspešna, protivnička strana „*mora da razume (implicitnu ili eksplicitnu) pretnju i donose odluke koje su rezultat kalkulacije troškova i koristi*" (Trager & Zagorcheva, 2005-2006, 87). Neuspeli pokušaji da se spreči istrajni protivnik ukazuju da ima mnogo više prepreka, nego koristi od ove strategije. Kada se ova strategija primeni na kiber domen, koji nije nužno vezan za jednu istu lokaciju nameće se pitanje: Kako da delujemo na pojedinca ili grupu terorista u kiber prostoru bez pouzdane informacije ko su oni zapravo ili gde žive? Još jedan faktor koji komplikuje primenu ove strategije u kiber domenu je motivacija. Može se reći da terorista koji deluje u kiberprostoru ceni sopstveni život, obzirom da se služi kiberoružjem i virtuelnim identitetom. Dakle, on nije direktno ugrožen. Dok, teroristi koji deluju operativno u realnom / fizičkom svetu kompromituju sebe i spremni su da izgube vlastiti život zarad ostvarenja ciljeva organizacije.

„*Strategija odvraćanja od pretnji neprijateljskih država (Rogue State*s)“ se primenjuje radi očuvanja nacionalne bezbednosti. SAD primenjuju ovu strategiju odbrane u odnosu prema Siriji i Severnoj Koreji. Kako bi strategija odvraćanja bila što efikasnija razvijena je njena posebna forma – „*prilagođena odvraćanja (tailored deterrence)*“ (Knopf, 2013). To su specijalno dizajnirane strategije odvraćanja prema obaveštajnim informacijama o svakoj državi ili situaciji ponaosob, čija je svrha da ciljano deluju na psihološke profile lidera i njihove odluke. Primena ove strategije u kiber okruženju nije pogodna, zbog složenosti i raznolikosti učesnika u kiber napadu. Teroristi ne funkcionišu kao neprijateljski nastrojena država čija je krajnja svrha stabilnost sopstvenog režima i očuvanje liderstva.

Libicki navodi da je osnovni cilj kiber odbrane da smanji „*rizik od kibernapada na prihvatljiv nivo po prihvatljivim cenama*“ (Libicki, 2009, 32). U vezi „*strategije odvraćanje pomoću kazne*“, potrebno je da nacionalna država pre bilo kakve odmazde ni u kom slučaju ne zagovara uvredljive radnje, nego jedino pažljivo odabrane postupke u odbrambene svrhe. Jasielo smatra da uspešna strategija odvraćanja pomoću kazne počiva na „*tri osnovna aksioma: 1. pripisivanje (Attribution), 2. ponovljivost (Repeatability), 3. uspeh (Success)*“ (Iasiello, 2018, 46). Pre pokretanja bilo kakvog kontra-udarca neophodno je poznavati: identitet počinioca, njegovu nameru, motivaciju, način izvršenja napada, metu napada i konačni cilj. Odnosno, kako bi pripisivanje bilo što preciznije potrebno je imati odgovore na što veći broj pitanja: „*Da li je kiberterorista povezan sa nacionalnom državom? Da li deluje samostalno ili je dobio naređenja odozgo? Da li odmazda proporcionalno odgovara pričinjenoj šteti? Da li je konačni cilj napada nacionalna država ili je cilj nešto drugo? Da li je namera napadača bila da: uništi, degradira, ospori ili nešto drugo? Da li je napad imao drugu svrhu osim one koja se vidi na površini?*“ (Iasiello, 2018, 47). Dalje, ne može jedna ista strategija da se primenjuje za kiberodbranu od različitih vrsta napada, napadača i ciljeva. Uspeh zavisi od primenjene taktike. Odnosno različite taktike kažnjavanja treba primenjivati pre, tokom ili nakon što se određeni kibernapad desio.

Obzirom da je „*domen kiberprostora inherentno nestabilan*“ (Mulvenon & Rattray, 2012, 23), Udruženje za ispitivanje kiberkonflikata (*Cyber Conflict Studies Association*) predlaže pet niovoa odbrane: „*1. strategija, 2. vojska i operativa, 3. nedržavni akteri u kiber prostoru, 4. domaće i međunarodno pravo, 5. pristupi za ublažavanje kiberkonflikata*“ (Mulvenon & Rattray, 2012, 17-27).

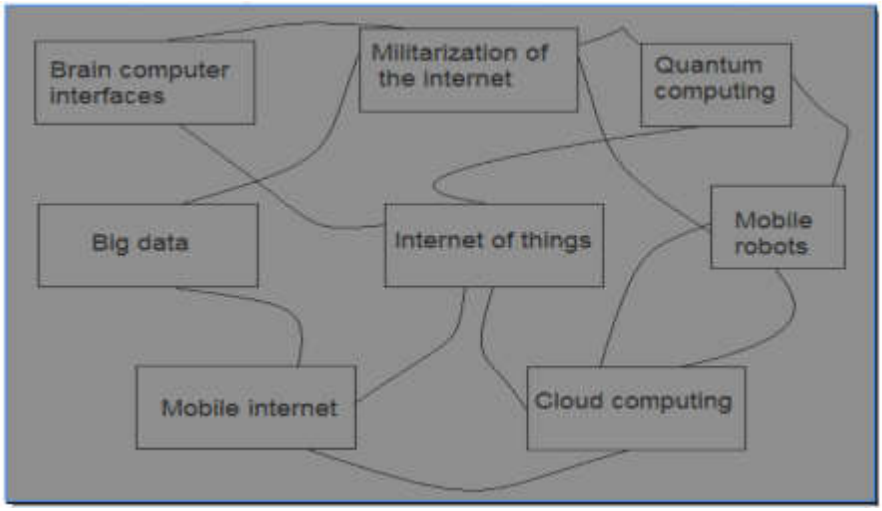
Begs i Batler kiberodbranu raščlanjuju na još više nivoa, odnosno devet tačaka. Otuda oni navode da efikasna borba protiv kiberterorizma treba da se odvija prema bezbednosnom planu „*SPECTR FCC: Strategy (strategija), Policy (politika), Education (obuka), Communication (komunikacija), Technology (tehnologija), Responsibility (odgovornost), Funding (finansiranje), Commitment (posvećenost) i Co-operation (saradnja)*“ (Beggs & Butler, 2004, 389).

Nove ideje odbrane od kiberterorizma se proširuju na ulogu nedržavnih aktera. Dosadašnje shvatanje o dominaciji državnih aktera u suočavanju sa kibernetskim sukobima i izazovima je pogrešno. Privatni sektor poseduje procentualno više globalnih računarskih mreža. Potrebna je tesna saradnja između državnog i privatnog sektora, naročito sa privatnim specijalizovanim jedinicama za kiber oblast. Privatni sektor treba da pruži otpor kiberterorizmu, spreči ili izbegne napad.

Kako se organizacije mogu odbraniti od pretnji kiberterorizma? Osnova dobre borbe protiv kiberterorizma je planiranje. Donešene strategije treba da se implementiraju redom u skladu sa ciljevima, prema višegodišnjem planu. Politika je drugi neizostavni deo bezbednosnog plana jer omogućava zaposlenima u organizacijama da se informišu o pravilima ponašanja, da ih razumeju i primenjuju u svakodnevnim radnim aktivnostima i na taj način podrže funkcionisanje bezbednosnih mehanizama. Dok, obuke omogućavaju rukovodiocima i menadžerima da prate trendove i razvoj bezbednosnih mehanizama, što je neophodno imajući u vidu dinamičnost kiber domena. Četvrta stavka je dobra komunikacija kako između organizacija, tako u unutar same organizacije. Dok je, primena napredne tehnologije jedna od stavki, ali ne i najznačajnija, obzirom da su tehnološke ranjivosti uzročnici kibernapada. Neizostavni deo bezbednosnog plana je odgovornost, odnosno svi zaposleni unutar organizacije treba da se ophode odgovorno prema podacima i usvojenim mehanizmima zaštite. Efikasna odbrana od kiberterorizma podrazumeva finansiranje bezbednosnih mehanizama i obuka zaposlenih. Neophodno je da svi zaposleni budu podjednako posvećeni očuvanju kiberbezbednostii da održavaju saradnju sa drugim organizacijama, radi razmene iskustva i problema u ovoj oblasti. Obaveza države je da pretnje i kiberteroristički napad blagovremeno otkrije, goni i procesuira. Efikasna odbrana od kiberterorizma podrazumeva saradnju između privatnog i državnog sektora. Tako da je potrebno da privatni sektor aktivno sarađuje i dostavlja podatke državi o kiberincidenatima i sumnjivom ponašanju u kiberprostoru.

Podjednako državni, privatni sektor i pojedinaci dele odgovornost za bezbednost informacionih sistema. Neophodna je saradnja da bi se kiberprostor stavio pod jedinstveni bezbednosni okvir, koji treba da „*uključi zajedničku strategiju i viziju različitih ekonomskih, tehničkih i komercijalnih pitanja sigurnosti*“ i „*sve slojeve bezbednosti: obuka i svesnost, prevencija, istraživanje i otkrivanje, reagovanje i oporavak*“ (Alqahtani, 2016, 13). Pored toga, potrebno je fokusirati se na stvaranje uspešne saradnje između timova koji su specijalizovani da pružaju rešenja u oblasti kiberbezbednosti (Sommestad, 2012).

Slika 8. Procenjene glavne discipline koje se razvijaju u oblasti kiberbezbednosti u budućnosti (Alqahtani, 2016, 13)



6. MERE I POSTUPCI ZA SUZBIJANJE KIBERTERORIZMA NA REGIONALNOM I GLOBALNOM PLANU

6.1. Pravno - organizacioni aspekt borbe protiv kiberterorizma

Kiberprostor je neophodan, nezamenljiv deo svakodnevnog života pojedinaca, kompanija i čitavih naroda. Iako je zavisnost od informaciono-komunikacionih tehnologija poprimila planetarne razmere postoje tri suštinska problema: tehniči, politički i pravni.

1. „*Osnovni tehnički problem leži u srcu kiberprostora, pošto osnovna arhitektura nikada nije bila dizajnirana imajući na umu bezbednost; štaviše prvobitni dizajneri nisu nikada ni pomišljali da će se mreža koristiti u zlonamerne svrhe*“ (Mulvenon & Rattray, 2012, 1). Prioriteti prvobitnih dizajnera su bili primenjivost i lako povezivanje korisnika (konekcija), tehnološke inovacije koje olakšavaju život.

2. „*Osnovni problem politike u kiberprostoru jeste to što je evolucija tehnološke arhitekture znatno prevazišla odgovarajući skup idejnih, doktrinarnih, organizacionih, i pravnih struktura, što rezultira reaktivnom i atavističkom dinamikom politike, gde se sadašnje ideje i organizacije često bave jučerašnjim problemima bez fleksibilnosti da se bave budućim problemima na osnovu najavljenih tehnoloških inovacija*“ (Mulvenon & Rattray, 2012, 1)

3. Primena zakonodavstva na internet i pravno regulisanje njegovih brojnih mogućnosti dilema je pravnika širom sveta. Stavljanje pod pravni okvir, kao i primena „*analognih*“ teritorijalnih zakona na neodređene digitalne granice beskonačne globalne komunikacione mreže, „*čini se da je previše za naše konvencionalne pravne sisteme*“ (Akhgar i dr., 2014, 3).

Imajući u vidu da ranjivosti kiberprostora stvaraju mogućnosti za izvršenje kiberterorizma, potrebno je regulisati aktivnosti koje se sprovode u ili u vezi sa kibernetskim prostorom. Kotim (Cottim, 2010) predlaže pet jurisdikcionih teorija i pristupa:

1. „*Teritorijalna teorija*“ - mesto gde je krivično delo počinjeno, u celosti ili delimično određuje jurisdikciju. Slabost ovog pristupa ogleda se u tome što je on zasnovan na pretpostavci da država ima neupitno suverenitet nad teritorijom koja je predmet rasprave, što nije nimalo lako potvrditi obzirom na fluidne granice kibernetskog prostora. Inače, ova teorija ima svoje korene u modelu državnog suvereniteta prema kojem su uspostavljeni Vestfalski mirovni sporazumi (Beaulac, 2004, 181) 1684. godine.

2. „*Teorija nacionalnosti (ili aktivne ličnosti)*“ - zasnovana je prvenstveno na nacionalnosti počinioca krivičnog dela.

3. „*Teorija pasivne ličnosti*“ - Dok se „*teorija nacionalnosti*“ bavi nacionalnošću počinioca, „*pasivna teorija ličnosti*“ se bavi nacionalnošću žrtve. Kotim ovo naziva „*područje kiberkriminologije*“ i kao dobar primer ovog pristupa navodi slučaj kada je jedan ruski državljanin osuđen na sudu u Hartfordu u Konektikatu zbog hakovanja računara u Sjedinjenim Američkim Državama.

4. „*Teorija zaštite*“ (takođe poznata kao „*princip sigurnosti*“ i „*teorija o povređenim forumima*“) - bavi se povređenim nacionalnim ili međunarodnim interesima i dodeljivanjem nadležnosti državi koja ostvaruje interes, bilo nacionalni ili međunarodni u situaciji prouzrokovanoj napadom. Kotim navodi da se ova teorija retko primenjuje, uglavnom kod zločina poput falsifikovanja novca i vrednosnih papira.

5. „*Teorija univerzalnosti*“ – oslanja se na princip univerzalnosti koji je zasnovan na međunarodnom karakteru krivičnog dela koji omogućava svakoj državi da traži nadležnost za učinjena krivična dela, čak i ako ta dela nemaju direktnog uticaja na tu državu. Iako deluje da ova teorija ima najviše potencijala za primenu u kibernetskom prostoru, Kotim ukazuje da postoje njena dva ključna ograničenja. Prvo ograničenje je to što država mora da ima optuženog u pritvoru kada zahteva nadležnost pod pretpostavkom da je učinjeno krivično delo. Dok je drugo ograničenje to što zločin treba da bude „*naročito uvredljiv za međunarodnu zajednicu*“. Postoje značajne praktične poteškoće koje otežavaju definisanje parametara principa univerzalnosti i mogućnosti proširenja ovog principa na oblast kibernetskog prostora i aktivnosti u njemu. Teorija univerzalnosti se uglavnom primenjuje kod krivičnih dela piraterije i kod ilegalne trgovine robom.

Kao što primećuje Hafner (Hafner, 1998) iako je internet mreža nastala 1960-ih godina, kibersukobi nisu bili viđeni kao zabrinjavajuća pretnja sve do kraja 1980-ih, kada su dva značajna događaja podstakla zabrinutost oko sigurnosti i pouzdanosti na internetu. Prvi događaj je bio 1987. godine kada je istraživač Klif Stol (Stoll, 2005) otkrio hakera koji je koristio mrežu nacionalne laboratorije „*Lawrence Berkeley*“ da bi hakovao druge mreže uključujući vojne baze i odbranu. Krajem osamdesetih je Robert Moris, prvi put pustio „*crva*“ (Orman, 2003) i time ugrozio bezbednost interneta, nakon čega je osuđen na osnovu Zakona o računarskim prevarama i zlostavljanju, uprkos njegovim izjavama da je želeo da izmeri veličinu interneta i da nije bio

zlonameran. Dakle, sa zakašnjenjem tek nakon 80-tih godina započinje evolucija krivičnog prava u oblasti kiberbezbednosti. Kao što navodi Siber (Sieber, 1994, 25-28), 1992. godine usvojene su osnovne smernice za sankcionisanje zlonamerne upotrebe računara u Nemačkoj. Prema navodima Šjolberga (Schjolberg, 2014, 24-31) prvi zakoni kojima se inkriminiše zloupotreba računara usvojeni su krajem XX veka u mnogim zemljama (Italija, SAD, Velika Britanija, Australija, Nemačka, Danska, Švedska, Norveška i Austrija, Francuska, Holandija, Španija, Finska i dr.).

Svedoci smo svakodnevnog razvoja informacionih tehnologija koji se odvija toliko velikom brzinom da ga gotovo jedva primećujemo. Svake godine izlaze novi savremeniji modeli pametnih telefona, računarske opreme i druge vrste uređaja, čiju primenu brzo i olako prihvatamo. Tehnološki razvoj je proširio mogućnosti za zloupotrebu savremene tehnologije. Pravna regulativa i međunarodna saradnja nisu išli u korak sa ovim razvojem, što takođe primećuje i Šmit kada navodi: „*Nažalost, postojeće pravne norme ne nude jasan i sveobuhvatan okvir unutar kojeg države mogu da oblikuju političke odgovore na opasnost od neprijateljskih kiberoperacija*“ (Schmitt, 2010, 152). Jer, ubrzan razvoj informacionih tehnologija iziskuje konstantne napore, edukaciju i druga ulaganja za praćenje novih izazova u oblasti IT industrije. Zato samo nekolicina zemalja poseduje adekvatne pravne regulative koje omogućavaju efikasno sankcionisanje i kažnjavanje kiberkriminala i kiberterorizma. To je podstaklo nameru država da prilagode zakonsku regluativu savremenim rizicima i da postojeće krivične zakone upotpune novim odredbama, ne samo na nivou jedne države, nego i na međunarodnom nivou u oblasti kiberbezbednosti. Međutim, formiranje pravne osnove na međunarodnom nivou je proces koji traje i zahteva šire, sveobuhvatnije razmišljanje o uzrocima i dinamici kiberterorizma.

Međunarodno humanitarno pravo prema Bjankiju pruža „*regulatorni okvir*“ i „*efikasne*“ mehanizme „*za kažnjavanje terorističkih akcija*“ (Bianchi, 2011, 21). Odnosno, međunarodno humanitarno pravo „*osuđuje teroristička dela i na međunarodnom i unutrašnjem planu i nudi sistem za gonjenje i kažnjavanje*“ (Condorelli & Naqvi, 2004, 37).

Međutim, rezultati istraživanja potvrdili su da „*vlade, kada su pod pretnjom terorizma, krše neka od prava koja žele na prvom mestu da zaštite*“ (Dreher, Gassebner & Siemers, 2010, 88). Suprostavljanje terorizmu generalno, može da „*stvori opasnu i pogrešnu sliku o relativnosti ljudskih prava, i skoro neizbežno podrazumeva intruzivni nadzor i gubitak privatnosti, ograničeno kretanje u zemlji i inostranstvu i oduzimanje osnovnih prava i zaštite u sistemu*

krivičnog pravosuđa“ (Jones & Howard-Hassmann, 2005, 62-63). Međutim, „*uprkos zabrinutosti mnogih zagovornika ljudskih prava, vlade ne reaguju uvek na terorističke napade ograničavanjem prava. Umesto toga, odnos je komplikovaniji, jer teroristički napadi podstiču ograničenja nekih prava, ali ne i drugih. Drugo, kršenje ljudskih prava od strane vlada može da bude snažan preduslov za kasnije terorističke napade*“ (Piazza & Walsh, 2010, 407).

Kiberteroristička dela po prirodi mogu ili ne mogu da pokrenu oružani sukob, u zavisnosti od konkretnih okolnosti. Kada je u pitanju tumačenje i primena zakona jedne konkretne države preko njenih administrativnih granica jurisdikcije, suočavanje sa kiberterorizmom je diskutabilno. Jer je linija razdvajanja između upotrebe sile i međunarodnog humanitarnog prava zamućena. Otuda Šmit navodi četiri ključna pitanja vezana za regulisanje kiberoperacija kroz prizmu međunarodnog prava:

„*1) Kada kiber operacija predstavlja nedozvoljenu „upotrebu sile“ kojom se krši Povelja Ujedinjenih nacija, član 2 (4) i međunarodno običajno pravo?;*

2) Kada kiber operacija predstavlja „pretnju i kršenje mira ili postupak agresije“ tako da Savet bezbednosti može da dozvoli pružanje odgovora za to?;

3) Kada kiber operacija predstavlja „oružani napad“, takav da može država - žrtva da se brani, čak i kinetički, u skladu sa pravom na samoodbranu iz člana 51. Povelja UN i prema običajnom međunarodnom pravu?;

4) Kada se kiber operacija podiže do nivoa „oružanog sukoba“, tako da ga međunarodno humanitarno pravo reguliše kao ratne aktivnosti?“ (Schmitt, 2010, 152).

Šmit (Schmitt, 1999, 18) je identifikovao niz faktora pomoću kojih se ekonomska i politička prinuda mogu ograničiti od upotrebe oružane sile. Primena ovih faktora na kiber domen može da utiče na procenu države o tome da li određene kiber operacije predstavljaju upotrebu sile:

1. „*Težina posledica*“ - Procena ozbiljnosti štete u zavisnosti od skale, opsega i trajanja posledica. Da li pričinjene štete predstavljaju samo manju neprijatnost ili provokaciju za pojedinca i / ili imovinu? Ili je više ekstremna i utiče na kritične nacionalne interese? (Schmitt, 1999, 18).

2. „*Momentalnost*“ - U zavisnosti od vremenskog aspekta, odnosno pojavljivanja štetnih posledica: neposredno ili odloženo i sporo štetno dejstvo. Kada se štetne posledice odmah manifestuju pred državom je zadatak da brzo reaguje (Schmitt, 1999, 18).

3. „*Direktnost*“ - Odnosi se na lanac uzročnosti, što je veza između početnog čina i posledica slabija manja je verovatnoća da će država smatrati aktera odgovornim za kršenje zabrane upotrebom sile. Na primer, eventualne posledice ekonomske krize određuju tržišne snage, pristup tržištima i dr. Kauzalna veza između inicijalnih akata i njihovih efekata je indirektna. Nasuprot tome, kod eksplozije su uzrok i posledica direktno povezani (Schmitt, 1999, 18).

4. „*Invazivnost*“ - Što je ciljani sistem sigurnosno bolje obezbeđen, to je veća zabrinutost u pogledu prodiranja u sistem. Konkretan primer je kiber špijunaža koja iako je veoma invazivna, ne predstavlja upotrebu sile (ili oružani napad), već se prema međunarodnom pravu tretira kao nedozvoljen fizički prodor na teritoriju ciljane države, kao u slučaju ratnog broda ili vojnog aviona koji prikuplja obaveštajne podatke iz njenog teritorijalnog mora ili vazdušnog prostora (Schmitt, 1999, 19).

5. „*Merljivost*“ - U interesu države je da izmeri što je moguće preciznije količinu pričinjene štete. Razmatrano sa aspekta međunarodnog prava, ekonomska prinuda može da izazove značajne patnje, ali ne predstavlja upotrebu sile. Sa druge strane vojni napad se klasifikuje na osnovu izmerenog stepena razaranja. Teško je identifikovati ili kvantifikovati štetu koja je pričinjena u kiberprostoru (Schmitt, 1999, 19).

6. „*Pretpostavljeni legitimitet*“ - Međunarodno pravo izričito zabranjuje određena dela, a ona koja nisu zabranjena pretpostavka je da su legitimna. Bilo u domaćem ili međunarodnom pravu, primena nasilja smatra se nelegitimnom, s posebnim izuzetkom kada je u pitanju samoodbrana (Schmitt, 1999, 19).

7. „*Odgovornost*“ - Zakonom se uređuje kada će država da bude odgovorna za kiber operacije. Što je čvršća veza između određene države i operacija u kiberprostoru, to će biti veća verovatnoća da će ostale države to karakterisati kao upotrebu sile, što dovodi u pitanje međunarodnu stabilnost (Schmitt, 2010, 916). Zato je potrebno posebnu pažnju usmeriti na vojnu politiku, koja bi prema navodima Kara: „*trebalo da bude usmerena ka uvođenju međunarodnih pravnih mehanizama koji bi omogućili sprečavanje potencijalnih agresora da nekontrolisano i potajno koriste kiber naoružanje*“ (Carr, 2010, 168). Tehnološki razvoj je iznedrio nove forme kiber alata/oružja čije posledice mogu da budu destruktivne isto kao i prilikom upotrebe regularnog oružja. Otuda brojni analitičari (Weigant, 2013; Rauscher, 2013) ukazuju da je ratni zakon postao neadekvatan i predlažu da se poveća regulacija kiberprostora.

6.1.1. Međunarodna dokumenta posvećena borbi protiv kiberterorizma

Obzirom da je kiberterorizam posebna forma terorizma, kratko ćemo pobrojati neke od relevantnih međunarodnih dokumenata, konvencije i rezolucije čija je osnovna tematika borba protiv terorizma:

- Konvencija Organizacije američkih država o suzbijanju i kažnjavanju akata terorizma, 2.2.1971.

- SAARC (Azija) regionalna konvencija o sprečavanju terorizma, 4.11.1987.

- Arapska konvencija o suzbijanju terorizma, doneta od strane Arapske lige 22.04.1998.

- Međunarodna konvencija za suzbijanje terorističkog bombardovanja, 1997.

- Ugovor o saradnji između država članica Zajednice nezavisnih država o suzbijanju terorizma, 4.6.1999.

- Konvencija organizacije islamske konferencije o borbi protiv međunarodnog terorizma, 1.7.1999.

- Konvencija organizacije Afričkih država o prevenciji i borbi protiv terorizma, 14.7.1999.

- Konvencija o sprečavanju terorizma, CETS br. 196, 16. maj 2005.

- Međunarodna Konvencija o suzbijanju finansiranja terorizma, (Službeni list SRJ - Međunarodni ugovori, br. 7/2002)

- Evropska konvencija o suzbijanju terorizma, 27.1.1977. (Službeni list SRJ - Međunarodni ugovori, br. 10/2001)

- Globalni forum za borbu protiv terorizma, „The Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector“ (Rabatski memorandum o dobrim praksama za efikasan rad u suzbijanju terorizma u sektoru krivičnog pravosuđa), 2012. godine.

Na osnovu navedenih dokumenata, skoro da i ne postoji svetski region u kojem nije razmatrana borba protiv terorizma. Međutim, iako su mnoge zemlje potpisnice brojnih konvencija i protokola iz oblasti terorizma i njegovih pojavnih oblika, praktična primena nije nimalo jednostavna. Kao što primećuju Komlen Nikolić i saradnici, osnovne prepreke za

suzbijanje kiberkriminala na međunarodnom nivou su: pravna neusaglašenost oko definisanja radnji i oblika izvršenja pojedinih krivičnih dela; nedovoljna obučenost lica zaduženih za postupanje u predmetima kiber kriminala (policije, tužilaca i sudija), neusklađenost pravila istrage krivičnih dela kiber kriminala i neusklađenost ili odsustvo mehanizama pravne pomoći i sporazumne ekstradicije na međunarodnom nivou (Komlen Nikolić i dr., 2010, 31).

Imajući u vidu da je kiberterorizam pretnja međunarodnih razmera, veliki broj međunarodnih organizacija se bavi kiberbezbednošću radi sveobuhvatnijeg i kvalitetnijeg suprostavljanja ovom problemu. Donet je velik broj dokumenata i organizovan je veliki broj konferencija koje razmatraju pitanje kiberbezbednosti na međunarodnom nivou. Dokumenta koja su nastala kao rezultat ranijih zasedanja mnogo puta su predstavljana u literaturi. Zato ćemo za ovu priliku navesti samo neke od aktuelnih dogovora i konferencija, novijeg datuma koja se bave problemom bezbednosti u kibernetskom prostoru.

- Dogovor EU za područje kiber bezbednosti za 2019. godinu (*EU cybersecurity organizations agree on 2019 roadmap*) (Enisa, 2018 - *European Union Agency for Network and Information Security*).

Pomenuti dogovor je nastao kao rezultat sastanka koji je održan 6. novembra 2018. između direktora: Memoranduma o razumevanju (MoU - *Memorandum of Understanding*), Agencije Evropske unije za sigurnost mreže i informisanja (ENISA), Evropske agencije za obelodanjivanje (EDA - *European Defence Agency*), Europola, Kompjuterskog tima za hitno reagovanje (CERT - *Computer Emergency Response Team for the EU Institutions*). Cilj sastanka je međusobna saradnja i razmena informacija o relevantnim dešavanjima, procena postignutog napretka u oblasti sigurnog i otvorenog kiberprostora. Kako bi poboljšali međusobnu razmenu informacija dogovoreno je da fokus buduće saradnje bude na zajedničkoj obuci i kibervežbama, zajedničkim projektima i događajima kojima se dopunjava rad pomenutih organizacija i izbegava dupliranje napora.

- Konferencija Međunarodne telekomunikacione unije (*ITU Plenipotentiary Conference 2018*) koja je održana u Dubai-u 2018. godine u periodu 29.oktobra do 16.novembra (ITU, 2018).

Međunarodna telekomunikaciona unija (ITU- *International Telecommunication Union*) stvorena je 2005. godine na Svetskom samitu o informacionom društvu. ITU na svake četiri godine saziva konferenciju za svoje države članice na kojoj se donose odluke o njenom daljem

radu i izrađuju strateški i finansijski planovi koji imaju za cilj da utiču na razvoj informacionih i komunikacionih tehnologija širom sveta. Jedan od ITU projekata je Indeks globalne kiber-sigurnosti (GCI- *Global Cybersecurity Index*) koji služi za merenje i unapređenje kiberbezbednosti nacionalnih država. Forum za upravljanje internetom, (IGF - I*nternet Governance Forum*) je posebno formiran organ koji nema mandat da međunarodne ugovore i ostala pravna dokumenta usvaja, ali predstavlja bazu odluka koju usvajaju druge insitucije za upravljanje internetom.

- Zasedanje WSIS (The World Summit on the Information Society) foruma u Ženevi 19. do 23 marta. 2018 godine (WSIS forum, 2018)

Svetski samit za informaciono društvo (WSIS - *World Summit on the Information Society*), čiji je osnovni cilj izgradnja poverenja i sigurnosti za korišćenje informacionih i komunikacionih tehnologija je marta 2018. dodelio Srbiji prestižnu nagradu za doprinos i stvaranje povoljnog okruženja za razvoj informacionog društva. WSIS je globalna platforma koja se bavi održivim razvojem informacionog društva tako što podstiče partnerstva, razmenu informacija i najboljih praksi, stvaranje znanja istovremeno identifikujući trendove koji se pojavljuju u IT oblasti. Predloženo je da naredeni forum bude održan 8-12.aprila 2019. (WSIS forum, 2019).

- predstojeća Konferencija (*ICT 2018 Imagine Digital - Connect Europe*) u Beču koja je zakazana za period od 4. decembra do 6. decembra 2018. godine sa fokusom na digitalnu transformaciju društva i industrije u EU. ICT je zaslužan za donošenje velikog broja dokumenata u *IT* oblasti (ICT, 2018).

- Samit APEC-a (*Asia-Pacific Economic Cooperation*) u Novoj Gvineji 19. novembra 2018 (APEC, 2018)

- APECTEL (*APEC Telecommunications and Information Working Group*) je nakon desetog zasedanja u martu 2015. godine (10th APEC TELMIN 30-31 March 2015) razvio strateški akcioni plan za period 2016-2020. god. koji ima za cilj da obezbedi da što više ljudi u azijsko-pacifičkom regionu imaju bezbedan pristup internetu i savremenim IT tehnologijama. Nekoliko zemalja članica Lige arapskih država koja datira iz 1945. godine usvojilo je zakone o kiberkriminalu (Pakistan, Saudijska Arabija i Ujedinjeni Arapski Emirati (UEA).

6.1.2. Multilateralna saradnja kao odgovor na pretnju od kiberterorizma

Mulrilateralna saradnja je neophodna za uspešno suočavanje sa problemom kiberterorizma, jer kao što primećuje Graboski: „*Digitalni kriminal ne poznaje granice između država*“ (Grabosky, 2007, 15.). Zato „*borba protiv visokotehnološkog kriminala treba da bude ili globalna ili nema smisla*“ (Broadhurst, 2006, 414). Primetno je pojačano interesovanje za saradnjom po pitanju kiberbezbednosti, kako od strane međunarodnih organizacija tako i pojedinih zemalja. Borbu protiv kiberterorizma treba tumačiti sa stanovišta teorije „*crnog labuda*“ (Nicholas, 2007) koja se odnosi na nepredvidive i malo verovatne događaje koji imaju snažan uticaj na ljudsku zajednicu i koji nakon prvog događanja postaju verovatniji i predvidljiviji.

Opšti okvir multilateralne saradnje za suprotstavljanje kiberterorizmu propisuje mehanizme za pružanje međunarodne krivično-pravne pomoći. Saradnja se odvija na sva tri nivoa: makro-nivo, podrazumeva ugovornu saradnju između država i međunarodnih organizacija, mezo-nivo se odnosi na kooperativnost državnih organa koji su specijalizovani i nadležni za *ad hoc* potrebe i mikro-nivo podrazumeva neposrednu i neformalnu saradnju nadležnih organa jedne države (Bryant & Stephens, 2014, 112-113).

6.1.3. Ujedinjene nacije (UN)

Ujedinjene nacije su takođe prepoznale kiberterorizam kao jednu od najznačajnijih opasnosti koja preti savremenom čovečanstvu. Razvoj savremenih informaciono-komunikacionih tehnologija i primena tehnologije u gotovo svim sferama ljudske delatnosti nesumnjivo ukazuju da će pitanje kiberbezbednosti postati sve aktuelnije u budućnosti.

Ujedinjenje Nacije su dale veliki doprinos po pitanju bezbednosti i odbrane od terorizma i donosioci su brojnih međunarodnih dokumenata, rezolucija i drugih dokumenata počev od 30-tih godina XIX veka. Nakon atentata 9. oktobra 1934. u Marselju donešena je rezolucija kojom se zabranjuje „*bilo kakvo uplitanje u politički život druge države*“ (Chandan, 1935, 405). U periodu od 1. do 16. novembra 1937. godine u Ženevi je održana Međunarodna konferencija posvećena terorizmu. Od prve polovine XIX veka do danas donešena su brojna dokumenta koja su rezultat brojnih sednica, zasedanja i konferencija. Kako se terorizam vremenom usložnjavao, tako su i UN propisivale nova dokumenta i formirale organe za suprostavljanje terorizmu. Nakon terorističkog napada na Njujork i Vašington Ujedinjene nacije su donele odluku za osnivanje Komiteta za borbu protiv terorizma 2001. godine.

Kofi Anan je kao vršilac dužnosti generalnog sekretara UN predložio svetskim čelnicima da prihvate zajedničku definiciju terorizma i dogovore uslove pod kojima međunarodna zajednica može da upotrebi silu radi odbrane mira i sigurnosti. Takođe, UN su donosilac Globalne antiterorističke strategije *(UN Global Counter - Terrorism Strategy)* koja je jedinstveni instrument za suprostavljanje terorizmu na međunarodnom nivou. Ova strategija se iznova razmatra na svake dve godine, kako bi pratila trend razvoja terorizma i bazira se na: četiri osnovna stuba: prvi - otkrivanje uslova koji pogoduju širenju terorizma, drugi – prevencija i suzbijanje terorizma, treći - izgradnja državnih kapaciteta i jačanje uloge Ujedinjenih nacija i četvrti – osiguranje vladavine ljudskih prava i zakona (UN Global Counter - Terrorism Strategy, 2006).

UN se aktivno bave problemom terorizma. Ove godine, 28. i 29. juna na predlog Generalnog sekretara Ujedinjenih nacija održana je Konferencija na kojoj su učestvovali rukovodioci agencija zemalja članica. Osnovni cilj konferencije je izgradnja novog partnerstva i jačanje multilateralne saradnje u borbi protiv terorizma (United Nations, 2018). Ujedinjene nacije su jedna od vodećih međunarodnih organizacija koja ozbiljno i kontinuirano ulaže napore za suprostavljanje pomenutom problemu.

6.1.4. NATO

NATO, političko-vojna evroatlantska alijansa je već duže vreme svesna pretnji nove forme ratovanja - kiberratovanja, kao i ostalih pretnji koje proizilaze iz kiberprostora. U novembru 2002. godine održan je samit u Pragu, na kojem su lideri NATO-a odlučili da ojačaju svoje sposobnosti odbrane od kibernapada. Pomenuta odluka, podstakla je sistematičniji pristup i mnoge inicijative i programe za suzbijanje terorizma u okviru NATO-a. Tada su formirana različita NATO tela koja su dobila nadležnosti po pitanju zaštite i odbrane od kiberincidenata:

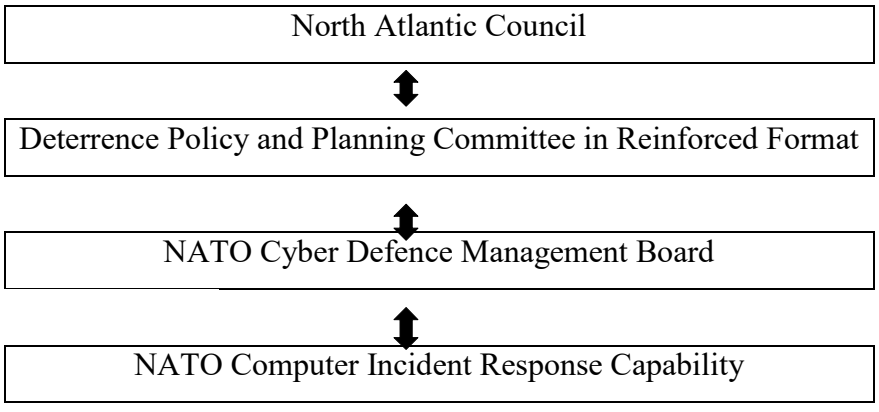
- Agencija NATO-a za komunikacije i informacione sisteme (NCSA - *NATO Communication and Information Systems Services Agency*) se smatra prvom linijom odbrane od kiberterorizma.

- NATO INFOSEC Tehnički Centar (NITC - *NATO INFOSEC Techinical Center*) je odgovoran za kompjutersku i komunikacijsku sigurnost.

- Operativni centar (NIAOC - *NATO Information Assurance Operations Centre*) nadležan je za poslove upravljanja i koordinaciju kriptografske opreme koja se koristi za pružanje odgovora na kibernapade koji su usmereni protiv NATO;

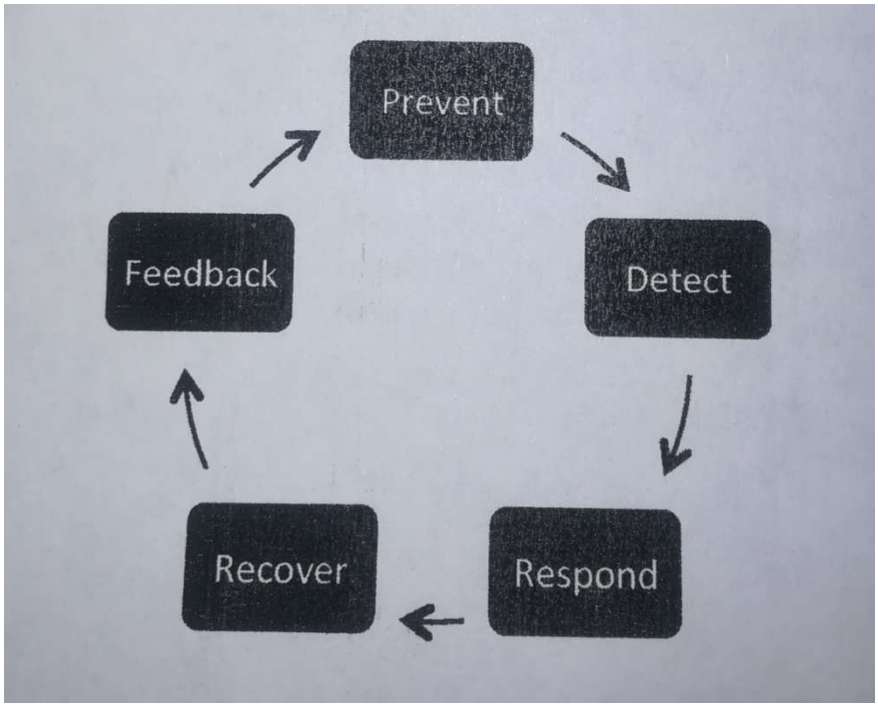
- NATO centar za pružanje odgovora na kompjuterske incidente (NCIRC - *NATO Computer Incident Response Capability*), čiji je osnovni zadatak zaštita šifrovane komunikacije unutar NATO sistema. NCIRC je glavni izvor tehničke i operativne stručnosti i mogućnosti NATO-a u oblasti kiberodbrane, koji služi da zaštiti NATO subjekte (npr. upravu NATO-a) i misije; služi za rešavanje pretnji kojima je ugrožena kibersigurnost NATO informacionih sistema (NATO, 2002).

Slika 9. Nato kiber odbrana (Fidler, Pregent & Vandurme, 2013,7)



Nakon lošeg iskustva koji je izazvao kibernapad u Estoniji 2007. godine, počinje period intenzivnijeg NATO fokusa na kiberodbranu. 2008. godine u Nordvijku su ministri NATO-a postigli dogovor o „*konceptu kiberodbrane*“ na osnovu kojeg je razvijena odbrambena NATO kiberpolitika, koja je 2010. godine postala deo „*Strateškog koncepta*“ (Bogdanovski & Petreski, 2016, 66).

Slika 10. NICRC metodologija (Fidler, Pregent & Vandurme, 2013,10)



Potom su usledili samit u Velsu 2014. i Varšavi 2016. godine na kojima su takođe razmatrana pitanja kibebezbednosti i kiberodbrane. U periodu 16. do 18. oktobra 2018. godine održan je simpozijum NIAS18 - *Cyber Security Simposium* (NIAS18, 2018) kako bi NATO članice razmenile svoja iskustva i najbolje prakse i ponudile inovativna rešenja za unapređenje IT sigurnosti. Nato kiberterorizam vidi kao ozbiljnu pretnju koja u budućnosti može značajno da naruši bezbednost i stabilnost zato održava dobru saradnju sa međunarodnim organizacijama koje se takođe bave pitanjima međunarodne bezbednosti: UN, OEBS i dr.

6.1.5. Savet Evrope

Savet Evrope (CoE - *Councile of Europe*) je dao veliki doprinos u oblasti borbe protiv kiberkriminala. Na predlog Saveta Evrope osnovan je 1997. godine Komitet eksperata za oblast kriminala u kiber prostoru (*Committee of Experts on Crime in Cyber-space*) koji su radili na izradi „*Konvencije o kibernetičkom kriminalu*“ (*Convention on Cybercrime*). Konvencija je završena u junu 2001. godine i predstavlja prvi međunarodni sporazum na temu kiberkriminala. U novembru iste godine u Budimpešti je potpisana od strane trideset četiri zemalja koje su učestvovale u ceremonijalnom činu, dok je šest zemalja ratifikovalo ovu Konvenciju (Estonija, Litvanija, Mađarska, Rumunija, Albanija i Hrvatska). Do novembra 2018. godine ovoj konvenciji su pristupile 62. zemlje.

Konvencija sadrži: listu zločina koje svaka država potpisnica mora da unese i kriminalizuje u svoje zakone, proceduralne mehanizme i standarde koje svaka država potpisnica treba da implementira u okviru svojih zakona, obavezuje ih na međusobnu saradnju i najšire međunarodne istražne mere i postupanja u vezi sa krivičnim delima koja se odnose na kompjuterske sisteme i podatke ili za prikupljanje dokaza u elektronskom obliku koji su vezani za krivična dela. Ova Konvencija uživa velik međunarodni autoritet i otvorena je za sve, ne samo za države članice Saveta Evrope.

6.1.6. OEBS (OSCE)

OEBS (OSCE - *Organization for Security and Co-operation in Europe*) je počeo intenzivnije da se bavi kiberbezbednošću nakon odluke Saveta ministara 2004. godine da se prati upotreba interneta od strane terorista za različite aktivnosti kao što su: finansiranje terorista, propaganda i njihovo regrutovanje (Bogdanovski & Petreski, 2016, 68).

Na 23-ćem OSCE zasedanju 9. decembra 2016. godine u Hamburgu donešena je Odluka br. 5/16, kojom se ulažu napori OEBS-a u vezi sa smanjenjem rizika od sukoba koji proizilaze iz upotrebe informacionih i komunikacionih tehnologija (Decision No.5/16 - OSCE) i Deklaracija o jačanju napora OEBS-a za prevenciju i suzbijanje terorizma (OSCE, 2016). OEBS-ov Forum za bezbednosnu saradnju koji je prevashodno osnovan da prati proces naoružavanja zarad postizanja vojne sigurnosti i stabilnosti u Evropi i koji uključuje neke od najosnovnijih političko-vojnih sporazuma među državama članicama OEBS-a, u svoj rad sve više uključuje razmatranje kiberbezbednosnih izazova i kiberoružja (FSC - *Forum for Security Co-operation*, OSCE).

6.1.7. Evropska Unija (EU)

Evropska Unija takođe poklanja veliku pažnju pitanju kiberbezbednosti. Prema podacima Eurostata do 2018. godine, udeo domaćinstava EU koji imaju internet priključak porastao je na 89%, što je za oko 29 % više nego u 2008. godini. Širokopojasni pristup internetu ima 86% domaćinstava što je približno dvostruko veći udeo od zabeleženog u 2008. godini (48%). Procenat osoba starosne dobi od 16 do 74 godina u Evropskoj Uniji koji su naručili ili kupovali robu ili usluge putem interneta za privatnu upotrebu iznosi oko 60% u 2017. godini (Eurostat Statistics Explained, 2019).

Doprinos Evropske unije u suprotstavljanju kibterorizmu bazira se na Strategiji kiberbezbednosti za dostizanje otvorenog i sigurnijeg kiberprostora. Strategija je usvojena 2013. godine, nakon višegodišnje saradnje zemalja članica Evropske unije u oblasti bezbednosti. Osnovni ciljevi strategije su: jačanje kiberotpornosti, značajnije smanjenje kiber kriminalnih aktivnosti, jačanje mogućnosti kiberodbrane razvijanjem industrijskih i tehnoloških sredstava i stvaranje jedinstvene evropske politike kiberbezbednosti koja je u skladu sa dosadašnjom bezbednosnom i odbrambenom politikom EU koja se bazira na poštovanju i promovisanju osnovnih principa i vrednosti na kojima počiva Evropska unija (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace European Commission, Brussels, 2013).

Zemlje EU su donele i prihvatile Evropsku bezbednosnu agendu (2015 -2020. godine) u okviru koje je posebna pažnja posvećena borbi protiv kiberkriminala i kiberterorizma (The European Agenda on Security, 2015). Usvajanju agende je prethodila Direktiva o bezbednosti mreža i informacija kojom su se članice EU obavezale 2013. godine, koja pored bolje saradnje zagovara i izgradnju kapaciteta svake članice ponaosob za sprovođenje kiberbezbednosti (European Agenda on Security: Questions & Answers, European Commission, 2015). Sve članice EU prema odredbi Evropske komisije usvojile su da „*napad posredstvom informacionih sistema*“ bude kažnjiv kao teroristički akt, ukoliko ima za cilj „*ozbiljnu izmenu ili uništenje političkih, ekonomskih ili socijalnih struktura*“ (Bogdanovski & Petreski, 2016, 64).

Iz navedenog možemo da zaključimo da je međunarodna zajednica itekako sv0esna rizika upotrebe savremenih informaciono-komunikacionih tehnologija i da je problem bezbednosti kiberprostora aktuelna tema koja je neretko razmatrana. Međutim, veliki broj dokumenata i multilateralna saradnja ne garantuju kvalitetnu prevenciju i odbranu ukoliko donešene odluke i usvojena dokumenta postoje samo kao mrtvo slovo na papiru. Odnosno, potrebna je njihova pratkična primena i efikasana operativa.

6.2. Operativno- organizacioni aspekt borbe protiv kiberterorizma na regionalnom i globalnom planu

Pored vladinih organizacija, u svetu postoje mnoge agencije i nevladine organizacije koje se bave kibersigurnošću i odbranom od kiberpretnji, kao što su: Tim za reagovanje na kompjuterske incidente (CSIRT - *Computer Security Incident Response Team*), *Cybercom group* - nordijska IT konsalting kompanija, nevladine organizacije *Human Rights Watch* i *Amnesty International*, organizacija APWG - *Unifying the Global Response to Cybercrime* koja se bavi pružanjem objedinjenog globalnog odgovora na kompjuterski kriminal, ISACI - konzorcijum za postizanje bezbednosti na internetu i mnoge druge.

FIRST (*Forum for Incident Response and Security Teams*) je operativni globalni lider u suočavanju sa pretnjama u kibernetičkom prostoru. Broji više od 400 članova kojima pruža brz odgovor i razmenu informacija, pristup najnovijim dokumentima najbolje prakse i razmenu iskustva na konferencijama.

Vajmen navodi tri koraka za operativno praćenje i nadgledanje terorista na internetu. Prvi korak je nadgledanje terorističkih veb stranica s ciljem praćenja toka terorističkih razmišljanja, motiva, pratilaca terorista i njihovih aktivnosti, planova i potencijalnih ciljeva napada. Drugi korak je prikupljanje podataka sa vebsajtova. Organizacije koje se bore protiv terorizma treba da "*koriste*" terorističke vebsajtove da identifikuju i lociraju propagandiste, moderatore diskusija, internet provajdere, operativce i njihove učesnike. Prikupljeni podaci se arhiviraju i matematički obrađuju zarad identifikacije ključnih osoba ili klastera ljudi unutar mreže i da bi se merila robustnost mreže. Treći korak podrazumeva ometanje terorističkih vebstranica i drugih online platformi na različite načine bilo negativnom kampanjom, kibernapadima - virusima i crvima ili zbunjivanjem terorista i njihovih pristalica lažnim tehničkim informacijama (Weimann, 2015, 188-190).

SIRT (*Security Incident Response Team*) radi po principu detektovanja kiberincidenata pomoću indikatora, zatim se alarmiraju/informišu vojska, lica i organizacije sa spiska („*alert roster*“) i odašilje im se poruka („*alert message*“) - skriptovani opis kiberincidenta, koji pruža dovoljno informacija za adekvatan kiberodgovor.

Nakon što se šteta u potpunosti eliminiše, sledi postupak oporavka, i pre nego što se pređe na svakodnevne rutinske dužnosti, stručnjaci SIRT tima izrađuju precizan izveštaj „*after - action review*“ koji sadrži informacije od prvog koraka (detektovanja kiberincidenta) do poslednjeg koraka (oporavka). Pomenuti izveštaj služi kao obuka osoblja za buduće zaposlene SIRT tima (Mattdort & Whitman, 2011, 283).

Indikatori koji prema Matdortu i Vitmanu upućuju na verovatni kiberincident:

„*1. iznenadne neočekivane aktivnosti (Activities at unexpected times);*

2. pojava novih naloga (Presence of new accounts);

3. prijavljeni napadi (Reported attacks);

4. obaveštenja (Notification from IDS)“ (Mattdort & Whitman, 2011, 278).

Matdort i Vitman takođe navode i šest indikatora koji definitivno potvrđuju kiber napad:

„*1. upotreba neaktivnih naloga (Use of dormant accounts);*

2. promene pristupnih naloga (Changes to logs);

3. prisustvo hakerskih alata (Presence of hacker tools);

4. obaveštenja partnera, saradnika (Notifications by partner of peer);

5. obaveštenja hakera (Notification by hacker)

6. upotreba neobičnih protokola (Use of unusual protocols)“ (Mattdort & Whitman, 2011, 278-279).

Pored Rusije, Kine i Francuske, SAD imaju najsofisticiranije operativno-organizacione sposobnosti odbrane od kiberterorizma. Pomak u realizovanju kiberbezbednosti napravljen je 2008. godine kada je Savezna regulatorna agencija za energetiku (*Federal Electric Regulatory Agency*) propisala mere i pravila koja važe za sve kompanije koje posluju u oblasti energetike, i sankcionisala nepoštovanje tih pravila i procedura novčanom kaznom od milion dolara dnevno (Clarke & Knake, 2010, 88). Vlada SAD-a koristi Ajnštajn (*Einstein*) napredni sistem za nadgledanje mrežne komunikacije i detekciju napada. Kao što navode Klark i Knejk postoje tri dela ovog sistema „*Ajnštajn 1, Ajnštajn 2 i Ajnštajn* 3“ i svaki od njih ima zasebnu funkciju. Prvi deo služi za praćenje protoka saobraćaja, drugi deo služi za otkrivanje upada i malicioznih programa, dok treći deo ima funkciju odbrane, tako što blokira maliciozne programske pakete sa Interneta (Clarke & Knake, 2010, 101-102).

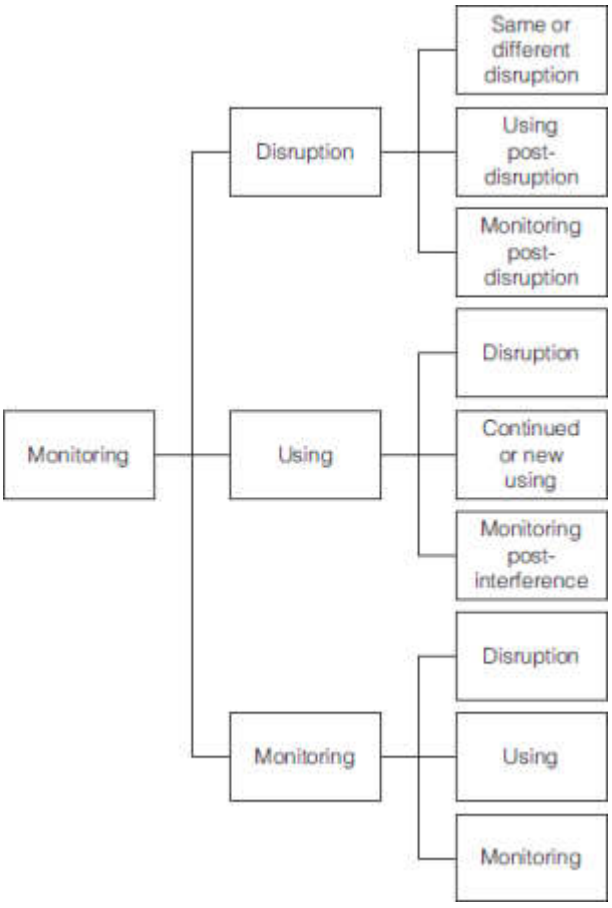
Bezbednost mreže se u SAD povećava zahvaljujući odbrambenoj trijadi: „*kičma (potpora), zaštita mreže snabdevanja električnom energijom i lična zaštita (samozaštita)*“ (Clarke & Knake, 2010, 131-134) koja služi ne samo da stopira različite vrste kibernapada, nego omogućava i jaču kontrolu aktivnosti u kiberprostoru. Dva ključna problema kiberodbrane su tehničke i političke prirode.

Internet saobraćaj je teško pratiti zbog velikog protoka informacija. Elektronski nadzor telekomunikacija podrazumeva elektronsko prisluškivanje telefonskih razgovora i praćenje drugih načina komunikacije, što se kosi sa poštovanjem politike privatnosti. Elektronski nadzor komunikacija se sprovodi prevashodno zbog prikupljanja relevantnih dokaza u sudskom postupku, za otkrivanje mreže članova terorističke organizacije, utvrđivanje hijerarhije i celokupnog kriminalnog delovanja. Ovu metodu mogu da primenjuju jedino zakonski ovlašćene osobe, uz poštovanje određenih načela. Sprovođenju ovih mera pristupa se u slučajevima kada se istragom nije moglo doći do adekvatnih dokaza, ili kada primena prethodnih mera nije dala rezultat, pa se prema tačno navedenom zahtevu koji sadrži „*činjenice, navedene okolnosti pod kojima su iskorišćene sve metode koje nisu davale adekvatan rezultat, kao i razloge zbog kojih se smatra da bi primena metoda tajnog prisluškivanja dala rezultate. Zahtev za prisluškivanje treba da sadrži i vremenski rok u kojem će se sprovoditi nadzor komunikacije koji može trajati do trideset dana, koji se sprovodi na osnovu naredbe nadležnog sudije. Mera nadzora može se produžavati na još trideset dana u nekoliko navrata, takođe uz saglasnost nadležnog sudije*“ (Weaver, Abramson & Bacigal, 2007, 564). Ukoliko okolnosti koje proističu iz terorističke aktivnosti to osobito nalažu, može se primeniti i tajni nadzor lica čiji identitet nije u potpunosti utvrđen, a koja su povezane sa najtežim zločinima, kao i metod prikrivenog islednika. Ovaj metod se ređe primenjuje zbog nedovoljno jasne pravne regulative i teškoća koje proizilaze iz same realizacije planiranih poslova prikrivenog islednika. Većina članova terorističke organizacije je nepoverljiva prema novopridošlicama, što dodatno otežava prodor do vrha terorističke organizacije. Situaciju prikrivenog islednika dodatno komplikuje specifičnost okolnosti „*u slučajevima kada prikriveni islednik treba da učestvuje u zločinu, za šta mu odobrenje daje Odbor za vođenje tajnih istraga u slučajevima nužde, kako bi se pribavile informacije i saznanja koje ostvaruju cilj vođenja krivičnog postupka osumnjičenog; ukoliko bi se na taj način sačuvala verodostojnost prikrivenog islednika ili ukoliko bi na taj način*

prikriveni islednik otklonio od sebe smrtnu opasnost ili opasnost od težeg telesnog povređivanja“ (Jović, 2001, 181).

Na septembarskoj NATO radionici 2006. godine u Izraelu prvi put je predstavljen „*M.U.D model*“ kao vid odgovora na kiberterorizam, koji je potom razmatran u oktobru 2007. na NATO radionici koja je održana u Ankari, u Turskoj. Sajnaj opisuje M.U.D kao višestepeni model koji podrazumeva opcije: monitoringa, odnosno nadgledanje, pasivni nadzor, korišćenje smetnji u internet saobraćaju i online sadržajima kako bi se uklonili štetni materijali i blokirao im se pristup (Sinai 2011, 23-24).

Slika 11. Vizuelna predstava M.U.D. modela (Weimann, 2015, 190).



7. MERE I POSTUPCI ZA SUZBIJANJE KIBERTERORIZMA NA NACIONALNOM PLANU

7.1. Normativno uređenje metoda za suzbijanje kiberterorizma u Srbiji

Geostrateški položaj Srbije i minuli istorijski događaji: građanski rat i raspad nekadašnje Socijalističke Federativne Republike Jugoslavije, NATO bombardovanje, nametnute sankcije Saveznoj Republici Jugoslaviji i problemi tranzicije znatno su oblikovali savremeni položaj Republike Srbije u međunarodnoj zajednici i uticali na njeno celokupno bezbednosno stanje. Najveću savremenu pretnju po bezbednost Republike Srbije predstavljaju separatističke ideje. Problem samoproglašene republike Kosovo je jedan od najznačajnijih faktora destabilizacije i izvora terorističkih težnji na ovim prostorima, što uz nerešen problem izbeglih lica sa prostora bivše Jugoslavije i Sirije dodatno komplikuje bezbednosnu situaciju.

Državni organi Republike Srbije koji u delokrug svojih aktivnosti uključuju oblast razvoja i primene informaciono-komunikacionih tehnologija su:

- Ministarstvo za telekomunikacije i informaciono društvo, nadležno je za izgradnju politike i strategije informacionog društva. Prema „*Zakonu o ministarstvima*“ (Službeni glasnik RS, br. 65/08 i 36/09), prema članu 18 pored ostalih aktivnosti ministarstvo za telekomunikacije i informaciono društvo zaduženo je za: „*utvrđivanje politike i strategije izgradnje informacionog društva; pripremu zakona, drugih propisa, standarda i mera u oblasti elektronskog poslovanja; primenu informatike i interneta; pružanje informacionih usluga; razvoj i unapređenje akademske računarske mreže; koordinaciju u izradi strateško-razvojnih dokumenata na nivou Republike Srbije; razvoj i funkcionisanje informacione infrastrukture, kao i druge poslove određene zakonom*” (Službeni glasnik RS, br. 65/08 i 36/09).

- Ministarstvo za državnu upravu i lokalnu samoupravu u oblasti primene informaciono-komunikacionih tehnologija nadležno je za sistem državne uprave (Službeni glasnik RS, br. 67/91) i „*stručno usavršavanje zaposlenih u državnim organima*” prema „*Zakonu o ministarstvima*”, članu 12 (Službeni glasnik RS, br. 65/08).

- Republički zavod za informatiku i internet, prema *Zakonu o ministarstvima*, član 37: „*obavlja stručne poslove i poslove državne uprave koji se odnose na: unapređenje, razvoj i funkcionisanje informacionog sistema državnih organa, lokalne samouprave i javnih službi; primenu i korišćenje interneta u radu državnih organa, lokalne samouprave i javnih službi; zaštitu podataka; razvoj i primenu standarda u uvođenju informacionih tehnologija u državnim organima, kao i druge poslove određene zakonom*” (Službeni glasnik RS, br. 79/02).

- Uprava za zajedničke poslove republičkih organa (*UZPRO*) pored ostalog nadležna je za „*sistemsku i tehničku podršku iz oblasti informaciono-komunikacionih tehnologija u funkcionisanju Uprave za zajedničke poslove republičkih organa koja podrazumeva: održavanje računarske i komunikacione opreme i lokalnih računarskih mreža, razvoj i održavanje aplikativnog i sistemskog softvera za potrebe Uprave za zajedničke poslove republičkih organa*“ (Službeni glasnik RS, br. 63/13, 73/17 – dr.uredba, 76/17).

- Kancelarija za informacione tehnologije i elektronsku upravu „*obavlja stručne poslove koji se odnose na: projektovanje, usklađivanje, razvoj i funkcionisanje sistema elektronske uprave i informacionih sistema i infrastrukture organa državne uprave i službi Vlade*“ (Službeni glasnik RS, br. 73/17, 8/19). Kancelarija je nadležna za brojne poslove među kojima su: pružanje podrške za razvoj, uvođenje i primenu standarda, održavanje, unapređenje i izgradnju računarske mreže republičkih organa. Takođe obavlja različite „*poslove za potrebe Centra za bezbednost IKT sistema u republičkim organima (CERT republičkih organa); koordinaciju i pružanje podrške za ostvarivanje međunarodne saradnje i poslovanja na globalnom tržištu za digitalne, inovativne i kreativne delatnosti, praćenje i promociju povezivanja javnog i privatnog sektora u oblastima digitalne inovativne kreativne ekonomije*“ (Službeni glasnik RS, br. 73/17, 8/19), kao i druge poslove.

Pored pomenutih i drugi državni organi i organizacije su nadležni za razvoj i implementaciju informacionih sistema (Informacioni sistemi MUP-a, Ministarstva odbrane i Vojske Srbije, Poreske uprave, Uprave carina, Uprave za trezor, Geodetski informacioni sistem i dr.). Vlada Republike Srbije usvojila je 23. decembra 2015. godine „*Strategiju razvoja elektronske uprave u Republici Srbiji za period od 2015 – 2018. i Akcioni plan za sporovođenje Strategije za period 2015-2016. godine*“ (Službeni glasnik RS br. 107/15) kojom se podstiču razvoj i sigurnost elektronske uprave organa javne vlasti.

Vlada Republike Srbije se zalaže za razvoj pametnih mreža, podstiče inovacije i bolju vezu između nauke, tehnologije i preduzetništva i upotrebu kapaciteta nove informacione i komunikacione tehnologije za istraživanje i razvoj otuda je propisala „*Strategiju razvoja mreža nove generacije do 2023. godine*“ ("Službeni glasnik RS", br. 33/18). Sve veća primena savremenih informaciono-komunikacionih tehnologija i digitalizacija podrazumevaju i sve veću uključenost i drugih državnih organa, kao što su: Ministarstvo prosvete, Ministarstvo zdravlja, Ministarstvo pravde i dr.

Ministarstvo prosvete i nauke Republike Srbije poseduje sektor za digitalizaciju, koji je osnovan u cilju sveobuhvatne digitalizacije u skladu sa aktuelnim međunarodnim i nacionalnim standardima. Osnovne aktivnosti ovog sektora su: digitalizacija podataka kojima Ministarstvo prosvete i nauke raspolaže, plansko uvođenje i organizovanje digitalizacije usluga i procesa; uspostavljanje, unapređenje i upravljanje postojećim e-servisima kako bi se oni unapredili za bolje funkcionisanje, postigla veća bezbednost i kontrola dostupnosti podataka. Zbog širokog dijapazona delovanja sektora za digitalizaciju u prosveti i nauci izvršena je njegova podela na tri grupe gde je svaka grupa posebno nadležna za digitalizaciju u: prosveti, nauci i obrazovanju: „*1. grupa za e-Prosvetu, 2. grupa za e-Nauku i 3. grupa za digitalizaciju u obrazovanju*“ (Republika Srbija - Ministarstvo prosvete, nauke i tehnološkog razvoja, 2018, 25). U okviru „*Strategije naučnog i tehnološkog razvoja Republike Srbije za period od 2016. do 2020. godine*“ (Službeni glasnik RS br. 25/16) koju je Vlada Srbije usvojila u martu 2016. godine na predlog Ministarstva prosvete, nauke i tehnološkog razvoja podstiče se razvoj istraživanjem kako bi se došlo do novih inovacija tzv.„*istraživanje za inovacije*“ (Verbić, 2016, 6). Istraživači su dali najbolje rezultate u oblasti elektronike, telekomunikacija i informacionih tehnologija. „*Od ukupnog broja novih tehničkih rešenja, 38% su rezultati u ovim oblastima, od kojih je već 90 % komercijalizovano na domaćem ili međunarodnom tržištu*“ (Verbić, 2016, 34). Vlada Republike Srbije i Evropska Unija potpisale su sporazum kojim je dogovoreno da Republika Srbija bude deo programa *Horizont 2020* koji podrazumeva davanje grantova za realizaciju istraživačkih projekata, što umnogome potpomaže razvoj i primenu novih standarda i ideja.

Imajući u vidu da je kiberterorizam kao i svaki oblik terorizma u tesnoj vezi sa nasiljem, dokument koji se indirektno odnosi na kiberterorizam je „*Pravilnik o protokolu postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemarivanje*“ (Službeni glasnik RS, br. 46/19) koji je usvojilo Ministarstvo prosvete. Prema pomenutom dokumentu nasilje se ne definiše jedino kao fizičko ili psihičko (emocionalno) ili pak socijalno zlostavljanje, nego uključuje i elektronsko nasilje. „*Elektronsko nasilje i zlostavljanje je zloupotreba informacionih tehnologija koja može da ima za posledicu povredu druge ličnosti i ugrožavanje dostojanstva i ostvaruje se slanjem poruka elektronskom poštom, SMS-om, MMS-om, putem veb-sajta (web site), četovanjem, uključivanjem u forume, socijalne mreže i sl.*“ (Službeni glasnik RS, br. 46/19). Postojanje svesti o elektronskom nasilju je korak napred u prepoznavanju i razlikovanju elektronskog nasilja uopšte, ali i onog elektronskog nasilja koje ima političku konotaciju.

Primena informaciono-komunikacionih tehnologija u oblasti trgovine i telekomunikacija je u nadležnosti Ministarstva trgovine turizma i telekomunikacija koje je na osnovu: „*Zakona o elektronskom dokumentu, elektronskoj identifikaciji i ulugama od poverenja u elektronskom poslovanju*“ (Službeni glasnik RS, br. 94/17) usvojilo sledeće pravilnike i uredbe:

- „*Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati*“ (Službeni glasnik RS, br. 34/18 i 81/18)
- „*Pravilnik o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata i uslovima koje mora da ispunjava imenovano telo*“ (Službeni glasnik RS, br. 34/18)
- „*Pravilnik o Registru pružalaca kvalifikovanih usluga od poverenja*“ (Službeni glasnik RS, br.31/18)
- „*Pravilnik o Registru kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata*“ (Službeni glasnik RS, br. 31/18)
- „*Uredba o uslovima za pružanje kvalifikovanih usluga od poverenja*“ (Službeni glasnik RS, br. 37/18)
- „*Uredba o bližem uređenju uslova koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti*“ (Službeni glasnik RS, br. 60/18)
- „*Pravilnik o Registru pružalaca usluga elektronske identifikacije i šema elektronske identifikacije*“ (Službeni glasnik RS, br. 67/18)

U okviru „*Zakona o informacionoj bezbednosti*“ (Službeni glasnik RS, br. 6/16, 94/17) usvojene su sledeće uredbe i pravilnik:

- „*Uredba o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja*” (Službeni glasnik RS, br. 94/16)
- „*Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenta i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja*” (Službeni glasnik RS, br. 94/16)
- „*Uredba o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja*” (Službeni glasnik RS, br. 94/16)

- „*Uredba o utvrđivanju liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja*" (Službeni glasnik RS, br. 94/16)
- „*Pravilnik o bližim uslovima za upis u Evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima*" (Službeni glasnik RS, br. 12/17)

Ministarstvo trgovine turizma i telekomunikacija takođe je usvojilo:

- „*Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija*" (Službeni glasnik RS, br. 61/16)
- „*Pravilnik o izboru programa od javnog interesa u oblasti razvoja informacionog društva koje realizuju udruženja*" (Službeni glasnik RS, br. 47/13 i br. 88/16)
- „*Pravilnik o zahtevima za uređaje i programsku podršku za zakonito presretanje elektronskih komunikacija i tehničkim zahtevima za ispunjenje obaveze zadržavanja podataka o elektronskim komunikacijama*" (Službeni glasnik RS, br. 88/15) prema kojem „*zakonito presretanje elektronskih komunikacija obuhvata otkrivanje sadržaja komunikacija i nadzor podataka o saobraćaju subjekta nadzora u skladu sa zakonom; zadržani podaci su podaci o elektronskim komunikacijama koje je operator dužan da zadrži u skladu sa Zakonom o elektronskim komunikacijama*" (Službeni glasnik RS, br. 88/15, Uvodne odredbe, član 2).

Na predlog Republičke agencije za elektronske komunikacije Ministarstvo spoljne i unutrašnje trgovine i telekomunikacija usvojilo je „*Pravilnik o tehničkim i drugim zahtevima pri izgradnji prateće infrastrukture potrebne za postavljanje elektronskih komunikacionih mreža, pripadajućih sredstava i elektronske komunikacione opreme prilikom izgradnje poslovnih i stambenih objekata*" (Službeni glasnik RS, br. 123/12) u kojem je definisano značenje pojedinih izraza kao što su: razne vrste aplikacija, kao što su: aplikacije radiodifuznih i komunikacionih tehnologija (*BCT – broadcast and communication technology applications*), aplikacije informaciono-komunikacionih tehnologija (*ICT - information and communications technology applications*), aplikacije upravljanja, nadzora i komunikacije (*CCB - commands, controls and communications in building*), *ICT – information and communications technology* usluge i dr.

Oblast informacionog društva u Republici Srbiji je regulisana brojnim zakonima, od kojih su najznačajniji:

- „*Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*“ (Sl. glasnik RS, br. 61/05 i 104/09) reguliše otkrivanje, krivično gonjenje i suđenje za krivična dela koja spadaju u oblast visokotehnološkog kriminala. Prema članu 2: „*Visokotehnološki kriminal u smislu ovog zakona predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku*“ (Sl. glasnik RS, br. 61/05 i 104/09).

- „*Zakon o elektronskim komunikacijama*“ (Službeni glasnik RS, br. 44/10, 60/13 – US, 62/14 i 95/18) uređuje uslove za obavljanje i razvoj delatnosti u oblasti elektronskih komunikacija, reguliše dostupnost usluga uz poštovanje domaćih i međunarodnih standarda i procedura, osigurava bezbednost komunikacionih mreža i usluga, kao i zaštitu podataka korisnika elektronskih komunikacija i dr.

- „*Zakon o informacionoj bezbednosti*“ (Službeni glasnik RS, br. 6/16, 94/17) reguliše mere zaštite informaciono-komunikacionog sistema (IKT sistem), uređuje međunarodnu saradnju u oblasti informacione bezbednosti, prevenciju i zaštitu od bezbednosnih rizika, upravljanje rizikom, kriptobezbednost, kriptozaštita, tajnost podataka, kriptografski proizvod, kriptomaterijali i dr. „*Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite*” (Službeni glasnik RS, br. 6/16, 94/17).

- „*Zakon o elektronskoj trgovini*“ (Službeni glasnik RS, br. 41/09, 95/13, 52/19) propisuje mere kojima se uređuje pružanje usluga informacionog društva, uslovi koje je pružalac usluga dužan da poštuje, obavezne informacije koje je dužan da dostavi korisniku usluga (potrošaču) i nadzornom telu (Inspektorat za usluge informacionog društva), obaveze potrošača, kao i zahteve koje moraju da zadovolje komercijalna poruka i elektronski ugovor za dostizanje punovažnosti, privremeno i trajno skladištenje podataka i kaznene odredbe za prekršaje.

- „*Zakon o elektronskom dokumentu, elektronskoj identifikaciji i ulugama od poverenja u elektronskom poslovanju*“ (Službeni glasnik RS, br. 94/17). Ovim zakonom se uređuje elektronsko poslovanje i ostali elementi neophodni za obavljanje elektronske usluge, kao što su: elektronska identifikacija, digitalizovani dokument i elektronski potpis, elektronski pečat, elektronski vremenski žig, validacija ispravnosti elektronskog potpisa i pečata, sertifikat za elektronski potpis, sertifikat za autentikaciju vebsajta i drugo. U stavki VII Zakona o elektronskom dokumentu, elektronskoj identifikaciji i ulugama od poverenja u elektronskom poslovanju, član 66-71 propisane su novčane kazne u rasponu od 50.000 do 2.000.000 rsd u zavisnosti od prekršaja (Službeni glasnik RS, br. 94/17).

- „*Zakon o upravnim sporovima*“ (Službeni glasnik RS, br.111/09) pored toga što reguliše predmet upravnog spora reguliše i ostale uslove vezane za predaju tužbe u obliku elektronskog dokumenta kao što je navedeno u članu 20 i postupanje sa elektronskim dokumentima prema članu 21. „*Način, tehničke uslove predaje i utvrđivanje vremena predaje podnesaka i dostave akata u obliku elektronskog dokumenta, kao i druga pitanja vezana za postupanje sa elektronskim dokumentom, bliže se uređuju Sudskim poslovnikom*“ (Službeni glasnik RS, br.111/09).

- „*Zakon o zaštiti podataka o ličnosti*“ (Službeni glasnik RS, br. 87/18) član 1: „*Ovim zakonom uređuje se pravo na zaštitu fizičkih lica u vezi sa obradom podataka o ličnosti i slobodni protok takvih podataka, načela obrade, prava lica na koje se podaci odnose, obaveze rukovalaca i obrađivača podataka o ličnosti, kodeks postupanja, prenos podataka o ličnosti u druge države i međunarodne organizacije, nadzor nad sprovođenjem ovog zakona, pravna sredstva, odgovornost i kazne u slučaju povrede prava fizičkih lica u vezi sa obradom podataka o ličnosti, kao i posebni slučajevi obrade*” i „*pravo na zaštitu fizičkih lica u vezi sa obradom podata*”(Službeni glasnik RS, br. 87/18).

- „*Zakon o elektronskoj upravi*“ (Službeni glasnik RS, br. 27/18) propisuje načela za efikasno i sigurno upravljanje opremom i sistemom elektronske uprave, evidenciju u elektronskom obliku (uspostavljanje i vođenje registara), korišćenje i zaštitu baza podataka, čuvanje bezbednosnih kopija baza podataka i dokumenata; propisuje pravilnosti njihovog pribavljanja i ustupanja, propisuje jedinstveni nalog elektronske pošte, licence za uspostavljanje i vođenje veb portala, kao i njegovu upotrebu, zabranu diskriminacije, prekršajnu odgovornost i dr.

- „*Zakon o platnim uslugama*“ (Službeni glasnik RS, br. 139/14, 44/18) uređuje oblast platnih transakcija, platni račun, platni nalog, platne instrumente, zaštita prava i interesa korisnika platnih usluga (platilaca i primalaca plaćanja) i imalaca elektronskog novca, uređuje referentni kurs, gotov i elektronski novac, kamatnu stopu, uslove i način pružanja domaćih i međunarodnih platnih transakcija, dozvoljeno i nedozvoljeno prekoračenje računa, vrste platnih usluga, uređuje devizno poslovanje, platni sistem i njegov nadzor.

- „*Zakon o oglašavanju*” (Službeni glasnik RS, br. 6/16, 52/19 – dr. zakon) uređuje oblast oglašavanja u najširem smislu (tv oglašavanje, u štampanim medijima, na otvorenim površinama, u elektronskim medijima), bilo da je u pitanju javno oglašavanje ili poslovno za plasiranje određenih proizvoda/usluga, pravila i ograničenja vezana za sadržaj oglasnih poruka, odgovornost prenosioca oglasne poruke, propisuje zabranu podsticanja bilo koje vrste diskriminacije, ugrožavanje bezbednosti i zdravlja, obmane, prikriveno oglašavanje i dr. Tako u članu 6 koji propisuje društvenu odgovornost stoji: „*Oglašavanje mora biti zasnovano na principu korišćenja dozvoljenih sredstava za postizanje cilja i drugim principima društvene odgovornosti. Oglasnom porukom se ne sme izazivati mržnja ili netolerancija, zloupotrebljavati poverenje, odnos zavisnosti, lakovernost, nedostatak iskustva ili znanja i sujeverje primalaca oglasne poruke. Oglasna poruka ne sme da sadrži izjave ili vizuelno predstavljanje koje se može smatrati uvredljivim. Oglasna poruka mora da bude istinita, u skladu sa zakonom, dobrim poslovnim običajima lojalne konkurencije i profesionalnom etikom*” (Službeni glasnik RS, br. 6/16, 52/19 – dr. zakon).

- „*Krivični zakonik*“ (Službeni glasnik RS, br. 85/05, 88/05- ispravka, 107/05 – ispravka, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19) zabranjuje terorizam, odnosno:

- „*diverzija, sabotaža, špijunaža, odavanje državne tajne, izazivanje nacionalne, rasne i verske mržnje i netrpeljivosti, povreda teritorijalnog suvereniteta, udruživanje radi protivustavne delatnosti, pripremanje dela protiv ustavnog uređenja i bezbednosti Srbije, teška dela protiv ustavnog uređenja i bezbednosti Srbije*“ (član 312- član 321)

- „*javno podsticanje na izvršenje terorističkih dela*“ (član 391)

- „*vrbovanje i obučavanje za vršenje terorističkih dela*“ (član 391a, 3916)

- „*upotreba smrtonosne naprave*“ (član 391v)

- „*uništenje i oštećenje nuklearnog objekta*“ (član 391g)

- „*ugrožavanje lica pod međunarodnom zaštitom*“ (član 392)

- „*finansiranje terorizma*“ (član 393)

- „*terorističko udruživanje*“ (član 393a)

Srbija je u martu 2009. godine ratifikovala Konvenciju Saveta Evrope o kiberkriminalu, koja je doneta 23. novembra 2001. godine u Budimpešti. Počev od 1. januara 2006. godine stupio je na snagu „*Krivični zakonik*“ (Službeni glasnik RS, br. 85/05, 88/05- ispravka, 107/05- ispravka, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19), u kojem su propisana „*Krivična dela protiv bezbednosti računarskih podataka*“ (glavi br. XXVII, čl. 298. do čl. 304a) sledeća krivična dela:

- oštećenje računarskih podataka i programa - „*Ko neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program, kazniće se novčanom kaznom ili zatvorom do jedne godine*“ (član 298).

- računarska sabotaža – „*Ko unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest meseci do pet godina*“ (član 299).

- pravljenje i unošenje računarskih virusa – „*Ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili zatvorom do dve godine*“ (član 300, stav 1 i stav 2).

- računarska prevara –„*Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine*“ (član 301, stav 1). Ranih 80-tih godina se pojavila prevara pod imenom „*nigerijska prevara*“ ili „*prevara 419*“ koja podrazumeva krivično delo prevare koje se vrši pomoću računara, tako što pošiljaoc elektronske poruke, koja je najčešće u *spam*-u, traži inostranu pomoć oko transfera velike količine novca iz Nigerije, gde je pošiljaoc elektronske poruke spreman da učinjenu uslugu novčano nadoknadi određenim procentom od prebačene sume (Urošević, 2009, 2-3).

Celokupan proces se čuva u strogoj tajnosti. Sadržaj elektronskih poruka je u suštini isti, bez obzira na sitnije detalje koji mogu da se razlikuju. Prevaranti se najčešće služe ukradenim identitetima lica koja zaista postoje, a nisu ni svesna da neko zloupotrebljava njihov identitet za vršenje kriminalne radnje. Najčešće su izvršioci krivičnih dela pripadnici manjih organizovanih kriminalnih grupa, nekada deluju i samostalno, ali tada najčešće nisu u mogućnosti da izvrše prevare većih razmera. Ukoliko žrtva pristane na elektronski poslatu ponudu, izvršioci krivičnih dela traže žrtvi da uplati određeni novčani iznos na ime realizacije dogovorenog posla i šalju joj falsifikovana dokumenata i traže nova odlaganja uz obećanje brze isplate dogovorenog procenta. Kada žrtva shvati da je prevarena, tada je već kasno i uplaćeni novac ne može nikako da povrati nazad.

- neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka – „*Ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko snimi ili upotrebi podatak dobijen na način predviđen u stavu 1. ovog člana, kazniće se novčanom kaznom ili zatvorom do dve godine*“ (član 302, stav 1 i 2).

- sprečavanje i organičavanje pristupa javnoj računarskoj mreži – „*Ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, kazniće se novčanom kaznom ili zatvorom do jedne godine*“ (član 303)

- neovlašćeno korišćenje računara ili računarske mreže – „*Ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili zatvorom do tri meseca*“ (član 304)

- pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka – Prema „*Krivičnom zakoniku Republike Srbije*” zabranjena je proizvodnja, upotreba, uvoz, prodaja, distribucija i nabavka uređaja i računarskih programa, računarske šifre ili sličnih podataka koji su prvenstveno projektovani u svrhe izvršenja nekog krivičnog dela zatvorskom kaznom od šest meseci do tri godine ili novčanom kaznom (član 304 a).

- nezakonito rukovanje elektronskim novcem - Prema „*Zakonu o platnim uslugama*” (Službeni glasnik RS, br. 139/14, 44/18), član 2, tačka 13: „*elektronski novac označava elektronski (uključujući magnetno) pohranjenu novčanu vrednost koja čini novčano potraživanje prema izdavaocu tog novca, a izdata je nakon prijema novčanih sredstava radi izvršavanja*

platnih transakcija i prihvata je fizičko i/ili pravno lice koje nije izdavalac tog novca“. Narodna banka Srbije ima ovlašćenje da posredno ili neposredno proveri usluge koje se naplaćuju elektronskim novcem, i ukoliko pravno ili fizičko lice ne omogući Narodnoj banci Srbije tražene informacije i dokumentaciju u roku, prema Zakonu o platnim uslugama, član 182. (Službeni glasnik RS, br. 139/14, 44/18) Narodna banka Srbije može tom licu da propiše novčanu kaznu od: „*100.000 do 500.000 dinara za pravna lica i od 30.000 do 100.000 dinara za odgovorna lica u pravnom licu; od 30.000 do 100.000 dinara za fizička lica*“.

Više javno tužilaštvo u Beogradu je nadležno za krivično gonjenje svih krivičnih dela koja su izvršena pomoću visoke tehnologije, prema odredbama „*Zakona o javnom tužilaštvu*“ (Službeni glasnik RS, br. 116/08, 104/09, 101/10, 78/11 - dr. zakon, 101/11, 38/12 - odluka US, 121/12, 101/13, 111/14 - odluka US, 117/14, 106/15, 63/16-US). Posebno tužilaštvo za visokotehnološki kriminal osnovano je 2006. godine. Pri Višem sudu u Beogradu za sva suđenja visokotehnološkog kriminala nadležno je Odeljenje koje je posebno formirano za borbu protiv pomenute vrste kriminala, dok je Apelacioni sud u Beogradu nadležan za postupanje po pravnim lekovima.

Uporedo sa normativnim razvojem i primenom pomenutih zakona u Republici Srbiji usložnjavala se i primena informaciono-komunikacionih tehnologija u javnoj administraciji i privatnom sektoru. Kako bi uredila oblast informacionog društva Vlada Republike Srbije je usvojila različite strategije, uredbe i akcione planove:

- „*Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine*“ (Službeni glasnik RS, br. 55/05, 71/05-ispravka, 101/07 i 65/08)

- „*Strategija razvoja telekomunikacija u Republici Srbiji od 2006. do 2010. godine*“ (Službeni glasnik RS, br. 99/06 i 4/09);

- „*Strategija razvoja širokopojasnog pristupa u Republici Srbiji do 2012. godine*“ (Službeni glasnik RS, broj 84/09);

- „*Strategija razvoja širokopojasnih mreža i servisa u Republici Srbiji do 2016. godine*“ (Službeni glasnik RS, br. 81/14);

- „*Strategija razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine*“ (Službeni glasnik RS, br. 68/10)

- „*Strategija razvoja elektronske uprave za period od 2009. do 2013. godine*“ zajedno sa Akcionim planom (Službeni glasnik RS, br. 83/09 i 5/10). Deo dugoročnog Akcionog plana koji je usvojila Vlada je modernizacija državne uprave E-uprava. Mere i aktivnosti za razvoj e-uprave, prioriteti i načela propisani su ovom strategijom;

- „*Strategija razvoja elektronske uprave u Republici Srbiji za period od 2015 – 2018. i Akcioni plan za sporovođenje strategije za period 2015-2016. godine*“ (Službeni glasnik RS br. 107/15)

- „*Strategija naučnog i tehnološkog razvoja Republike Srbije u periodu od 2010. do 2015. godine*“ („Službeni glasnik RS”, br. 13/10);

- „*Strategija naučnog i tehnološkog razvoja Republike Srbije u periodu od 2016. do 2020. godine - Istraživanje za inovacije*“ (Službeni glasnik RS, br. 25/16)

- „*Strategija razvoja industrije informacionih tehnologija za period od 2017. do 2020. godine*“ (Službeni glasnik RS, br. 95/16) čijim objavljivanjem je prestala da važi prethodno donešena „*Strategija razvoja i podrške industriji informacionih tehnologija*“ (Službeni glasnik RS, br. 25/13)

- „*Strategija zaštite podataka o ličnosti*“ (Službeni glasnik RS, br. 58/10)

- „*Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine*“ (Službeni glasnik RS, br. 53/17)

- „*Strategija razvoja mreža nove generacije do 2023. godine“* (Službeni glasnik RS, br. 33/18)

- „*Strategija za prelazak sa analognog na digitalno emitovanje radio i televizijskog programa u Republici Srbiji*“ (Službeni glasnik RS, br. 52/09, 18/12 i 26/13).

- „*Uredba o Programu rada, razvoja i organizaciji integrisanog zdravstvenog informacionog sistema „e-Zdravlje*” (Službeni glasnik RS, br. 55/09)

- „*Akcioni plan (2013-2014) za sprovođenje Strategije razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine*“ (Službeni glasnik RS, br. 26/13)

- „*Akcioni plan za efikasno korišćenje telekomunikacione infrastrukture“* (Službeni glasnik RS, br. 36/17);

- „*Strategija za borbu protiv visokotehnološkog kriminala za period od 2019. do 2023. godine*“ (Službeni glasnik RS, br. 71/18)

- „*Akcioni plan za period 2018. do 2019. god. za sprovođenje Strategije razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine*“(Službeni glasnik RS, br. 67/18)

- „*Akcioni plan za sprovođenje Strategije naučnog i tehnološkog razvoja Republike Srbije od 2016. do 2020. godine – Istraživanja za inovacije*“ (Službeni glasnik RS, br. 60/18)

- „*Akcioni plan za period od 2018 - 2019. god. za sprovođenje Strategije razvoja informacionog društva u Republici Srbiji za period do 2020.godine*“ (Službeni glasnik RS, br. 14/18)

- „*Akcioni plan za 2018. godinu za sprovođenje Strategija razvoja industrije informacionih tehnologija za period od 2017. do 2020. godine*“ (Službeni glasnik RS, br. 7/18).

Pored pomenutih strategija, uredbe i akcionih planova, ključnu ulogu za suzbijanje kiberterorizma na nacionalnom planu imaju:

- „*Nacionalna strategija za sprečavanje i borbu protiv terorizma za period 2017-2021. godine*“ (Službeni glasnik RS, br. 94/17)

-„*Strategija nacionalne bezbednosti Republike Srbije*“ (Službeni glasnik RS, br. 88/09) i „*Strategija odbrane Republike Srbije*“ (Službeni glasnik RS, br. 88/09). Prema Zakonu odbrane „*Strategija nacionalne bezbednosti Republike Srbije je najviši strateški dokument čijom realizacijom se štite nacionalni interesi Republike Srbije od izazova, rizika i pretnji bezbednosti u različitim oblastima društvenog života*“. Dok, „*Strategija odbrane Republike Srbije je najviši strateški dokument u oblasti odbrane kojim se definišu stavovi o bezbednosnom okruženju, odbrambenim interesima, misijama i zadacima Vojske Srbije, struktura i funkcionisanje sistema odbrane*“ (Službeni glasnik RS, br. 116/2007, 88/2009, 88/2009 - dr. zakon, 104/2009 - dr. zakon, 10/2015 i 36/2018).

- „*Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma*“ (Službeni glasnik RS, broj 89/08 i 3/15)

- „*SEE Agenda za razvoj informacionog društva*“ (Službeni glasnik RS, broj 29/09) i drugo.

7.1.1. Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma

Prvi značajniji korak Vlade Republike Srbije u borbi protiv terorizma bio je 25. septembra. 2008. godine kada je usvojena „*Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma*“ (Službeni glasnik RS, broj 89/08), sa osnovnim ciljem postizanja efikasne sveobuhvatne borbe protiv finansiranja terorizma i pranja novca, odnosno da „*u potpunosti zaštiti finansijski sistem i privredu države od opasnosti koje uzrokuju pranje novca i finansiranje terorizma i širenje oružja za masovno uništenje, čime se jača integritet finansijskog sektora i doprinosi bezbednosti i sigurnosti*“ (Službeni glasnik RS, broj 89/08). Ova nacionalna strategija Republike Srbije je bila prvi korak u oblasti borbe protiv pranja novca i finansiranja terorizma.

Pranje novca se odnosi na nezakonito prikrivanje porekla novca ili imovine koji su stečeni na bespravan način, kriminalnim aktivnostima. Podrazumeva tri faze: „*faza ulaganja, faza raslojavanja ili prikrivanja, faza integracije*“ (Službeni glasnik RS, broj 89/08). Finansiranje terorizma se odvija u nekoliko faza. Prva faza je prikupljanje sredstava. Teroristi pribavljaju sredstva koja su stečena vršenjem raznih krivičnih dela kao što su trgovina drogom, prevare i slično. Služe se različitim metodama kao što su iznude, otmice da prikupe sredstava iz novčanih izvora koja su stečena na zakoniti način, ali ih teroristi protivpravno prisvajaju. Takođe pribavljaju sredstva od donacija koje dobijaju od simpatizera koji podržavaju ciljeve terorističkih organizacija. Druga faza podrazumeva, čuvanje prikupljenih sredstava na različite načine. Treća faza je prenos sredstava radi njegovog operativnog korišćenja. Prenos se obavlja na različite načine od krijumčarenja preko državnih granica do korišćenja raznovrsnih mehanizama za pranje novca. Poslednja četvrta faza je upotreba finansijskih sredstava u terorističke svrhe.

„*Osnovni ciljevi ove strategije su:*

1. preventivnim i represivnim merama uticati na smanjenje kriminaliteta u vezi sa pranjem novca i finansiranja terorizma;

2. implementirati međunarodne standarde čije sprovođenje omogućava članstvo ili povoljniji status države u međunarodnim organizacijama;

3. razviti sistem saradnje i odgovornosti svih učesnika u borbi protiv pranja novca i finansiranja terorizma;

4. unaprediti saradnju javnog i privatnog sektora na planu borbe protiv pranja novca i finansiranja terorizma;

5. obezbediti transparentnost finansijskog sistema“ (Službeni glasnik RS, broj 89/08).

U periodu od 2008. do 2015. godine usvojeni su novi međunarodni standardi u oblasti sprečavanja pranja novca i finansiranja teorizma, te je u skladu sa time usvojena nova „*Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma*“ 2015. godine. U okviru „*Nacionalne strategije za borbu protiv pranja novca i finansiranja terorizma*“ osnovni cilj se sprovodi „*kroz četiri strateške teme, i to:*

- Smanjivanje rizika od pranja novca i finansiranja terorizma kroz strateško planiranje, koordinaciju i saradnju svih učesnika u sistemu;

- Sprečavanje unošenja imovine za koju se sumnja da je stečena krivičnim delom u finansijski sistem i druge sektore, odnosno otkrivanje i prijavljivanje već unete imovine;

- Uočavanje i otklanjanje pretnji od pranja novca i finansiranja terorizma, kažnjavanje izvršilaca krivičnih dela i oduzimanje nezakonito stečene imovine;

- Kvalifikovani kadrovi osposobljeni za delotvorno učešće u svim segmentima sistema za borbu protiv pranja novca i finansiranja terorizma i razumevanje u javnosti uloge i planova nadležnih organa“ (Službeni glasnik RS, broj 89/08 i 3/15).

Da bi Strategija bila delotvorna zagovara se saradnja svih nadležnih državnih organa „*kroz razmenu informacija i ekspertize, pristup bazama podataka i obrazovanje radnih timova*“ (Službeni glasnik RS, broj 89/08 i 3/15).

Glavni učesnici za sprovođenje pomenute strategije navedeni su: Uprava za sprečavanje pranja novca, Republičko javno tužilaštvo, sudovi, policija, Vojno-bezbednosna agencija (VBA), Vojno-obaveštajna agencija, Bezbednosno-informativna agencija (BIA), Narodna banka Srbije (NBS), Komisija za hartije od vrednosti, Sektor tržišne inspekcije, Uprava carina, Porska uprava, Agencija za borbu protiv korupcije, Pravosudna akademija i Kriminalističko-policijska akademija, Udruženje banaka Srbije i Advokatska komora Srbije. U skladu sa pomenutom strategijom donešen je i akcioni plan, koji pokriva redom sve četiri strateške teme (Službeni glasnik RS, broj 89/08 i 3/15).

7.1.2. Nacionalna strategija za sprečavanje i borbu protiv terorizma za period od 2017-2021. godine

Republika Srbija je u nastojanju da očuva mir i stabilnost na regionalnom i globalnom planu potpisnica mnogih najznačajnijih međunarodnih dokumenata iz oblasti borbe protiv terorizma. Da bi se na nacionalnom planu obezbedila od terorističkih pretnji i opasnosti koje one sa sobom nose, 2017. godine je usvojena „*Nacionalna strategija za sprečavanje i borbu protiv terorizma za period od 2017-2021. godine*“ (Službeni glasnik RS, br. 94/17).

Strategija nudi osnovne smernice za unapređenje postojećih metoda i mera borbe protiv terorozma, i razvoj novih metoda borbe i mehanizama prevencije, „*sa ciljem da uspostavi proporciju između obima angažovanih resursa i stepena pretnje. Ova strategija ima za svrhu zaštitu Republike Srbije od terorističke pretnje po njene građane, vrednosti i interese, uz istovremeno podržavanje međunarodnih napora u borbi protiv terorizma*“ (Službeni glasnik RS, br. 94/17).

Strategijom su predviđene četiri prioritetne oblasti za čije sprovođenje su predloženi sledeći ciljevi:

- Prva oblast „*Prevencija terorizma nasilnog ekstremizma i radikalizacije koji vode u terorizam*“ (Službeni glasnik RS, br. 94/17) sprovodi se pomoću pet ciljeva:

1. „*Izgrađena bezbednosna kultura građana*“ – podrazumeva formalno i neformalno edukovanje koje će omogućiti podizanje svesti o pretnjama i opasnostima od terorizma na viši nivo, pa samim time i njegovo izbegavanje, lakše uočavanje i alarmiranje nadležnih organa.

2. „*Rana identifikacija uzroka i faktora koji pogoduju širenju nasilnog ekstremizma i radikalizacije koji vode u terorizam*“ – omogućava planiranje i koordinaciju, pa samim time i stvaranje povoljnijeg ambijenta i uključivanje svih činilaca društva za borbu protiv terorizma.

3. „*Okruženje koje demotiviše regrutovanje mladih za učešće u terorističkim aktivnostima*“ – omogućava jačanje svesti kod mladih i jačanje demotivišućih elemenata koji sprečavaju mlade da se opredele za terorizam kao vid ispoljavanja nezadovoljstva i delovanja protiv postojećeg društveno-političkog sistema.

4. „*Visokotehnološki sistemi komunikacije i digitalnih mreža koji su otporni na širenje radikalizacije i nasilnog ekstremizma*“ – stavljanje ovih sistema u službu bezbednosne politike.

5. „*Veština strateške komunikacije*“ – podrazumeva planski usmerenu komunikaciju i onemogućavanje bilo kakve zlonamerne komunikacije i interpretacije u službi terorizma i ekstremističkih poruka (Službeni glasnik RS, br. 94/17).

Druga oblast, „*Zaštita, uočavanje i otklanjanje pretnji od terorizma i slabosti u sistemu zaštite*“, sprovodi se pomoću:

1) „*Potpuno razumevanje pretnji od terorizma u Republici Srbiji kroz ranu identifikaciju ciljanih grupa i radikalnih metoda;*

2) *Unapređena koordinacija i saradnja između državnih organa nadležnih za prikupljanje obaveštajnih podataka;*

3) Podignut nivo operativnih sposobnosti policijskih i obaveštajno-bezbednosnih kapaciteta;

4) Unapređen sistem za borbu protiv finansiranja terorizma;

5) Deradikalizacija i reintegracija radikalizovanih osoba;

6) Podignut nivo zaštite kritične infrastrukture;

7) Unapređena efikasnost mehanizama integrisanog upravljanja granicom;

8) Podignut nivo bezbednosti u oblasti transporta, trgovine, razmene roba i usluga“ (Službeni glasnik RS, br. 94/17)

Treća oblast, „*Krivično gonjenje terorista, uz poštovanje ljudskih prava, vladavine prava i demokratije*“ predloženo je da se sprovede pomoću tri cilja:

1. „*Usklađeni nacionalni propisi sa odgovarajućim rezolucijama Saveta bezbednosti Ujedinjenih nacija, pravnim tekovinama Evropske unije i drugim međunarodnim standardima*

2. *Unapređen sistem otkrivanja, identifikacije i krivičnog gonjenja izvršilaca krivičnog dela terorizam i krivičnih dela povezanih sa terorizmom, uz poštovanje ljudskih prava*

3. *Efikasno suđenje za krivično delo terorizam i druga krivična dela povezana sa terorizmom*“ (Službeni glasnik RS, br. 94/17)

Četvrta oblast, „*Odgovor sistema u slučaju terorističkog napada*“ (Službeni glasnik RS, br. 94/17) predloženo je da se sprovodi kroz:

1) „*Unapređen sistem upravljanja posledicama terorističkog napada*“ i

2) „*Smanjenje posledica terorističkog napada*“ (Službeni glasnik RS, br. 94/2017). Strategijom su predviđeni sprovođenje, praćenje, koordinacija i finansiranje u cilju sprečavanja i borbe protiv terorizma.

7.1.3. Odluka o usvajanju Strategije nacionalne bezbednosti Republike Srbije

Na osnovu člana 99. stav 1. tačka 7. Ustava Republike Srbije, člana 9. stav 2. tačka 2 „*Zakona o odbrani*“ (Službeni glasnik RS, broj 116/07), a u vezi sa članom 136. Poslovnika Narodne skupštine Republike Srbije (Službeni glasnik RS, br. 14/09– prečišćen tekst), Narodna skupština je oktobra 2009. godine donela „*Odluku o usvajanju Strategije nacionalne bezbednosti Republike Srbije*“ (Službeni glasnik RS, br. 88/09).

U drugom poglavlju „*Strategije nacionalne bezbednosti Republike Srbije*“ (Službeni glasnik RS, br. 88/09) navedeni su osnovni rizici, izazovi i pretnje po nacionalnu bezbednost: separatistička nastojanja pojedinih nacionalističkih i verskih ekstremističkih grupa, naročito albanske nacionalne manjine na Kosovu i Metohiji, jednostrano proglašena nezavisnost Kosova, nacionalni i verski ekstremizam, terorizam i njegova povezanost sa drugim oblicima kriminala (organizovani, transnacionalni i prekogranični), nerešen status i težak položaj izbeglih, prognanih i interno raseljenih lica, povećan rizika od visokotehnološkog kriminala i dr.

Terorizam se smatra jednim od najvećih rizika i pretnji za globalnu, regionalnu i nacionalnu bezbednost. U Strategiji je takođe naveden rizik od ugrožavanja bezbednosti informacionih i telekomunikacionih sistema. Tehnološki razvoj treba usmeriti tako da bude u funkciji razvoja društva i jačanja nacionalne bezbednosti. Jer, se na taj način stvara dobra osnova za ubrzan razvoj odbrambene industrije i njenu primenu. Otuda je u Strategiji predložena „*celovita integracija u međunarodni sistem komunikacija i informacija i razvoj strateškog partnerstva sa državama koje su nosioci savremenih tehnologija*“ (Službeni glasnik RS, br. 88/09).

U poglavlju 4 navedeno je da je politika unutrašnje bezbednosti usmerena prevashodno na: „*zaštitu ustavnog poretka, života i imovine građana, sprečavanje i suzbijanje svih oblika terorizma, organizovanog, finansijskog, ekonomskog i visokotehnološkog kriminala, korupcije, pranja novca, trgovine ljudima, narkomanije, proliferacije konvencionalnog naoružanja i oružja za masovno uništenje, obaveštajnih i subverzivnih delatnosti, kao i drugih izazova, rizika i pretnji bezbednosti. Za ostvarivanje ciljeva politike unutrašnje bezbednosti poseban značaj ima stalno unapređivanje informativne i preventivne delatnosti*“ (Službeni glasnik RS, br. 88/09).

U „*Strategiji nacionalne bezbednosti Republike Srbije*“ (Službeni glasnik RS, br. 88/09) pominje se da je primećena tendencija za intenzivnije korišćenje informaciono-komunikacionih tehnologija, pa samim time i „*konstantno povećanje rizika od visokotehnološkog kriminala i ugrožavanja informacionih i telekomunikacionih sistema. Rizik u ovom pogledu postoji od ugrožavanja spolja, ali i u mogućnosti zloupotrebe podataka o građanima i pravnim licima*“ (Službeni glasnik RS, br. 88/09). U okviru politike tehnološkog razvoja koji je u funkciji razvoja društva i jačanja nacionalne bezbednosti podstiče se tehnološki razvoj usvajanjem savremenih tehnologija, kao i održavanje i razvijanje strateškog partnerstva sa državama koje imaju vodeću ulogu u razvoju savremenih tehnologija. Očuvanje bezbednosti Republike Srbije je dinamičan proces, koji zahteva stalno unapređivanje i prilagođavanje savremenoj društveno-političkoj situaciji u Republici Srbiji.

Adekvatna zaštita od kiberterorizma podrazumeva organizovanje stručnih tela za koordinaciju radi sprečavanja i suzbijanja kiberterorizma, po uzoru na organizovanje takvih tela u drugim zemljama. Međunarodni i nacionalni programi koji predlažu i propisuju mere bezbednosti i zaštite od kiberterorizma predlažu blagovremeno otkrivanje kiberterorističkih pretnji kroz: adekvatnu procenu opasnosti, otkrivanje ugrožavajućih terorističkih organizacija, njihovih planova, ciljeva i motiva, tehnoloških sredstava i znanja kojima teoristi raspolažu, koordinaciju policijskih organa i protivterorističkih snaga na nacionalnom, regionalnom i međunarodnom nivou, blagovremeno otkrivanje i savlađivanje potencijalnih napadača u kiberprostoru radi efikasnog sprečavanja izvođenja kiberterorističkog napada i onemogućavanja daljih aktivnosti napadača, blagovremeno lišavanje slobode, efikasno vođenje istražnog postupka, adekvatnim suđenjem i strogim kažnjavanjem napadača, programe vaspitnog usmeravanja radi odvraćanja od kiberterorizma. Složenost i specifičnost kiberterorizma zahteva neprekidne napore, usavršavanje mera zaštite, istraživanje i usaglašavanje mera bezbednosti na međunarodnom nivou.

7.1.4. Odluka o usvajanju Strategije odbrane Republike Srbije

Vojskom Srbije komanduje Predsednik Srbije u miru i ratu. Dok, Vlada predlaže Narodnoj Skupštini Republike Srbije politiku odbrane koja se sprovodi u skladu sa međunarodnim pravom i obavezama. U skladu sa nacionalnim i odbrambenim interesima Republika Srbija izgrađuje potrebne kapacitete i sposobnosti koje su neophodne za odbranu od savremenih bezbednosnih pretnji.

„*Odluka o usvajanju Strategije odbrane Republike Srbije*“ doneta je na osnovu člana 99. stav 1. tačka 9. Ustava Republike Srbije, člana 9. stav 2. tačka 3 „*Zakona o odbrani*“ (Službeni glasnik RS, broj 116/07), a u vezi sa članom 136. Poslovnika Narodne skupštine Republike Srbije (Službeni glasnik RS, broj 14/09 – prečišćen tekst). „*Strategija odbrane Republike Srbije*“ (Službeni glasnik RS, broj 88/09) usmerena je na dostizanje razvoja društva i jačanje nacionalne bezbednosti, zaštitu suverenosti i teritorijalne celovitosti i pružanje podrške civilnim vlastima u suprotstavljanju od pretnji kojima se narušava bezbednost.

„*Elementarne nepogode i hemijske, biološke, nuklearne, tehničke i tehnološke nesreće stalna su bezbednosna pretnja za Republiku Srbiju, njeno stanovništvo, materijalna dobra i životnu sredinu. Negativne posledice ovih pojava mogu da zahvate i ugroze teritorije susednih država, a isto tako se mogu sa teritorija susednih država proširiti na Republiku Srbiju i ugroziti njenu teritoriju i stanovništvo*“ (Službeni glasnik RS, broj 88/09). Strategijom se predlaže unapređivanje odnosa i saradnja sa bezbednosnim službama drugih zemalja na osnovu međunarodnih i bilateralnih ugovora i sporazuma radi postizanja kolektivne bezbednosti.

Terorizam i svi njegovi pojavni oblici prepoznati su kao ozbiljna bezbednosna pretnja. „*Separatističke težnje, posebno zastupljene kod pojedinih nacionalističkih i verskih ekstremističkih grupa, kao i interesnih organizacija, predstavljaju izvor stalnog bezbednosnog rizika i direktnu pretnju teritorijalnoj celovitosti Republike Srbije*“ (Službeni glasnik RS, broj 88/09). U zavisnosti od mogućnosti i stepena ugroženosti države planiraju i razvijaju antiterorističke timove. „*Republika Srbija organizuje i razvija antiterorističke timove u sastavu vojnih oružanih i policijskih snaga*“ (Pejanović & Bejatović, 2009, 270). Kao što Pejanović ukazuje antiteroristički timovi pri vojnim snagama usmereni su na elitne, brze, organizovane i efikasne vojne operacije kao oblik suprostavljanja terorističkom delovanju (Pejanović, 2003, 87).

Ministarstvo odbrane Republike Srbije izradilo je Nacrt strategije nacionalne bezbednosti Republike Srbije i Strategije odbrane Republike Srbije 2017. godine. Prema novom Nacrtu predlaže se jačanje domaće odbrambene industrije, tehnološka modernizacija oružanih snaga, razvoj sposobnosti i potencijala odbrambene industrije, naučno-tehnološki razvoj, međunarodni projekti i širenje tržišta odbrambene industrije, kao i plasiranje domaće vojne opreme u Evropi i u svetu. Specijalne elitne jedinice za protivterorističkа dejstva pouzdano mogu da deluju ukoliko sprovode sopstvena istraživanja i sarađuju sa policijskim antiterorističkim jedinicama i drugim obaveštajnim organima i službama.

7.1.5. Strategija za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine

Vlada Republike Srbije je podstaknuta pregovorima sa Evropskom Unijom u okviru „*Poglavlja 24 – pravda, sloboda, bezbednost*“ (Ministarstvo unutrašnjih poslova, 2015) usvojila „*Strategiju za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine*“ (Službeni glasnik RS, broj 71/18).

U okviru pomenute Strategije kao krucijalne pretnje u oblasti visokotehnološkog kriminala su prepoznate:

„*1) kriminal koji zavisi od napednih tehnologija;*

2)“onlajn” seklsualna ekspoloatacija dece;

3) prevare vezane za plaćanje;

4)“onlajn” kriminalna tržišta;

5) preplitanje sajber kriminala i terorizma;

6) unakrsni faktori kriminala;

7) „onlajn” trgovina falsifikovanom robom” (Službeni glasnik RS, broj 71/18).

„*Strategija za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine*“ (Službeni glasnik RS, broj 71/18) sadrži predloge i preporuke za suočavanje sa prethodno navedenim pretnjama. Predlaže se detaljnija analiza pretnji i sagledavanje adekvatnih inicijativa za pružanje *online* bezbednosti i odbrane, kroz fokusiranje na vršioce kiberkriminala i najčešće identifikovana sredstva koja su korišćena za izvršenje kiberkriminala (*trojanci*, *malveri*, dobavljači neophodnih sredstava za izvršenje *DDoS* napada i dr.), razvijanje antivirusa i drugih mehanizama za adekvatno i efikasno reagovanje na pomenute pretnje; ističe se važnost koordinacije i saradnje između državnih organa nadležnih za sporovođenje zakona u oblasti visokotehnološkog kriminala i privatnog sektora koji koristi usluge savremenih informaciono-komunikacionih tehnologija, zagovara se dostupnost mera i istraživačkih sredstava za potrebe istraživanja, analize i evidentiranja *online* organizovanog kriminala, predlaže se održavanje zajedničke prevencije na nivou cele zajednice, edukacija roditelja i dece radi upoznavanja sa pretnjama od seksualne eksploatacije dece putem interneta i ostalih savremenih tehnoloških sredstava komunikacije, globalna saradnja za destabilizaciju *darknet-a*.

7.1.6. Nacionalna strategija održivog razvoja

Osnovni cilj „*Nacionalne strategije održivog razvoja*“ (Službeni glasnik RS, broj 57/08) je: „*da dovede do ravnoteže tri ključna faktora, odnosno tri stuba održivog razvoja: održivog ekonomskog rasta i privrednog i tehnološkog razvoja, održivog razvoja društva na bazi socijalne ravnoteže, zaštite životne sredine uz racionalno raspolaganje prirodnim resursima, spajajući ih u jednu celinu podržanu odgovarajućim institucionalnim okvirom*“ (Službeni glasnik RS, broj 57/08). „*Nacionalna strategija održivog razvoja*“ (Službeni glasnik RS, broj 57/08) prevashodno je orjentisana na dugoročno održiv sveobuhvatni razvoj društva, odnosno svih aspekata: „*ekonomskih, socijalnih, ekoloških i institucionalnih na svim nivoima*“, što zahteva usklađivanje i unapređenje pomenutih aspekata i rešavanje konflikata, kao i snažnu političku podršku, vođstvo, kako društvenu tako i medijsku podršku i unapređivanje atraktivnosti zemlje.

Osnovne postavke održivog razvoja:

- u ekonomskom smislu podrazumevaju razvoj znanja za održivi razvoj proizvodnje i potrošnje, odabir odgovarajuće ekonomske politike koja je u skladu sa ciljevima na nacionalnom (mikroekonomskom) i makroekonomskom planu, tranzicionim tokovima, razvoj i primena informaciono-komunikacionih tehnologija u ekonomskom sektoru koja je u skladu sa nacionalnom naučnotehnološkom politikom uz očuvanje i zaštitu intelektualne svojine i dr.

- u socijalnom smislu održivi razvoj se odnosi na razvoj i unapređenje svih društvenih postavki, razvoj kulture, populacione i inkluzivne politike, unapređenje kvaliteta života, smanjenje siromaštva i nezaposlenosti, otvaranje novih radnih mesta, društveno odgovorno poslovanje, borba protiv diskriminacije, uključivanje ranjivih i socijalno izolovanih društvenih grupa i dr.

- u ekološkom smislu podrazumeva očuvanje životne sredine, prirodnih resursa, smanjenje štetnih uticaja i rizika zagađenja pametnom ekološki svesnom proizvodnjom i dr.

- institucionalni okvir se odnosi na jačanje i razvoj stabilnih institucija koje posluju u skladu sa EU propisima i pravnom regulativom, članstvo u EU.

Kao ključni nacionalni prioriteti Republike Srbije za ostvarenje vizije održivog razvoja do 2017. godine navedeni su:

„*1) članstvo u EU;*

2) razvoj konkurentne tržišne privrede i uravnotežen ekonomski rast, podsticanje inovacija, stvaranje boljih veza između nauke, tehnologije i preduzetništva, povećanje kapaciteta za istraživanje i razvoj, uključujući nove informacione i komunikacione tehnologije;

3) razvoj i obrazovanje ljudi;

4) razvoj infrastrukture i ravnomeran regionalni razvoj ;

5) zaštita i unapređenje životne sredine uz racionalnu potrošnju prirodnih resursa“ (Službeni glasnik RS, broj 57/08).

U okviru „*Nacionalne strategije održivog razvoja*“ (Službeni glasnik RS, broj 57/08) predlaže se „*veći oslonac na informacione i komunikacione tehnologije koje omogućavaju nove radne aranžmane (rad od kuće, rad sa skraćenim i fleksibilnim radnim vremenom), povećanje upotrebe i učinka kodifikovnog znanja, kao i smanjivanje troškova širenja znanja*”. Stoga su kao podrška konceptu održivog razvoja usvojene ostale strategije koje se odnose konkretno na razvoj informaciono-komunikacionih tehnologija u Republici Srbiji.

7.1.7. eSEE Agenda za razvoj informacionog društva

Može se reći da je prvi značajniji korak u oblasti razvoja i uređenja informacionog društva na prostorima Jugoistočne Evrope načinjen 4. juna 2002. godine u Ljubljani kada je usvojena „*eSEE Agenda za razvoj informacionog društva*“ (Pakt za stabilnost u Jugoistočnoj Evropi- Inicijativa, 2002) koja je potpisana od strane učesnika u Beogradu 29. oktobra 2002. godine. Ovom Inicijativom se podstiče razvoj informacionog društva tokom perioda od 2007. do 2012. godine prema predviđenom razvojnom okviru gde su prioriteti razvijanje:

- „*jedinstvenog JIE informacionog prostora*“ (Službeni glasnik RS, broj 29/09) kroz: razvijanje brzog i bezbednog pristupa raznovrsnim sadržajima pomoću širokopojasnih mreža mobilne komunikacije i bezbednih servisa, stimulisanje razvoja digitalnog sadržaja i njihova što šira primena u različitim oblastima od javnog značaja (obrazovanje, nauka, kultura, zdravstvo i dr.). Da bi se omogućila kompatibilnost i saradnja predložen je razvoj nacionalnih okvira interoperabilnosti za administracije, harmonizacija propisa i podataka kroz uvođenje javnih ključeva kako bi se zaštitili elektronski identiteti i potpisi i učinilo e-poslovanje i trgovina bezbednim na domaćem i regionalnom nivou.

- „*inovacije i investicije na poljima ICT istraživanja i obrazovanja*“ (Službeni glasnik RS, broj 29/09) što se postiže kroz: obaveznu kompjutersku pismenost i pristup internetu u svim školama, unapređenje obrazovnog sistema, investicije za bolju opremljenost škola i razvoj informaciono-komunikacione infrastrukture u obrazovnim institucijama, pospešivanje istraživanja i stručnih treninga, bolju povezanost razvojem akademskih i istraživačkih mreža.

- „*inkluzivno informaciono društvo*“ (Službeni glasnik RS, broj 29/09) - jednake mogućnosti za pristup tehnologiji bez obzira na rod i druge socio-demografske karakteristike, reforme državne administracije zarad osposobljavanja javnih servisa, podsticanje razvoja E-uprave, E- poslovanja, digitalizacije bibliotečko- informacionih sistema, podsticanje e-Učešće građana i pravnih lica.

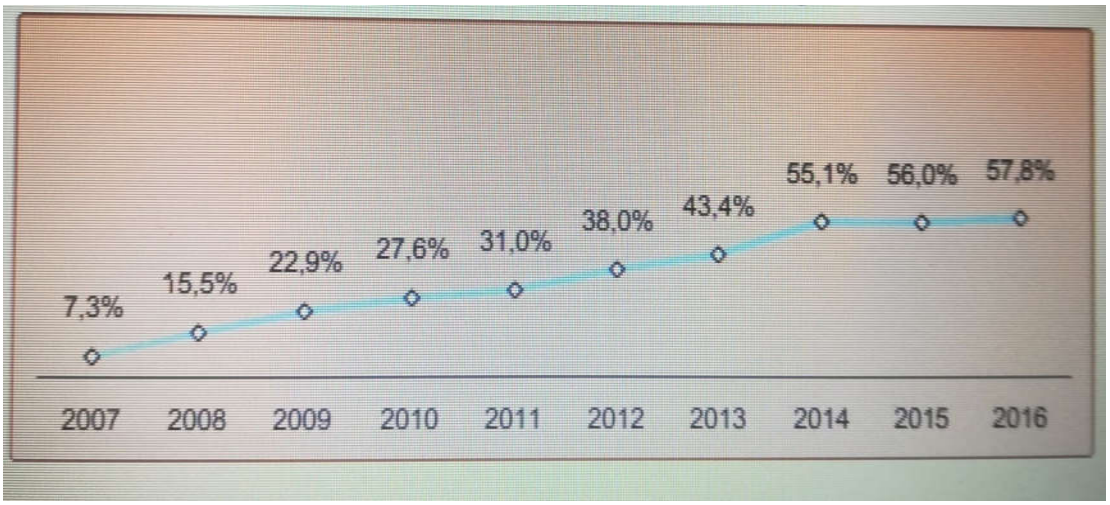
„*eSEE Agenda za razvoj informacionog društva*“ (Službeni glasnik RS, broj 29/09) predstavlja opšti okvir koji je Vlada Republike Srbije usvojila, što je podstaklo dalje izradu i usvajanje različitih strategija kojima se uređuje i podstiče razvoj oblasti informacionog društva.

7.1.8. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine

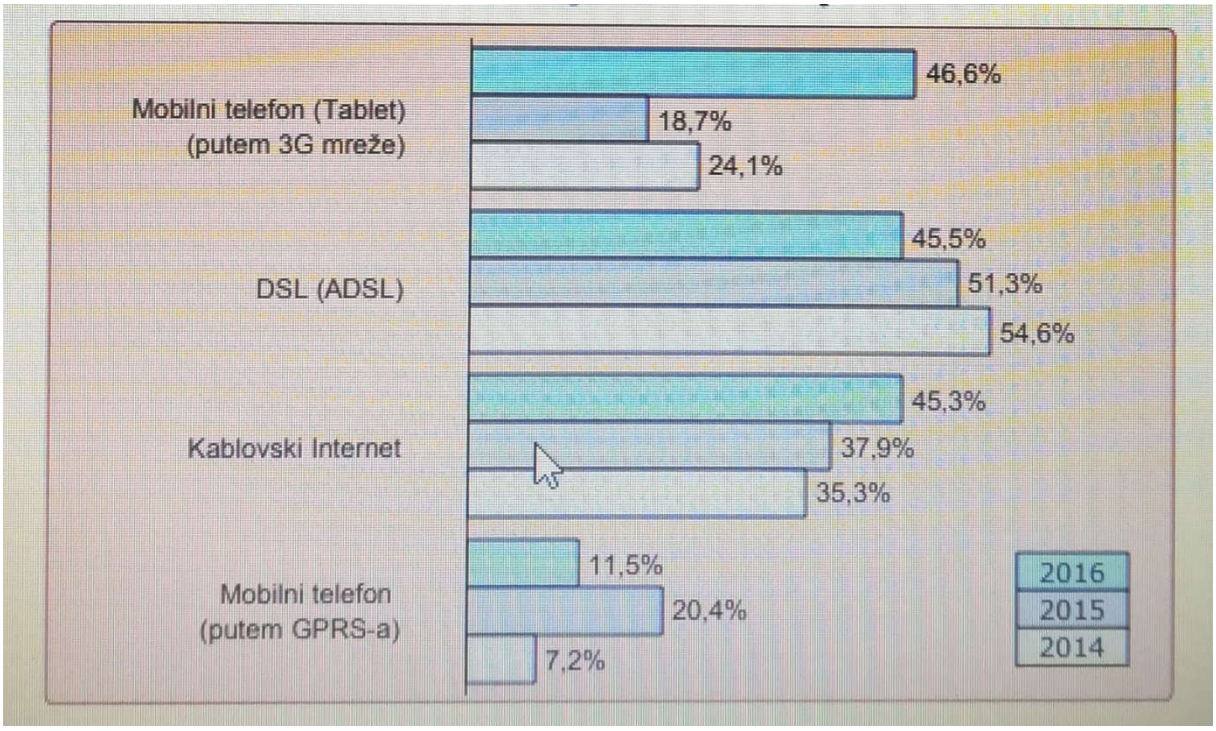
Vlada je usvojila „*Strategiju razvoja informacionog društva u Republici Srbiji do 2020. godine*“ na osnovu člana 45. stav 1. „*Zakona o Vladi*“ (Službeni glasnik RS, br. 55/05, 71/05-ispravka, 101/07 i 65/08). Prvi akt Vlade Srbije kojim se uređuje oblast informacionog društva donešen je 2006. godine kada je usvojena „*Strategija razvoja informacionog društva u RS*“ (Službeni glasnik RS, broj 87/06) koja je prestala da bude na snazi donošenjem nove strategije 2010. godine.

Strateški se usmerava razvoj informacionog društva na iskoristivost potencijala informaciono-komunikacionih tehnologija kako u oblasti rada, tako i u svakodnevnom životu zarad boljeg kvaliteta života. Jedan od ciljeva strategije je dostizanje pristupa širokopojasnom internetu po uzoru na prosek u zemaljama Evropske unije, što podrazumeva da cene i uslovi budu kao i u EU.

Slika 12. Širokopojasna internet konekcija u domaćinstvima (Kovačević, Pavlović & Šutić, 2016, 17)



Slika 13. Tip internet konekcije (Kovačević, Pavlović & Šutić, 2016, 17)



Iz priloženog možemo videti trend porasta broja domaćinstava u Republici Srbiji koja imaju širokopojasnu internet konekciju, koja je iznosila 2007. godine 7,3%, 2012. godine 38%, a 2016. godine 57,8% (Kovačević, Pavlović & Šutić, 2016, 17).

„*Strategijom razvoja informacionog društva u Republici Srbiji do 2020. godine*“ (Službeni glasnik RS, br. 51/10) je predviđeno šest ključnih oblasti na koje treba da bude usmeren razvoj informaciono-komunikacionih tehnologija i njihova primena:

1. „*Elektronske komunikacije*“ – podrazumeva nastojanje da internet visokog kvaliteta sa protokom koji nije manji od 100 Mb/s, odnosno 520 Kb/s kod mobilnog pristupa bude dostupan svim građanima u RS, digitalizaciju radio i televizijskog programa, reformu komunikacione infrastrukture javnog sektora.

2. „*E-uprava, e-zdravstvo i e-pravosuđe*“- primena IKT i elektronskih sertifikata prema „*Zakonu o elektronskom potpisu*“ (Službeni glasnik RS, br. 135/04) i „*Zakonu o elektronskom dokumentu*“ (Službeni glasnik RS, br. 51/09) omogućava građanima da bez obaveznog fizičkog prisustva obavljaju određene poslove brže i jeftinije u službama i organima javne uprave, pravosuđu i zdravstvenoj zaštiti.

3. „*IKT u obrazovanju, nauci i kulturi*“ – podrazumeva opremljenost ustanova, ali i primenu IKT u oblasti nauke, obrazovanja i kulture. Formirana akademska računarska mreža omogućava bržu i lakšu razmenu znanja i iskustva, istraživanja i inovacija što dalje pospešuje multidisciplinarnu primenu tehnologije.

4. „*Elektronska trgovina (e-trgovina)*“ - podsticanje razvoja i širenje dela tržišta primenom elektronskih usluga (elektronski računi i plaćanje i dr.) u oblasti trgovine. To podrazumeva određene izmene kojima se otklanjaju normativne i tržišne prepreke čija je osnovna svrha zaštita potrošača i bezbedna e-trgovina. Afirmisanje e-trgovine bio je jedan od prioritetnih ciljeva „*Strategije razvoja trgovine u Republici Srbiji*“ (Službeni glasnik RS, br. 55/05, 71/05-ispravka, 101/07 i 65/08).

5. „*Poslovni sektor IKT*“ – Strategijom se podstiče upotreba, proizvodnja i izvoz IKT opreme i IT usluga, razvijanje IT sektora start-up projektima i podsticanjem inovativnih kompanija, razvoj ljudskih resursa i „*zaštita intelektualne svojine softvera i digitalnih sadržaja*“.

6. „*Informaciona bezbednost*“ - podrazumeva uređenje svih aspekata primene IKT pomoću četiri stavki: „*1. unapređenje pravnog i institucionalnog okvira za informacionu bezbednost, 2. zaštita kritične infrastrukture 3. borba protiv visokotehnološkog kriminala, 4. Naučno-istraživački i razvojni rad u oblasti informacione bezbednosti*“ (Službeni glasnik RS, br. 51/10).

7.1.9. Strategija razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine

Primena savremenih tehnologija poboljšava kvalitet života. Razvoj elektronskih komunikacija je sastavni deo svih oblasti društvenog razvoja. Dok je, neosporna njihova sve značajnija upotreba u gotovo svim oblastima društvenog, ali i državnog delovanja. Širokopojasni pristup internetu i njegova primena u globalnoj i nacionalnoj privredi doprinosi povezivanju svih delova Republike Srbije što pospešuje razvoj ruralnih i udaljenih oblasti i njihovo intenzivnije uključivanje u nacionalnu privredu. Kako bi budući tok razvoja elektronskih komunikacija, uključujući i telekomunikacije bio usmeren u skladu sa relevantnim međunarodnim dokumentima i predviđenom modelu nacionalne mreže elektronskih komunikacija, Vlada Republike Srbije usvojila je „*Strategiju razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine*“ (Službeni glasnik RS, broj 68/10).

„*Elektronske komunikacije podrazumevaju svako emitovanje, prenos ili prijem poruka (govor, zvuk, tekst, slika ili podaci) u vidu signala, korišćenjem žičnih, radio, optičkih ili drugih elektromagnetskih sistema*“ (Službeni glasnik RS, broj 68/10). Kiberteroristi se uglavnom služe elektronskim komunikacijama zbog njihovih brojnih prednosti. Zato, iako se pomenuta „*Strategija razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine*“ (Službeni glasnik RS, broj 68/10) ne odnosi direktno na mere odbrane i borbe protiv kiberterorizma, njome se uređuje oblast elektronskih komunikacija tako što se ograničava njihovo korišćenje, i na osnovu „*Zakona o elektronskim komunikacijama*“ (Službeni glasnik RS, br. 44/2010, 60/2013 - odluka US, 62/2014 i 95/2018 - dr. zakon) sankcioniše zloupotreba usluga elektronskih komunikacija i telekomunikacija. Prema članu 137 „*Zakona o elektronskim komunikacijama*“ (Službeni glasnik RS, broj 68/10) za prekršaje u oblasti elektronskih komunikacija predviđena je novčana kazna pravnom licu u iznosu od 100.000 do 2.000.000 dinara u zavisnosti od prekršaja.

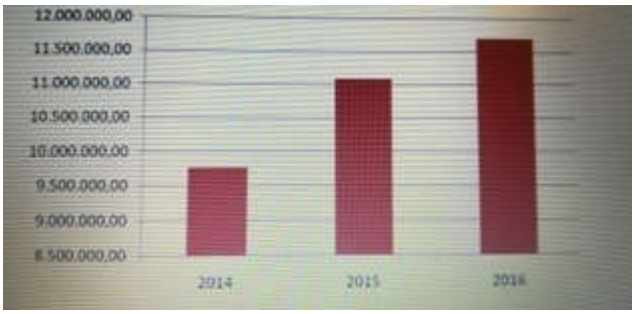
„*Strategijom razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine*“ (Službeni glasnik RS, broj 68/10) projektovan je okvir za primenu novih tehnologija u oblasti elektronskih komunikacija kako bi se razvio sektor industrije u ovoj oblasti, povećao

indeks konkurentnosti Republike Srbije i pratio razvoj servisa prema predviđenom modelu nacionalne mreže elektronskih komunikacija uz poštovanje zahteva za ispunjenje određenog tehnološkog okvira kojim su obuhvaćene: kablovske i bežične mreže, konvergencija mreža i servisa, radiofrenkvencijski spektar, energetska efikasnost mreža elektronskih komunikacija, upravljanje radiofrekvencijskim spektrom, mreže koje služe za emitovanje radio i televizijskog programa (kablovska i digitalna televizija) i razmene otvorenih servisa po otvorenim mrežama elektronskih komunikacija u Republici Srbiji (Službeni glasnik RS, broj 68/10).

7.1.10. Strategija razvoja industrije informacionih tehnologija za period od 2017. do 2020. godine

Sistematska podrška za jačanje i razvoj industrije informacionih tehnologija u Republici Srbiji stvara podsticajan ambijent i predstavlja šansu za privredni razvoj i ekonomski rast naše zemlje. Otuda je Vlada Republike Srbije usvojila „*Strategiju razvoja industrije informacionih tehnologija za period od 2017. do 2020. godine*" (Službeni glasnik RS, broj 95/16) s ciljem da se iskoriste i unaprede proizvodni i izvozni kapaciteti srpske industrije softvera, podstakne i podrži razvoj domaćih IT kompanija, promoviše srpska industrija informacionih tehnologija i unapredi njen položaj na svetskom tržištu. „*Prema podacima iz studije „IT industrija Srbije, 2015–2017." u periodu od 2006. godine srpska IT industrija značajno se razvila. Danas u IT industriji posluje blizu 2.000 preduzeća (700 više nego 2006. godine), broj zaposlenih dupliran je sa 10.000 (2006) na 20.000, a duplirani su i poslovni prihodi na preko 1,5 milijardu evra. Ukupan sopstveni kapital od 2006. povećan je sa 150 miliona na pola milijarde evra. Godišnje se osniva preko 200 IT firmi*" (Službeni glasnik RS, broj 95/16). Iz priloženih podataka nesumnjivo možemo zaključiti da IT industrija Srbije beleži pozitivan rast. Privredni subjekti čija oblast poslovanja se ne odnosi direktno na informaciono-tehnološku industriju, takođe su prepoznali savremeni trend razvoja i primenjuju nove tehnologije u svom poslovanju, čime se stvara pozitivan ambijent i postiže bolja konkurentnost Republike Srbije u oblasti savremenih tehnologija. Takođe je primetan rastući trend na tržištu softvera. Prema navodima Komisije za zaštitu konkurencije u 2016. godini ostvareni prihodi od prodaje softvera beleže „*rast od 20%*" (RS, Komisija za zaštitu konkurencije, 2017, 22) u odnosu na 2014. godinu, slika 14.

Slika 14. Prihod od veleprodaje softvera (u 000 rsd) (RS, Komisija za zaštitu konkurencije, 2017, 22)



Strategijom se pružaju različite mere podrške u oblasti informacionih tehnologija za razvoj preduzeća i plasiranje proizvoda kroz određene *startup* projekte, podsticajnu poresku politiku, modernizaciju poslovanja privrednih subjekata u svim privrednim granama, unapređenje i jačanje ljudskih resursa (kontinuiranjim praćenjem savremenih inovacija i načinima njihove primene, dokvalifikacijama i prekvalifikacijama kadrova) u oblasti informacionih tehnologija, plansko razvijanje bolje iskoristivosti postojećih kapaciteta: tehnoloških parkova i centara, modernizaciju industrije informacionih tehnologija i njeno promovisanje, pružanjem odgovarajućeg unapređenog pravnog okvira u skladu sa savremenim međunarodnim propisima koji pogoduju daljem razvoju industrije informacionih tehnologija u Republici Srbiji.

7.1.11. Strategija razvoja mreža nove generacije do 2023. godine

Vlada Republike Srbije usvojila je 3.maja 2018. godine „*Strategiju razvoja mreža nove generacije do 2023. godine*" (Službeni glanik RS, broj 33/18) radi ostvarenja održivog tehnološkog razvoja, ostvarenja bolje konkurentske pozicije na tržištu kroz inovacije, sistemske promene i investicije, produktivnu edukaciju i zapošljavanje kadrova, povećanje digitalne pismenosti, jačanje socijalne inkluzije, usaglašavannje sa pravnim regulativama Evropske Unije.

„*Strategija razvoja mreža nove generacije do 2023. godine*" (Službeni glanik RS, broj 33/18) predlaže razvoj „*jedinstvenog digitalnog tržišta zasnovanog na brzom i ultrabrzom internetu i interopreabilnim operacijama*" (Službeni glasnik RS, broj 33/18) njegovu najširu primenu u istraživačkoj praksi, poslovanju, privredi i svakodnevnim potrebama domaćinstva radi prevazilaženja krize, finansijske i ekonomske na osnovu tri temeljna cilja koja su prikazana u Tabeli 11. Povodom negovanja dobre komunikacije sa Evropskom Unijom i približavanja njenim standardima i pravnim regulativama pomenuta „*Strategija razvoja mreža nove generacije do 2023. godine*" (Službeni glanik RS, broj 33/18) je u skladu sa strategijom „*Evropa 2020: Strategija za pametni, održiv inkluzivni rast*" (Kronja, 2011) koju je 2010. godine usvojila Evropska Unija. Otuda je Republika Srbija usvojila inicijativu Evropske Unije za stvaranje „*jedinstvenog digitalnog tržišta*" (Službeni glanik RS, broj 33/18).

Tabela 11. Ciljevi jedinstvenog digitalnog tržišta (Službeni glasnik RS, broj 33/18).

Jedinstveno digitalno tržište		
Bolji pristup digitalnim dobrima i servisima	Okruženje u kome digitalne mreže i servisi mogu da se razvijaju	Digitalizacija kao pokretač razvoja
Pravila prekogranične internet prodaje	Telekomunikaciona pravila	Jačanje privrede koja se temelji na podacima
Poboljšanje prekogranične dostave paketa	Pravila o audiovizuelnim medijima	Prioriteti za norme i ineteroperabilnost
Ukidanje „geografskog blokiranja"	Procena uloge internet platformi	Izgradnja jedinstvenog digitalnog tržišta
Reforma evropskog zakona i autorskim pravima	Borba protiv nezakonitih internet sadržaja	
Smanjenje birokratije povezane sa PDV-om	Postupanje ličnih podataka u digitalnim uslugama	
	Javno-privatno partnerstvo o sajbersigurnosti	

7.1.12. Strategija zaštite podataka o ličnosti

Sve do pred kraj 2008. godine Republika Srbija je jedna od retkih zemalja u kojoj nije postojao zakon kojim se uređuje zaštita podataka o ličnosti. Zato je Vlada Srbije usvojila „*Strategiju zaštite podataka o ličnosti*“ (Službeni glasnik RS, br. 58/10) na osnovu „*Zakona o Vladi*“, član 45. stav 1 (Službeni glasnik RS, br. 55/05, 71/05- ispravka, 101/07 i 65/08).

Pre nego što započne postupak prikupljanja i obrade podataka o ličnosti, rukovalac podataka je dužan da u pismenom obliku o tome obavesti lice na koje se odnose podaci o pravnom osnovu, svrsi i načinu korišćenja podataka, njegovim pravima i dr. Ukoliko ne postoji osnov u propisima, bez pristanka lica obrada podataka o ličnosti nije moguća.

„*Zakon o zaštiti podataka o ličnosti uređuje i prava i zaštitu prava lica čiji se podaci obrađuju. U vezi sa zaštitom podataka o ličnosti, lice čiji se podaci obrađuju, ima sledeća prava: pravo na obaveštenje o obradi, pravo na uvid, pravo na kopiju i prava povodom izvršenog uvida (pod kojim se podrazumeva da lice ima pravo da od rukovaoca zahteva ispravku, dopunu, ažuriranje, brisanje podataka kao i prekid i privremenu obustavu obrade. Postupak ostvarivanja ovih prava detaljno je uređen Zakonom*“ (Službeni glasnik RS, br. 58/10, IV glava, stav 2).

Da bi se podaci o ličnosti obrađivali na zakonit način, neophodna je primena informacionih tehnologija koje su zaštićene takvim merama obezbeđenja koje omogućavaju ovlašćenom rukovaocu podataka da u bilo kom trenutku ima pristup podacima, kao što su: datum kada su podaci obrađivani, menjani ili korišćeni od strane koga i po kojoj osnovi. Otuda savremene tehnologije imaju značajnu ulogu u zaštiti podataka od zloupotrebe. Pristup podacima nije neograničen. On se sprovodi jedino uz dozvolu, odnosno pravni osnov za pristup podacima „*na osnovu izričitih ovlašćenja za vođenje određenih upravnih, sudskih ili drugih postupaka*“ (Službeni glasnik RS, br. 58/2010, IV glava, stav 2)

„*Strategija zaštite podataka o ličnosti*“ (Službeni glasnik RS, br. 58/10) indirektno predstavlja jedan vid borbe protiv kiberterorizma jer stavlja pod zakonski okvir „*prikupljanje, držanje, obradu i korišćenje podataka o ličnosti*“ kojim se zabranjuje diskriminacija u oblasti podataka o ličnosti i štite podaci svakog lica bez obzira na: pol, rasu, jezik, državljanstvo, nacionalnu pripadnost, veroispovest, političko uverenje, socijalni status i ostala lična svojstva.

Međutim, kako raniji „*Zakon o zaštiti podataka o ličnosti*“ (Službeni glasnik RS, br. 97/08, 104/09 - dr. zakon, 68/12 - US i 107/12) iz 2008. godine nije sadržao odgovarajuće „*propise kojima se uređuje pitanje obrade podataka o ličnosti koje je veoma zastupljeno u tim oblastima, kao što su npr. marketing, video nadzor, upotreba biometrijskih podataka i dr.*“, i obzirom da pravni okvir kojim se uređuje oblast zaštite podataka o ličnosti koji datira iz 2008. godine nije bio usklađen sa mnogim zakonima, podzakonskim aktima i propisima, Narodna skupština je usvojila novi „*Zakon o zaštiti podataka o ličnosti*“ (Službeni glasnik RS, br. 87/18) koji je stupio na snagu 21. novembra 2018. godine. Predviđeno je do 2020. godine njegovo usklađivanje sa ostalim zakonima i propisima u Republici Srbiji.

Novim „*Zakonom o zaštiti podataka o ličnosti*“ (Službeni glasnik RS, br. 87/18) iz 2018. su obuhvaćeni i posebni slučajevi obrade podataka o ličnosti, Član 88-94:

„*1) obrada i slobode izražavanja i informisanja;*

2) obrada i slobodan pristup informacija od javnog značaja;

3) obrada jedinstvenog matičnog broja građana;

4) obrada u oblasti rada i zapošljavanja;

5) u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja, ili u statističke svrhe;

6) obrada od strane crkve i verskih zajednica;

7) obrada podataka o ličnosti u humanitarne svrhe od strane organa vlasti” (Službeni glasnik RS, br. 87/18)

Za nepoštovanje prava u ovoj oblasti predviđene su kaznene mere. Sertifikovano stručno telo za praćenje i nadzor je Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, koji je prema članu 4, stav br. 22: „*nezavisan i samostalni organ vlasti ustanovljen na osnovu zakona, koji je nadležan za nadzor nad sprovođenjem ovog zakona i obavljanje drugih poslova propisanih zakonom*“ (Službeni glasnik RS, br. 87/18).

7.1.13. Strategija razvoja elektronske uprave u Republici Srbiji za period 2015–2018. godine i Akcioni plan za sprovođenje Strategije za period 2015–2016. godine

„*Strategija razvoja elektronske uprave*“ (Službeni glasnik RS, br. 107/15) se odnosi na razvoj informacionog društva u različitim oblastima: „*javne uprave, zdravstva, obrazovanja, pravosuđa, socijalne politike, javnih nabavki, participacija u odlučivanju, sigurnosti podataka i elektronskih transakcija, dostupnosti i pristupačnosti, bezbednosti podataka o ličnosti, kao i na razvoj i upotrebu otvorenih podataka koje poseduju organi javne vlasti, a koji su nastali u radu ili u vezi sa njihovim radom*“ (Službeni glasnik RS, br. 107/15).

Strategijom se podstiče razvoj elektronske uprave uz poštovanje četiri uslova: a) finansijski, podrazumeva da razvoj teče u skladu sa finansijskim performansama (prihodi, rashodi, iskoristivost zaliha, profitabilnost i dr.), b) korisnički, sagledavanje kvaliteta pružanja usluga i proizvoda, odnos cene i kvaliteta, raspoloživost i druga merila koja su značajna korisnicima; c) sagledavanje različitih procedura koje su u sklopu internih operativnih procesa, u smislu njihove efektivnosti i efikasnosti kod pružanja usluga korisnicima, i d) učenje i rast, jer se razvoj postiže jedino dugoročnim usavršavanjem i ulaganjem u znanje i veštine zaposlenih u državnoj upravi uz redovne evaluacije njihovog znanja i veština i praćenje trendova razvoja u okruženju i šire.

Osnovni cilj je ostvarenje brzog i kvalitetnog razvoja kroz unapređenje sistema državne uprave uspostavljanjem:

1. „*institucionalnog i zaokruživanje pravnog okvira za obezbeđenje koordinisanog upravljanja razvojem e-uprave*;
2. *interoperabilnosti između informacionih sistema organa državne uprave, autonomne pokrajine i jedinica lokalne samouprave*;
3. *osnovnih elektronskih registara povezanih sa drugim informacionim sistemima državnih organa, organa autonomne pokrajine i jedinica lokalne samouprave*;
4. *uspostavljanje novih elektronskih usluga na nacionalnom portal e-upava i drugim portalima;*
5. *usavršavanje zaposlenih u državnoj upravi za korišćenje IKT;*
6. *uspostavljanje otvorene uprave*” (Službeni glasnik RS, br. 107/15).

7.1.14. Normativno uređenje upotrebe informaciono-komunikacionih tehnologija kada su korisnici maloletna lica

Maloletna deca i mladi predstavljaju značajan deo populacije koji je aktivno uključen u informaciono-komunikacione tehnologije. Oni su korisnici različitih usluga koje internet nudi: video igre, *chat rooms*, *youtube* kanali, usluge različitih pretraživača, *e-mail* komunikacije i druge slične usluge. Maloletna deca su iz najrazličitijih razloga (neznanja, nezrelosti i dr.) lake žrtve za manipulaciju. Opšte je poznato da su neretko učinioci terorističkih dela i maloletna lica. Otuda je neophodno staviti pod zakonski okvir aktivnosti maloletnika na internetu u virtuelnom kiberprostoru, ali je nužno i sankcionisati dela učinjena nad maloletnim licima uz upotrebu savremenih informaciono-komunikacionih tehnologija.

Prema „*Zakonu o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica*“ (Službeni glasnik RS, br. 85/05) propisano je „*isključivanje krivičnih sankcija prema deci*“ i u zavisnosti od učinjenog krivičnog dela predlaže se primena vaspitnog naloga.

U okviru posebnog poglavlja koje je posvećeno zaštiti dece i maloletnika „*Zakon o oglašavanju*” (Službeni glasnik RS, br. 6/16, 52/19 – dr. zakon) propisuje posebna pravila za:

- „*zaštitu dece i maloletnika od neprikladnog oglašavanja*” (član 21)
- regulisanje „*oglasne poruke namenjene deci i maloletnicima*” (član 22)
- „*zloupotrebe neiskustva, neznanja i lakovernosti*” (član 23)
- „*zaštita zdravlja i razvoja*” (član 24)
- „*zaštita integriteta*” (član 25)
- „*oglašavanje u obrazovnim i vaspitnim ustanovama*” (član 25).

Ovakva zakonska regulativa sankcioniše i otežava puštanje poruka koje se ciljano odnose na populaciju maloletnih lica u javnost bilo putem elektronskih medija ili drugog načina oglašavanja kako od strane terorista, tako i od strane bilo kog lica koje ne poštuje pravila koja su „*Zakonom o oglašavanju*” (Službeni glasnik RS, br. 6/16, 52/19 – dr. zakon) propisana.

Tokom korišćenja različitih internet usluga neretko ostavljamo veliki broj ličnih podataka. Maloletna lica najčešće to čine kada žele da postanu članovi različitih *chat* foruma i drugih socijalnih mreža u kiberprostoru. Zato je u okviru „*Zakona o zaštiti podataka o ličnosti*” (Službeni glasnik RS, br. 87/18) uređena oblast obrade podataka o ličnosti za maloletna lica, gde je prema članu 16. regulisan „*pristanak maloletnog lica u vezi sa korišćenjem usluga*

informacionog društva" tako da „*maloletno lice koje je navršilo 15 godina može samostalno da daje pristanak za obradu podataka o svojoj ličnosti*", a ukoliko „*nije navršilo 15 godina, pristanak mora dati roditelj koji vrši roditeljsko pravo, odnosno drugi zakonski zastupnik maloletnog lica*" (Službeni glasnik RS, br. 87/18). Na taj način se maloletna lica štite od zloupotrebe podataka prilikom korišćenja IT komunikacija.

Na koji način se maloletna lica štite od vršilaca krivičnih dela nad njima koja se izvode primenom informaciono-komunikacionih tehnologija? „*Krivičnim zakonikom*" (Službeni glasnik RS, br. 85/05, 88/05- ispravka, 107/05 – ispravka, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19) su sankcionisana krivična dela koja su izvršena nad maloletnim licima uz primenu savremenih informaciono-komunikacionih tehnologija kojima se krše polne slobode i vrši pribavljanje za sebe ili druge, posedovanje, prikazivanje ili javno izlaganje materijala pornografske sadržine. Prema članu 185. (Službeni glasnik RS, br. 85/05, 88/05- ispravka, 107/05 – ispravka, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19) zabranjuje se i zakonski sancioniše novčanom kaznom ili zatvorom iskorišćavanje maloletnog lica uz upotrebu sredstava informaciono-komunikacionih tehnologija:

- „*za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu*" (član 185a)
- ukoliko se „*dogovori sa maloletnikom sastanak i pojavi se na dogovorenom mestu radi sastanka*" (član 185b)
- „*pristupi slikama, audio-vizuelnim ili drugim predmetima pornografske sadržine nastalim iskorišćavanjem maloletnog lica*" (član 185, tačka 5) i dr.

Obzirom na savremenu tehnološku revoluciju i sve veću uključenost informaciono-komunikacionih tehnologija u obrazovni sistem i svakodnevni stil života mladih i maloletnika, potrebno je gotovo sve zakonske regulative kojima se posredno ili neposredno reguliše oblast informacionih-tehnologija i njene bezbednosti prilagoditi maloletnim licima i mladima.

7.2. Operativno -organizacioni aspekti borbe protiv kiberterorizma u Srbiji

7.2.1. Uloga policije i bezbednosnih službi

Policija, kao ovlašćeni državni organ za borbu protiv kriminala ide u susret savremenim oblicima kriminalnih aktivnosti, te ima pred sobom zadatak suočavanje sa izazovima i pretnjama visokotehnološkog kriminala. Prema „*Zakonu o policiji*“ (Službeni glasnik RS, br. 6/16, 24/18, 87/18), članu 11, tačka 5, Ministarstvo unutrašnjih poslova Srbije pored ostalih poslova nadležno je da: „*obavlja poslove zaštite i spasavanja ljudi, materijalnih i kulturnih dobara i životne sredine od elementarnih nepogoda, tehničko-tehnoloških nesreća, udesa i katastrofa, posledica terorizma, ratnih i drugih većih nesreća*“ (Službeni glasnik RS, br. 6/16, 24/18, 87/18).

Efikasna borba protiv kiberterorizma na nacionalnom nivou zahteva dobru kooperativnost svih organa unutrašnjih poslova i po vertikalnoj i po horizontalnoj osnovi, ali i dobru policijsku saradnju na regionalnom i međunarodnom nivou. Pored toga neophodni su i stručna obučenost kadrova, mobilnost službe, finansijsko planiranje i ulaganje u tehničke i ljudske kapacitete. Kiberterorizam kao kriminalni akt može da prouzrukuje veoma teške posledice i po svojoj nehumanosti prevazilazi brojne druge kriminalne akte. Tim pre je potreba policije za još čvršćom borbom protiv kibeterorizma veća, zarad očuvanja reda i stabilnosti, života i imovine nedužnih građana od pretnji kiberterorizma.

Policija i bezbednosne službe za postupanje u situacijama opasnosti od pretnji krivičnih dela terorizma i drugih sličnih dela nasilja, angažuju posebno organizovane policijske jedinice za intervenciju u vanrednim situacijama, koje čine posebno obučena lica za vršenje određenih policijskih zadataka. Ministarstvo unutrašnjih poslova Srbije poseduje Specijalnu antiterorističku jedinicu (SAJ).

Policijski organi tokom kriminalističke obrade u cilju otkrivanja i razjašnjenja krivičnog dela i njegovih učinilaca sprovode razne kriminalisatičko – taktičke radnje i procedure za prikupljanje dokaza. Operativni rad podrazumeva primenu adekvatnih kriminalističkih metoda s ciljem suprostavljanja kriminalitetu, kako preventino tako i represivno. Dok, izbor i primena metoda zavise od sadržaja učinjenog krivičnog dela, u ovom slučaju dela kiberterorizma. Operativni rad ima svoj pravni osnov i odvija se uz poštovanje zakonskih i odgovarajućih podzakonskih propisa.

Šta podrazumeva operativni rad, odnosno operativna delatnost? „*Operativna delatnost počinje samoinicijativnom delatnošću organa unutrašnjih poslova kada: postoje osnovi sumnje da je učinjeno krivično delo za koje se goni po službenoj dužnosti, a nema vidljive posledice (krijumčarenje, prikrivanje) i kada je posledica kriminalne delatnosti manifestovana javno (ubistva, krađa). Operativna delatnost može ići: od potencijalnog ili poznatog učinilaca i od krivičnog dela ka nepoznatom učiniocu (po NN)*“ (Vodinelić, 1984, 53). Postoji više oblika i faza realizacije operativne delatnosti u zavisnosti od svoje sadržine, vremena preduzimanja načina realizacije i rezultata.

Dva ključna problema kiberodbrane su tehničke i političke prirode. Policija sporovodi istražne radnje jedino kada su za to ispunjeni zakonski uslovi, odnosno pravni osnov. Kada se radi o najtežim krivičnim delima protiv Ustavnog uređenja i bezbednosti zemlje sa elementom inostranosti i visokim stepenom društvene opasnosti, policija koristi posebne operativne metode i sredstva na osnovu posebnog propisa Ministarstva unutrašnjih poslova Republike Srbije koji je predviđen za takve situacije. Služba državne bezbednosti (BIA) ima značajnu ulogu u očuvanju Ustavom utvrđenog poretka. BIA kao i policija primenjuje istovetna ili slična sredstva, metode i radnje za pribavljanje, procenu i proveravanje informacija o antiustavnoj delatnosti, jedina razlika je u delokrugu rada. Jer se bavi delima koja se u osnovi tiču političkog kriminaliteta i koja uglavnom imaju zajedničkih tačaka sa krivičnim delima opšteg kriminaliteta, ali ih razlikuju motivi izvršenja. Svrha operativne delatnosti je blagovremeno otkrivanje namera i ciljeva koji teže da ugroze ustavno uređenje i bezbednost zemlje i druge vitalne državne interese. Dakle operativna delatnost se sprovodi pre izvršenja krivičnog dela, ali i nakon što je ono izvršeno kada se sprovodi istražni postupak i prikupljanje materijalnih dokaza u skladu sa kriminalističkim pravilima i procesnim odredbama da bi oni bili upotrebivi na sudu. Međutim, „*informacije koje prikuplja obaveštajno bezbednosna služba primenom operativno tehničkih sredstava i metoda ne predstavljaju bilo kakav dokaz, ali mogu predstavljati osnovu za primenu osnovnih metoda kriminalističke metodike kojima se obezbeđuju valjani dokazi u odnosu na konkretno krivično delo i učinioca*“ (Matijević, 2002, 37). Obzirom da je kiberterorizam specifično kriminalno delo potrebno je prikupiti što više dokaza i informacija o učinjenom delu i njegovom počiniocu. Jer, internet saobraćaj je teško pratiti zbog velikog protoka informacija. Elektronski nadzor telekomunikacija podrazumeva elektronsko prisluškivanje telefonskih razgovora i praćenje drugih načina komunikacije, što se kosi sa poštovanjem politike privatnosti.

Elektronski nadzor komunikacija se sprovodi prevashodno zbog prikupljanja relevantnih dokaza u sudskom postupku, za otkrivanje mreže članova terorističke organizacije, utvrđivanje hijerarhije i celokupnog kriminalnog delovanja. Ovu metodu mogu da primenjuju jedino zakonski ovlašćene osobe, uz poštovanje određenih načela. Sprovođenju ovih mera pristupa se u slučajevima kada se istragom nije moglo doći do adekvatnih dokaza, ili kada primena prethodnih mera nije dala rezultat, pa se prema tačno navedenom zahtevu koji sadrži „*činjenice, navedene okolnosti pod kojima su iskorišćene sve metode koje nisu davale adekvatan rezultat, kao i razloge zbog kojih se smatra da bi primena metoda tajnog prisluškivanja dala rezultate. Zahtev za prisluškivanje treba da sadrži i vremenski rok u kojem će se sprovoditi nadzor komunikacije koji može trajati do trideset dana, koji se sprovodi na osnovu naredbe nadležnog sudije. Mera nadzora može se produžavati na još trideset dana u nekoliko navrata, takođe uz saglasnost nadležnog sudije*“ (Weaver, Abramson & Bacigal, 2007, 564). Ukoliko okolnosti koje proističu iz terorističke aktivnosti to osobito nalažu, može se primeniti i tajni nadzor lica čiji identitet nije u potpunosti utvrđen, a koja su povezana sa najtežim zločinima, kao i metod prikrivenog islednika. Ovaj metod se ređe primenjuje zbog nedovoljno jasne pravne regulative i teškoća koje proizilaze iz same realizacije planiranih poslova prikrivenog islednika. Većina članova terorističke organizacije je nepoverljiva prema novopridošlicama, što dodatno otežava prodor do vrha terorističke organizacije.

Timski i sinhronizovani rad i saradnja uz primenu adekvatnih naučnih metoda i dostignuća kako prirodnih i tehničkih nauka, tako i društvenih (politikologije, sociologije i psihologije) su neophodni u rasvetljavanju i dokazivanju kiberterorizma.

7.2.2. Mere odbrane i postupanje sa pretnjom od kiberterorizma u Srbiji

Država je bitan subjekt u suprostavljanju zloupotrebe kiberprostora. Strategijski pristup u suprostavljanju kiberterorizmu omogućava adekvatnu prevenciju i represiju, uz primenu tehnoloških, pravnih, političkih, ekonomskih, socijalnih i drugih mera koje deluju učinkovito na borbu protiv kiberterorizma.

Efikasno suprostavljanje pretnjama kiberterorizma podrazumeva nekoliko faza. Najpre je potrebno da država sa svim nadležnim organima i subjektima otkloni uslove koji pogoduju nastajanju, razvoju i sprovođenju dela kibeterorizma. Sledeća faza se odnosi na operativnu delatnost, identifikaciju pretnji i preduzimanje tehničkih i kriminalističkih radnji i mera sa ciljem otkrivanja i razjašnjavanja konkretnog krivičnog dela. Ova faza podrazumeva otkrivanje učinilaca i obezbeđivanje dokaza za dalje postupanje. Računarsko pretraživanje podataka je uvedeno 2006. godine u naše procesno zakonodavstvo izmenama i dopunama „*Zakonika o krivičnom postupku*“ (Službeni glasnik RS, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14 i 35/19) kojim su propisani uslovi i način sprovođenja računarskog pretraživanja podataka. Koji podaci mogu poslužiti kao elektronski dokaz? „*Elektronski dokaz je bilo koja informacija generisana, obrađena, uskladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao merodavnu, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokaznu vrednost i na koje se sud može osloniti u kontekstu forenzičke akvizicije, analize i prezentacije*“ prema članu 112. st. 17. i st. 26. „*Krivičnog zakonika Republike Srbije*“ (Službeni glasnik RS, br. 2005/88 ,2005/85 - ispr., 2005/107 - ispr., 2014/108 ,2013/104 ,2012/121 ,2009/111 ,2009/72 i 2016/94). Ovi dokazi se najčešće pribavljaju pomoću uređaja kao što su: računarski sistemi, sistemi video nadzora, tablet-uređaji, digitalni aparati, uređaji za skladištenje podataka (hard-diskovi i SDD diskovi, USB uređaji, memorijske kartice, optički kompakt diskovi i dr.) i drugi, ali i pomoću obaveštajnih službi. Na koji način obaveštajne službe dolaze do podataka? „*Obaveštajne službe dolaze do podataka preko niza specifičnih metoda i postupaka čija je zajednička karakteristika elemenat tajnosti u svim fazama i postupcima obaveštajnog rada. U svojim aktivnostima primenjuje skup metoda, radnji i postupaka na osnovu kojih obaveštajna služba ostvaruje svoju funkciju, mežu kojima su:*

- metod tajnog priklupljanja podataka o teroristima

- *metod prikrivenog prikupljanja podataka*

- *metod legalnog prikupljanja podataka*

- *metod obaveštajne dselatnosti*

-*metod ne obaveštajne delatnosti obaveštajnih službi*“ (Savić u: Pejanović & Bejatović, 2009, 279-270).

Poslednja, završna faza podrazumeva progon učinilaca i presudu što je u nadležnosti tužilaštva i suda. Važni preduslovi za efikasno suprostavljanje kiberterorizmu su stalno praćenje razvoja nauke i tehnologije, primena savremenih izuma i njihovo prilagođavanje postojećim raspoloživim kriminalističkim metodama.

Javna tužilaštva kao organi gonjenja i sudovi kao organi pravosuđa imaju značajnu ulogu u otkrivanju i razjašnjenju ispoljenih oblika kiberterorizma. Tabela 12. Prikazuje pojedinačni i zbirni statistički prikaz primljenih krivičnih prijava i izveštaja u Posebnom tužilaštvu za visokotehnološki kriminal u periodu od 2006. do 2016. godine. Uloga javnog tužilaca u fazi kriminalističke obrade je naročito važna. Posebno odeljenje za borbu protiv visokotehnološkog kriminala formirano je 2006. godine pri Višem javnom tužilaštvu u Beogradu prema članu 5. „*Zakona o organizaciji i nadležnosti drzavnih organa za borbu protiv visokotehnoloskog kriminala*“ (Službeni glasnik RS, br. 61/05 i 104/09).

Tabela 12. Pojedinačni i zbirni statistički prikaz primljenih krivičnih prijava i izveštaja u Posebnom tužilaštvu za visokotehnološki kriminal u periodu od 2006. do 2016. godine (Stamenković, Živanović, Paunović & Stevanović, 2017, 12)

Godina	Upisnik KT	Upisnik KTR	Upisnik KTN	Ukupno
2006	19	/	/	19
2007	75	68	11	154
2008	110	60	14	184
2009	91	114	42	247
2010	116	443	13	572
2011	130	502	28	660
2012	114	609	65	788
2013	160	558	243	961
2014	294	770	352	1416
2015	198	1306	570	2074
2016	240	1237	580	2058
Ukupno	1547	5667	1918	9132

Veoma je teško voditi borbu protiv kiberterorizma, jer nadležni subjekti moraju da otkriju i razjasne teško dokazive veze između učinjenog kibernapada i napadača. To potvrđuje tamna brojka i veliki broj neosuđenih izvršitelja kibernapada. Kako primećuje Gudmen „*žrtve mogu ozbiljno da sumnjaju u sposobnost policije da se bavi incidentima kompjuterskog kriminala efikasno, pravovremeno i na pouzdan način*“ (Goodman, 2001, 13). Jer, za sprovođenje zakona u oblasti kiberbezbednosti često nedostaje odgovarajuće znanje da bi se držao korak sa kiberteroristima (Gabrys, 2002).

Pisarić navodi izazove sa kojim se suočava policija u Srbiji povodom otkrivanja dela visokotehnološkog kriminala:

- „*neusklađenost pravne regulative sa savremenim oblicima izvršenja krivičnih dela;*

- *nedovoljna tehnička opremljenost i osposobljenost policijskih službenika vezana za otkrivanje izvršilaca u online okruženju;*

- *nedostatak operacionalnih obuka koje bi omogućile da policijski službenici koji se bave sprečavanjem visokotehnološkog kriminala budu dovoljno obučeni i tehnički opremljeni za vršenje ovih zadataka;*

- *poteškoće u otkrivanju izvršilaca krivičnih dela koji koriste lažne identitete u online okruženju, posebno kada se u obzir uzme činjenica da je u velikom broju slučajeva međunarodna policijska saradnja loša, a da u nekima čak i ne postoji;*

- *poteškoće u otkrivanju tačne lokacije izvršenja krivičnog dela, pošto se ova krivična dela vrše sa mnogih mesta širom sveta, a u velikom broju slučajeva izvršioci krivičnih dela koriste mreže sa javnim pristupom*“ (Pisarić, 2016, 54).

Zbog toga je važno adekvatno angažovanje svih nadležnih subjekata, počev od IT administratora, korisnika mreže pa do nadležnih subjekata u suprostavljanju kiberterorizma još u fazi postojanja indicija, odnosno kada se javljaju prva upozorenja i smetnje na mreži. Saradnja sa drugim državama na suzbijanju kiberterorizma je veoma značajna, naročito zbog pronalaženja i izručenja terorista u skladu sa pravilima međunarodne krivičnopravne pomoći uz angažovanje Interpola – međunarodne organizacije kriminalističke policije „*uz uslov da se to odnosi samo na one terorističke akte koji imaju međunarodne imlikacije tj. da angažovanje interpola podrazumeva borbu samo protiv terorizma koji ima elemente inostranosti*“ (Bošković & Jovičić, 2002, 59). Dakle, Interpol je takođe angažovan na sprečavanju i suzbijanju svih oblika

kiberterorizma. U septembru 2014. godine, u Singapuru je osnovan *IGCI* (*INTERPOL Global Complex for Innovation*), posebna organizaciona jedinica Interpola čiji je osnovni cilj borba protiv kompjuterskog kriminala, inovacije i razvoj u oblasti suprostavljanja računarskom kriminalitetu. Timovi vodećih IT stručnjaka iz celog sveta danonoćno su angažovani na prevenciji računarskog kriminaliteta, sarađuju sa nacionalnim policijskim službama, pružaju im pomoć u veštačenju i istragama, obaveštavaju ih o mogućim kriminalnim pretnjama.

Ministarstvo unutrašnjih poslova Republike Srbije sarađuje sa Evropolom. Između Republike Srbije i Evropske policijske organizacije potpisan je 18. septembra 2008. godine sporazum, koji je regulisan „*Zakonom o potvrđivanju Sporazuma o operativnoj i strateškoj saradnji između Republike Srbije i Evropske policijske kancelarije*“ (Službeni glasnik RS – Međunarodni ugovori, br. 5/14). Osnovna svrha Sporazuma prema članu 1. je unapređenje saradnje „*u sprečavanju i borbi protiv organizovanog kriminala, terorizma i drugih oblika međunarodnog kriminala u oblastima kriminala*“ (Službeni glasnik RS – Međunarodni ugovori, br. 5/14). Europol posebnu pažnju posvećuje borbi protiv kiberkriminala i od 2013. godine formiran je posebno specijalizovan centar *European Cybercrime Centre (EC3).*

Duži vremenski period su računari i računski programi u upotrebi u našoj zemlji. Računarski, odnosno visokotehnološki kriminalitet, nije novina na prostorima Republike Srbije. Prema podacima Posebnog odeljenja za visokotehnološki kriminal Višeg javnog tužilaštva u Beogradu u periodu 2006 do 2013. godine krivična dela ove vrste svake godine beleže rast (Stamenković, Živanović, Paunović & Stevanović, 2017, 12). Aktuelna bezbednosna situacija zahteva posvećenost i punu pažnju kao nikada ranije jer se incidenti i rizici povezani sa kibernapadima povećavaju (Choo, 2011).

ZAKLJUČNA RAZMATRANJA

Razvoj i primena informatičke tehnologije značajno su izmenili svakodnevni život. Tehnološki napredak je multiplikator društvenog razvoja, ali podrazumeva i određene rizike. Jer, dostupnost visokotehnološkim izumima po komercijalnim cenama na slobodnom tržištu, omogućava teroristima da koriste prednosti savremene tehnologije u različite svrhe. U visoko razvijenim zemljama tehnologija ima široku upotrebu, u tolikoj meri da je funkcionisanje krucijalnih infrastruktura značajno zavisno od tehnologije, što ih čini ranjivim na nove vrste pretnji iz kiberprostora. Otuda je bezbednost informaciono-komunikacionih tehnologija jedno od najznačajnijih pitanja današnjice.

Tema disertacije je obrađena u nekoliko poglavlja. U prvom poglavlju razrađeni su osnovni predmet i cilj istraživanja, njegovo teorijsko i operaciono određenje, osnovne hipoteze i metodološke postavke. Drugo poglavlje posvećeno je određenju pojma kiberterorizam, njegovim osnovnim karakteristikama, pojavnim oblicima, glavnim učesnicima, metama i posledicama. Obzirom da se kiberterorizam odvija u specifičnom *virtuelnom* okruženju, čije su posledice vidljive u realnom svetu, radi boljeg razumevanja ove pojave u okviru prvog poglavlja takođe je obrađen i pojam kiberprostor. Treće poglavlje razrađuje savremen društveno-politički kontekst, koncept globalizacije i njene posledice na makro i mikro nivo-u društvene stvarnosti. Globalizacija zbog svoje kontradiktornosti, porasta bogastva i standarda sa jedne strane uz istovremeni porast socijalne tenzije i siromaštva sa druge strane predstavlja neiscrpan izvor za regrutovanje novih članova terorističkih i drugih kriminalnih organizacija. Sve veći broj organizovanih kriminalnih grupa koristi terorističke taktike. Globalizacija je omogućila da povezanost između organizovanog kriminala i terorizma dobije globalnu dimenziju, što doprinosi ne samo njihovom tešnjem zbližavanju, nego i metamorfozi. Što, uz sponzorisanje terorizma od strane pojedinih država dodatno komplikuje situaciju na makro nivou društvene stvarnosti. Tehnološka revolucija iznedrila je nove vrste društvenih formi virtuelne zajednice i kiberkulturu, što uz alijenaciju koja je podstaknuta sve češćom komunikacijom putem savremenih informacionih-tehnologija i krizu identiteta uzrokovanu brojnim mogućnostima za formiranje identiteta koje se u kiberprostoru nude, na mikro nivo-u čini postojeću situaciju pogodnom za razvoj kiberterorističkih aspiracija i drugih zloupotreba na internetu.

U četvrtom poglavlju razmatrani su pojmovi: kiberkriminal, pogodnosti i zloupotrebe interneta, distinkcija i veza između kiberkriminala i kiberterorizma. Peto poglavlje posvećeno je borbi protiv kiberterorizma kroz tri faze: prevencija, suočavanje sa kibernapadom i saniranje posledica, aktivne i pasivne mere odbrane i nove strategije odbrane koje se primenjuju. Šesto poglavlje rada posvećeno je merama i postupcima za suzbijanje kiberterorizma na regionalnom i globalnom planu, pravno-organizacionim i operativno-organizacionim aspektima borbe protiv kiberterorizma. U sedmom poglavlju su prikazane mere i postupci za suzbijanje kiberterorizma koji se primenjuju u Republici Srbiji kroz normativni aspekt - zakoni, različite strategije, donešene odluke i akcioni planovi i operativno-organizacioni aspekt borbe protiv kiberterorizma- uloga policije i bezbednosnih službi, kaznene mere, mere odbrane i postupanje sa pretnjom od kiberterorizma u Srbiji.

Srbija je ratifikovala brojne konvencije i usvojila je mnoga druga međunarodna dokumenta koja se bave borbom protiv kiberterorizma, ali i terorizma uopšte. Terorizam je aktuelna tema u mnogim političkim i naučnim raspravama. Međunarodna zajednica ulaže velike napore da iznađe rešenje za probleme terorizma i sve njegove pojavne oblike. To potvrđuje veliki broj sastanaka i konferencija na pomenutu temu, rezolucija i usvojenih dokumenata koji su oblikovali bezbednosne politike na međunarodnom, regionalnom i nacionalnom nivou. Vlada Republike Srbije je prepoznala pretnje koje proizilaze iz kiberprostora i normativno-pravno ih regulisala. Dakle, Srbija je nesumnjivo pokazala svoju posvećnost u suprostavljanju kiberterorizmu i kiberkriminalu, međutim efikasno suprostavljanje kiberterorizmu zahteva:

- kontinuirano praćenje njegovog razvoja
- identifikaciju svih njegovih pojavnih oblika
- izbor adekvatnih preventivnih i represivnih metoda
- organizovan timski i stručan rad
- razmenu iskustva, informacija i najboljih praksi na međunarodnom, regionalnom nivou
- međusobnu saradnju državnih organa (policijskih, pravosudnih i drugih) koji su zaduženi za otkrivanje, nadzor i kontrolu na nacionalnom nivou
- uključivanje privatnog sektora u suprostavljanje kiberterorizmu
- saradnja državnog (javnog sektora) sa organizacijama koje posluju i rade u IT industriji (privatni sektor)
- bolja informisanost i edukacija građana o postojećim pretnjama

- sistematičnost, planiranje i ulaganja
- primena naučnih i praktičnih metoda, adekvatno korišćenje tehnoloških dostignuća
- multidisciplinarnost

LITERATURA

Naučni i stručni tekstovi, monografije i zbornici radova

1. Abadinsky, H. (1994). *Organized Crime*, Chicago: Nelson- Hall Publishers.

2. Abrahamson, P. (1995). Social Exclusion in Europe: Old Wine in New Bottles? *Družboslovne razprave* 11(19–20), 119–136.

3. Abrams, M., Podell H., Jajodia S. (1995). *Information Security: An Integrated Collection of Essays*, Los Alamitos, CA USA: Computer Society Press, 117.

4. Akhgar, B., Staniforth A. & Bosco F. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*, USA: Elsevier Inc.

5. Albrow, M. (1996). *The Global Age: State and Society Beyond Modernity*. Cambridge: Polity Press.

6. Alqahtani, S. H. (2016). Latest Trends and Future Directions of Cyber Security Information Systems. *Journal of Information Engineering and Applications* 6 (11), 9-14.

7. Appadurai, A. (2000). Grassroots Globalization and the Research Imagination. *Public Culture* 12 (1), 1-19 .

8. Appadurai, A. (2000). *Modernity at Large*. Minneapolis: University of Minnesota Press.

9. Arnett, J.J.(2002). The psychology of globalization. *American Psychologist*, Vol. 57, 774-783.

10. Ashley, K. B. (2003). *Anatomy of cyber terrorism: Is America vulnerable?* USA: Air University, Maxwell AFB, AL.

11. Auwema, N.M. (2015). *The Discourse of Cyberterrorism:Exceptional measures call for the framing of exceptional times*, Thesis MSc Political Science.

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

13. Baruch, Y. (2000). Teleworking: Bene ts and Pitfalls as Perceived by Professionals and Managers. *New Technology, Work and Employment*, Vol. 15, 34–49.

14. Basan, M., Kofman, V. & Žoa, D. (2005). Deset teza za sociološku teoriju urbane dinamike. U: Vujović, S. & Petrović M. (prir.) (2005). *Urbana sociologija* (229-238). Beograd: Zavod za udžbenike i nastavna sredstva.

15. Bauman, Z. (1998). *Globalization: the human consequences*. New York, Columbia University Press.

16. Bauman, Z.(2003). Turisti i vagabundi. U: Vuletić, V. (prir.) (2003). *Globalizacija – mit ili stvarnost* (251-273). Beograd: Zavod za udžbenike i nastavna sredstva.

17. Beaulac, S. (2004). The Westphalian model in defining international law: challenging the myth. *Australian Journal of Legal History* Vol. 7, 181–213.

18. Beck, U.(2002). The cosmopolitan society and its enemies. *Theory, Culture & Society*, Vol.19, 17-44.

19. Beggs, C & Butler, M. (2004). *Developing New Strategies to Combat Cyber-Terrorism*, Idea Group Publishing.

20. Bek, U. (2001). *Rizično društvo: u susret novoj modreni*. Beograd: Filip Višnjić.

21. Belenky, A. & Ansari, N. (2003). IP Traceback with Deterministic Packet Marking. *IEEE Communications Letters,* Vol. 7, No. 4.

22. Bender, G. (1998). Bavaria v. Felix Somm: the pornography conviction of the former CompuServe manager. *International Journal of Communications, Law and Policy* 1, 1-4.

23. Beriša, H. & Barišić, (2016). Bezbednosni izazovi - Kibernetski prostor i informaciono ratovanje, *Zloupotreba informacionih tehnologija i zaštita*, Beograd: IT veštak.

24. Bianchi, A. (2011). Terrorism and Armed Conflict: Insights from a Law & Literature Perspective. *Leiden Journal of International Law* 24 (1), 1–21.

25. Bishop, M. (1995). *A taxonomy of UNIX system and network vulnerabilities*. Technical report CSE 95/10. University of California at Davis: Department of Computer Science.

26. Blau, P. (1964). *Exchange and Power in Social Life*. New York: John Wiley & Sons.

27. Bobbitt, P. (2008). *Terror and Consent: The Wars for the Twenty-First Century*. New York: Anchor Books.

28. Boebert, W. E. (2010). A Survey of Challenges in Attribution. *Proceedings of a workshop on Deterring CyberAttacks*, *Informing Strategies and Developing Options for U.S. Policy*, Washington DC: National Academy of Sciences.

29. Bollen, J., Mao H. & Zeng, X. (2011). Twitter mood predicts the stock market. *Journal of Computational Science* 2 (1), 1–8.

30. Bolton D. C. (1972). Alienation and Action: A Study of Peace-Group Members. *American Journal of Sociology*, 78 (3), 537-561.

31. Boon, S. & Sinclair, C. (2009). A world I don't inhabit: disquiet and identity in Second Life and Facebook. *Educational Media International* 46 (2), 99–110.

32. Bossler, A.M. & Holt, T.J.(2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management* 35 (1), 165-181.
33. Bošković, M. (1998). *Organizovani kriminalitet*, Beograd: Policijska akademija.
34. Bošković. M. & Jovičić, D. (2002). *Kriminalistika metodika*. VŠUP: Banja Luka.
35. Božilović, N. (2004). *Rok kultura*. Niš: Studenstski kulturni centar.
36. Brenner,S.W.(2007).At Light Speed, *The Journal of Criminal Law and Criminology*,Vol. 97, No. 2, 379-475.
37. Britz, M. T. (2013). *Computer Forensics and Cyber Crime – An Introduction*, Prentice Hal, 3th edition.
38. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime, *Policing: An International Journal of Police Strategies and Management* 2, 408-433.
39. Bryant R.& Stephens, P. (2014). Policing Digital Crime: the International and Organisational Context. In: Bryant R.& Bryant S. (eds.)(2014). *Policing Digital Crime* (111-123). Surrey: Ashgate Publishing Limited.
40. Burdije, P. (1999). *Signalna svetla: prilozi za otpor neoliberalnoj invaziji*. Beograd: Zavod za udžbenike i nastavna sredstva.
41. Carr J. (2010). *Inside Cyber Warfare*, Sebastopol: Reilly Media.
42. Carter, D., Schwartz, N.&Norris, F. (6. oktobar 2008). *Financial crises spread in Europe*, New York Times.
43. Castells, M. (2000). Informacijsko doba : ekonomija, društvo i kultura. Knj. 1, *Uspon umreženog društva*. Zagreb : Golden marketing.
44. Castells, M. (2000). Toward a Sociology of the Network Society. *Contemporary Sociology* 29 (5), 693-699.
45. Castells, M. (2002). *Moć identiteta*. Zagreb: Golden Marketing.
46. Chandan, K. S. (1935). *Le terrorisme devant la Societe des Nations*, Paris.
47. Cheng, Y. Y. (2010). *Social psychology of globalization: Joint activation of cultures and reactions to foreign cultural influence*. University of Illinois at Urbana-Champaign: PhD Dissertation.
48. Chiu, C.Y., Gries, P., Torelli, C. J. & Cheng, S. Y.Y. (2011). Toward a social psychology of globalization. *Journal of Social Issues* 67, 663–676.

49. Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security* 30 (8), 719-731.

50. Clarke R., Knake R. (2010). *Cyber War – The next treat to National Security and What to do about it*, Harper Collins Publisher.

51. Cohen, F. (1997). Information system attacks: a preliminary classification scheme. *Computer & Security* 16 (1), 29-46.

52. Collin, B. (1997).The Future of Cyberterrorism, *Crime and Justice International* 13(2),15-18.

53. Condorelli, L. & Naqvi, Y. (2004). The War Against Terrorism and Jus in Bello: Are the Geneva Conventions Out of" Date? In: Bianchi A. & Naqvi Y. (eds.) (2004) *Enforcing International Law Norms Against Terrorism* (25-37). Oxford ; Portland, Or. : Hart.

54. Correia, M. & Bowling, C. (1999). Veering toward digital disorder: computer-related crime and law enforcement preparedness. *Police Quarterly* 2 (2), 225-244.

55. Cottim, A. (2010). Cibercrime, cyberterrorism and jurisdiction: an analysisof article 22 of the COE convention of cybercrime. *European Journal of Legal Studies* 2 (3), European University Institute: San Dominico de Fiesole, Italy.

56. Cronin A.C. (2009). Behind the Curve, Globalization and International Terrorism. In: Howard, D. R., Sawyer, L.R & Bajema, E.N. (eds.), *Terrorism and Counter Terrorism, Readings and Interpretations* (30-58). Boston: Higher education.

57. Damnjanović, I. (2005). *Terorizam i internet: specijalistički rad*. Beograd: Fakultet političkih nauka.

58. Damnjanović, I. (2009). Postoji li sajberterorizam, *Politička revija* 8 (19) 1, 237-253.

59. Davis, T. J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component, *Policing: An International Journal of Police Strategies & Management* 35 (2), 272-284.

60. Davis, J. (2019). *Cyber's escape*. Sapiens Run book 2. Media Cast Productions.

61. Deardorff, A. & Stern, R. (2001). What you should know about globalization and the world trade organization? *Review of International Economics*, 403-427.

62. Deardorff, A. (2002). *What Might Globalization's Critics Belief?* Michigan: University of Michigan.

63. Della Porta D. (2012). Communication in movement: Social movements as agents of participatory democracy. In: Loader B. & Mercea D. (eds) *Social Media and Democracy: Innovations in Participatory Politics* (39–55). London: Routledge.
64. Denning, D. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy. In: Arquilla, J. & Ronfeldt, D. (eds.) (2001) *Networks and Netwars. The Future of Terror, Crime, and Militancy* (239-288). RAND Corporation.
65. Denning, D. (2014). Framework and Principles for Active Cyber Defense. *Computers & Security*, Vol. 40, 108-113.
66. Dogrul, M., Aslan A. & Celik E. (2011). *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, Turkey: Turkish Air War College Istranbul.
67. Dollar, D., Kraay, A. (2001). *Trade, Growth and Poverty*. Washington: The World Bank, Development Research Group.
68. Dreher, A., Gassebner M. & Siemers, L. H. (2010). Does Terrorism Threaten Human Rights? *The Journal of Law & Economics* 53 (1), 88.
69. Duggan, P. (2015). Harnessing cyber-technology's human potential, *Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School*, Vol. 28, Iss. 4, p. 15.
70. Dunn-Cavelty, M. (2008). *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age.* New York: Routledge, Print.
71. Đokić, Z., Živanović, S. (2005). Kompjuterski kriminal kao obilježje progresivnog kriminaliteta. U: D. Radovanović (ur.), *Kazneno zakonodavstvo - progresivna ili regresivna rješenja* (305-318), Beograd: Institut za kriminološka i sociološka istraživanja.
72. Everett, A. (2004). On cyberfeminisms and cyberwomanism: High-tech mediations of feminism's discontents. *Signs: Journal of Women in Culture and Society* 30(1), 1278–1285.
73. Farwell,J.P. & Rohozinski,R.(2012).The New Reality of Cyber War,*Survival* 54(4), 107–120.
74. Ferreira, F. (1999). *Inequality and Economic Performance*. Washington: World Bank.
75. Fidler, P. D, Pregent, R & Vandurme, A. (2013). Nato, Cyber Defense, and International Law, *ST. John's Journal of International & Law* 4 (1), 1-25.
76. Flaxner S. B. (1987). *The Random Hause Dictionary of the English language*, New York: Random House.

77. Fon Hajek, F. A.(2002). Principi liberalnog društvenog poretka. U: F. A. fon Hajek, *Studije iz filozofije, politike i ekonomije* (80-99), Beograd: Paideia.

78. Fon Hajek, F.A. (1998). *Poredak slobode*, Novi Sad: Global book.

79. Frances, S. (2004). Development and security, *Conflict, Security and Development* 4(3), 261-288.

80. Friedman, T.L (1999). *The Lexus and the Olive Tree*, US: Farrar, Straus and Giroux.

81. Fu, H. -Y., & Chiu, C. -Y. (2007). Local culture's responses to globalization: Exemplary persons and their attendant values. *Journal of Cross-Cultural Psychology*, Vol. 38, 636–653.

82. Gabrys, E. (2002). The international dimensions of cyber-crime. *Information Systems Security*, 11(4), 21-32.

83. Gaćinović, R. (1998). *Savremeni terorizam*, Beograd: Grafomark.

84. Gaćinović, R. (2011). Terorizam – Izazov nauke i politike. U: Šikman, M., Amidžić G. (ur.) *Suprostavljanje terorizmu- Međunarodni standardi i pravna regulativa*. Banja Luka: Visoka škola unutrašnjih poslova.

85. Geer, E. Daniel Jr. (2006). The Physics of Digital Law: Searching for Counterintuitive Analogies. In: Balkin, J. M., Grimmelmann J., Katz E., Kozlovski N.,Wagman S., Zarsky T., (Eds.), *Cybercrime***:** *Digital Cops in a Networked Environment* (13-36). New York University Press.

86. Gerc, K. (1998). *Tumačenje kultura*, Beograd : Čigoja štampa.

87. Giddens, A. (1985). *The nation state and violence*. Cambridge: Polity Press.

88. Giddens, A.(2005*). Odbjegli svijet: Kako globalizacija oblikuje naše živote?* Zagreb: Klub studenata sociologije Diskrepancija i Naklada Jesenski i Turk.

89. Gidens, E. (1998) *Posledice modernosti*, Beograd: Filip Višnjić.

90. Gidens, E. (2003). *Sociologija*, Beograd: Ekonomski fakultet.

91. Gilpin R. (2001). *Global Political Economy: Understanding the International Economic Order*, Princeton University Press.

92. Giri, A. K. (2006) Cosmopolitanism and beyond: Towards a multiverse of transformations. *Development and Change* 37(6), 1277-1292.

93. Goodman, M. (2001). *Making computer crime count*. FBI Law Enforcement Bulletin, 70 (8), 10-17.

94. Goodman, S. E. (2007). Cyberterrorism and Security Measures. In: National Academy of Sciences, R. Narasimha, A. Kumar, S. P. Cohen & R. Guenther (Eds.), *Science and Technology to CounterTerrorism. The Proceedingsof an Indo – U.S Workshop* (43-54), Washington DC: The National Academy Press.

95. Gorc, A. (1982). *Zbogom proletarijatu*, Beograd: Radnička štampa.

96. Gordon,S., Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology* 2 (1), 13–20.

97. Grabosky, P. (2007). *Electronic Crime*, New Jersey: Pearson Prentice Hall.

98. Gray, J. (1998). *False Dawn. The Delusions of Global Capitalism*, New York Press.

99. Greitzer F.L., Ferrymann T.A. (2013). Methods and metrics for evaluating analytic insider treat tools. In: *Proccedings of the 2013 IEE security and privacy workshops (SPW'13)*, (90-97). California, USA: IEE.

100. Hafner, K. (1998). Where Wizards Stay Up Late: The Origins of the Internet, New York: Simon & Schuster.

101. Halfond, W., Viegas, J, Orso, A. (2006). A Classification of SQL Injection Attacks and Countermeasures, *IEEE International Symposium on Secure Software Engineering*, The Institute of Electrical and Electronics Engineers.

102. Hantington, S. (2000). *Sukob civilizacija*, Podgorica: CID.

103. Hardt, M. & Negri, A. (2003), *Imperij*, Zagreb: Multimedijalni Institut i Arkzin.

104. Harmon, C.C. (2000). *Terorrism today*, London; Portland, OR: Frank Cass.

105. Hathaway, A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue W., Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review* 100 (4), 817-885.

106. Held, D. (2010). *Cosmopolitanism: Ideals and Realities*, Cambridge: Polity Press.

107. Held, D. (2003). Debate o globalizaciji. U: V. Vuletić (prir.), *Globalizacija – mit ili stvarnost* (48-60). Beograd: Zavod za udžbenike i nastavna sredstva.

108. Hengsbach, F. (1997). Ein neuer Gesellschaftsvertrag in Zeiten der Globalisierung. In: Fricke, W. (Ed.), *Jahrbuch Arbeit und Technik* (182–195), Dietz: Bonn.

109. Holm, H., Ekstedt, M &Andersson, D. (2012). Empirical analysis of system-level vulnerability metrics through actual attacks, *Transactions on Dependable and Secure Computing* 9 (6), 825–837.

110. Holton, R. J. (2009). *Cosmopolitanisms: New Thinking and New Directions*, Basingstoke, UK & New York: Palgrave Macmillan.
111. Hosseini, Hamed, H.S (2013). Occupy Cosmopolitanism: Ideological Transversalization in the Age of Global Economic Uncertainties, *Globalizations* 10 (3), 425-438.
112. Iasiello, E. (2013). *Cyber Attack: A Dull Tool to Shape Foreign Policy*, Tallinn: NATO CCD COE Publications.
113. Janczewski, L., Colarik, A. (2008). *Cyber Warfare and Cyber Terrorism*, Hersey (USA): IGI Global.
114. Jazić, A. (2010). Teroristička propaganda i uloga medija, *Međunarodni problemi*, Vol. 62, No.1, 113-135.
115. Jones, A. L, Howard- Hassmann R.E. (2005). Under Strain: Human Rights and International Law in the Post 9/11 Era, *Journal of Human Rights*, Vol. 4, 61–71.
116. Jonev, K. H. (2016). Opasnost od kiberterorizma. U: S. Petrović (ur.). *Zloupotreba informacionih tehnologija i zaštita- ZITEH16*, Beograd: IT veštak.
117. Jovašević, D. (2011). *Leksikon krivičnog prava*. Beograd: Službeni glasnik.
118. Jović, V. (2001). *Prikriverni islednik*, Beograd: Sezam
119. Kahn R. & Kellner, D. (2004). New media and internet activism: From the Battle of Seattle to blogging. *New Media and Society* 6(1), 87–94.
120. Kandias, M.,Stavrou V, Božović N., Mitrou L., Gritzalis, D. (2013). Predicting the insider threat via social media: the YouTube case, In: *Proccedings of the 12th ACM Workshop on privacy in the electronic society* (261-266), Berlin: ACM Press.
121. Katz, C. (2004). *Growing up global: economic restructuring and children's everyday lives*. Minneapolis, MN: University of Minnesota Press.
122. Kaul, I. (1994). *Human security: The need for a new security council. Roundtable on Global Change. Change: Social Conflict or Harmony?* United Nations Development Programme (UNDP), Stockholm, Sweden. Participant Paper no. 32 (22–24 July).
123. Kegley, C.W. Jr. (2003). *The New Global Terrorism: Characteristics, Cause, Control*, New Jersey: Prentice Hall.
124. Keith, J, Bejtlich, R. & Rose, C. (2008). *Real Digital Forensics*, New Jersey: AddisonWesley.

125. Khamis, S. (2015). Gendering the Arab Spring: Arab women journalists/activists, cyber-feminism and the socio-political revolution. In: Carter C, Steiner L and McLaughlin L (Eds.) *The Routledge Companion to Media and Gender* (565–575), London: Routledge.
126. Kizza J. (2009). *Guide to Computer Network Security*, London: Springer.
127. Komlen Nikolić L, Gvozdenović R., Radulović, S., Milosavljević, A., Jerković, R, Živković, V. Živanović, S, Reljanović, M, Aleksić, I. (2010). *Suzbijanje visokotehnološkog kriminala*, Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
128. Kovačević, M., Pavlović, K. & Šutić, V. (2016). *Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji*, Beograd: Republički zavod za statistiku Srbije.
129. Kovačević, S. (1992). *Terorizam i Jugoslavija*, Beograd: Arkade print.
130. Kuljanski R. S. (2010). RSA algoritam i njegova praktična primena. *Vojnotehnički glasnik: stručni i naučni časopis Jugoslovenske narodne armije* 58 (3), 65-77.
131. Lechner, J. F. & Boli, J.(2003). *The Globalization Reader*. Maiden: Mass.
132. Lemkin, R. (1933). Faut il un nouveau délit de droit gens nomme terrorisme, *Revue de droit penal et criminologie, Belge*, no. 13, 900–901.
133. Li, H., Squire, L. and Zou, H. (1998). Explaining International and Intertemporal Variations in Income Inequality. *The Economic Journal* Vol. 108, 26-43.
134. Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10(3), 393–411.
135. Lundberg, M. & Squire, L. (2000). *The Simultaneous Evolution of Growth and Inequality*. World Bank Working Paper.
136. Lutz M. J. & Brenda J. L. (2004). *Global Terrorism*, Routledge.
137. Ljajić, S., Meta, M., Mladenović, Ž. (2016). Globalizacija ekonomski i psihološki aspekti, *Ekonomski signali: poslovni magazin*, 11 (1), 39-62.
138. Mahoney, J. (2000). Path Dependence in Historical Sociology. *Theory and Society*, 29(4), 507-548.
139. Manap., N.A., & Tehrani, P.M. (2012). Cyber Terrorism: Issues in Its Interpretation and Enforcement. *International Journal of Information and Electronics Engineering*, 2(3), 409-413.
140. Mander, Dž. (2003). Pravila korporacijskog ponašanja. U: Dž. Mander i E. Goldsmit, T. Živić, M. Marković, I. Čorbić (Prir.). *Globalizacija – argumenti protiv*, Beograd: CLIO.

141. Marić, R. (1998). Potkulturni stil kao polje simboličke akcije. *Sociologija* 40(2), 159-190.
142. Matijašević, J. (2013). *Krivičnopravna regulativa računarskog kriminaliteta:monografija*, Novi Sad: Pravni fakultet za privredu i pravosuđe.
143. Matijašević-Obradović, J. (2014). The Significance and modalities of internet abuse as the primary global communicat. computer networks in cyberspace. *Megatrend revija* 11(1), 279-298.
144. Matijević, M. (2002). *Kriminalistika operativa*, VŠUP: Banja Luka.
145. Mattdort, J. H. & Whitman, E.M. (2011). *Roadmap to Information Security*, USA, Boston: Course Technology.
146. Merton, R.K. (1957). *Social theory and social structure*, Glencoe, Ill. : Free Press.
147. Mijalković, S. & Bošković, G. (2009). Pranje novca i finansiranje terorizma. U: *Korupcija i pranje novca – uzroci, otkrivanje, prevencija* (293–302). Sarajevo: Internacionalna asocijacija kriminalista.
148. Mijalković, S. (2008). Dihotomija organizovanog kriminala i terorizma iz ugla nacionalne bezbednosti, *Revija za bezbednost – stručni časopis o korupciji i organizovanom kriminalu* 2(12), 39-45.
149. Milašinović, R. i dr. (2011). Terorizam kao savremena bezbednosna pretnja. U: Šikman, M., Amidžić G. (ur.) *Suprostavljanje terorizmu- Međunarodni standardi i pravna regulativa*. Banja Luka: Visoka škola unutrašnjih poslova.
150. Milić, A. (2001). *Sociologija porodice: kritika i izazovi*, Beograd: Čigoja štampa.
151. Miller, C., Matusitz, J., O'Hair, D., & Eckstein, J. (2008). The complexity of terrorism: Groups, semiotics, and the media. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and retorical perspectives*. Cresskill, NJ: Hampton Press.
152. Mimica A., Bogdanović M. (2007). *Sociološki rečnik*, Beograd: Zavod za udžbenike.
153. Mittelman,H. J. (2000). *The Globalization Syndrome: Transformation and Resistance*, Princeton University Press.
154. Morris, M. W., Mok, A., Mor, S. (2011). Cultural identity threat: The role of cultural identifications in moderating closure responses to foreign cultural inflow. *Journal of Social Issues*, Vol. 67, 760–773.
155. Munkhdorj, B. & Yuji S. (2017). Cyber attack prediction using social data analysis, *Journal of High Speed Networks* 23 (2), 109–135.

156. Murthy, D. (2012). Towards a Sociological Understanding of Social Media: Theorizing Twitter, *Sociology* 46(6), 1059 –1073.

157. Nagar, et all (2002). Locating globalization: (re)readings of the subjects and spaces of globalization. *EconomicGeography* Vol. 78, 257–285.

158. Neeraj (2001). *Globalisation or Recolonisation*, ELGAR: Pune.

159. Nguyen, R. (2013). „Jus Ad Bellum“ in the Age of Cyber Warfare, *California Law Review* 101 (4), 1079-1129.

160. Nicholas N. (2007). *The Black Swon – The Impact of the Highly Improbable*, New York : Random House.

161. Ning, H., Liu, H., Ma, J., Yang, T. L., Huang, R. (2016). Cybermatics: Cyber-physical-social-thinking hyperspace based science and technology. *Future Generation Computer Systems* Vol. 56, 504-522.

162. Norasakkunkit,V. & Uchida,Y.(2011). Psychological consequences of postindustrial anomie on self and motivation among Japanese youth. *Journal of Social Issues* Vol. 67, 774–786.

163. Nosko, A., Wood, E., & Molema, S. (2010). All about me: disclosure in online social networking profiles: the case of Facebook. *Computers in Human Behavior* 26(3), 406–18.

164. O'Harrow, R. Jr. (2005). *No Place to Hide*, New York: Free Press.

165. Olsen, M. (1969). Two Categories of Political Alienation. *Social Forces* Vol. 47, 288-299.

166. Orman, H. (2003). The Morris Worm: A Fifteen-Year Perspective, *IEEE Security & Privacy* 1 (5), 35-43.

167. Palazzi, E. (1965). *Dizionario della lingua italiana*, Milano: Garzanti.

168. Paletz, L. D. & Schmid P. A. (1992). *Terrorism and the Media*, Sage Publications: Newbury Park.

169. Paul C. J. Robert, Rey, A., Debove J. Rey (1978). *Dictionnaire alphabétique et analogique de la langue française*[Le Grand Robert],Paris XIe, Société du nouveau Littré, Vol. 7, 1950.

170. Payne B. K., & Walton, C. D. (2002). Deterrence in the Post-Cold War World. In: John Baylis, James Wirtz, Eliot Cohen, and Gray Colin (Eds.), *Strategy in the Contemporary World, An Introduction to Strategic Studies*, Oxford: Oxford University Press.

171. Pejanović, Lj. (2003). *Terorizam i protivteroristička dejstva u vazdušnom saobraćaju*, Beograd:VIZ-JAT.

172. Pejanović, Lj. & Bejatović, M. (2009). *Avioterorizam*, Novi Sad: ABM ekonomik.

173. Petrović, B. & Jovašević, D. (2006). *Izvršno krivično/kazneno pravo.* Sarajevo: Pravni fakultet.

174. Petrović, D. (1998). Organizovani kriminalitet između vizije i realnosti. U: D. Stojanović (ur.) *Srbija i evropsko pravo* III (30-48), Kragujevac: Pravni fakultet Univerziteta: Institut za pravne i društvene nauke.

175. Petrović, R.S. & Stojanović R. M. (2016). Informaciona tehnologija u funkciji kriminala bele-kragne, *Zloupotreba informacionih tehnologija i zaštita*, Beograd: IT veštak, 13-26.

176. Petrović, S. (1994). Kompjuterski kriminalitet. *Bezbjednost* 1, 32-40.

177. Petrović, S.(2000). Kiber-terorizam, realnost ili fikcija? *Bezbednost* 42 (5/6), 643-675.

178. Petrović, S. (2001). Kiberterorizam, *Vojno delo* 53 (2), 100-122.

179. Piazza, J.A. & Walsh, J.I. (2010). Terrorism and Human Rights: Editors' Introduction. *Political Science and Politics* 43 (3), 407-409.

180. Pikettty, T. (2015). *Kapital u dvadesetprvom veku*, Sarajevo: Buybook.

181. Pipyros K., Thraskias C., Mitrou L., Gritzalis D., Apostolopoulos T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, *Computers & Security* Vol. 74, 371-383.

182. Pisarić, M. M. (2016). *Posebnosti dokazivanja dela visokotehnološkog kriminala*, Beogradski Univerzitet: Pravni fakultet.

183. Popović, L. (2017). *Metode borbe protiv kiberterorizma*. Master rad. Univerzitet u Beogradu: Fakultet političkih nauka.

184. Radovanović, R. & Lazarević, I. (2015). *Terorizam oružjem za masovno uništavanje*, Beograd: Kriminalističko - policijska akademija.

185. Robertson, R. (1992). *Globalization: Social theory and global culture*. London: Sage Publications Ltd.

186. Robertson, R. (2003). Globalizacija kao problem. U: Vuletić, V.(prir.) *Globalizacija – mit ili stvarnost* (182-213). Beograd: Zavod za udžbenike i nastavna sredstva.

187. Sasen, S. (2005). O globalizaciji i formiranju novih prava na grad. U: Vujović, S., Petrović, M.(prir.), *Urbana sociologija* (196-207). Beograd: Zavod za udžbenike i nastavna sredstva.

188. Sassen, S. (2002). Towards a sociology of information technology. *Current Sociology* 50(3), 365–385.

189. Savić, A., Stajić Lj. (2006). *Osnovi civilne bezbednosti*, Novi Sad: Fakultet za pravne i poslovne studije.

190. Savona, E.U., Adamoli, S., Di Nicola A. & Zoffi, P. (1998). *Organized Crime Around the World*, No. 31, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI).

191. Schimitt, N. M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press.

192. Schjolberg, S. (2014). *The History of Cybercrime: 1976-2014*, Koln.

193. Schmid, A. (1996). The links between transnational organized crime and terrorist crimes. *Transnational Organized Crime* 2(4), 40-82.

194. Schmid, A., Jongman A. (2005). *Political Terrorism*. Piscataway, NJ: Transaction Publishers.

195. Schuster, J. (2013). Invisible feminists? Social media and young women's political participation. *Political Science* 65(1), 8–24.

196. Selley, L. (2003). Organized Crime, Terrorism and Cybercrime. In: Alan Bryden, Philipp Fluri (eds.) *Security Sector Reform: Institutions, Society and Good Governance* (303-312). Nomos Verlagsgesellschaft: Baden-Baden.

197. Sennett, R. (1998). *The Corrosion of Character. The Personal Consequences of Work in the New Capitalism*. W. W. Norton & Company, New York/London.

198. Shelley, L. I. & Melzer, S., A. (2008). The Nexus of Organized Crime and Terrorism: Two Case Studies in Cigarette Smuggling, *International Journal of Comparative and Applied Criminal Justice* 32 (1), 1-21.

199. Shinder, L. D. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. USA; Rockland, MA: Syngress Publishing Inc.

200. Sieber, U. (1994). *Information Technology Crime – National Legislations and International Initiatives*, Köln: Carl Heymanns Verlag.

201. Silvey R. (2009). Development and geography: anxious times, anemic geographies and migration, *Progress in Human Geography*, 33(4), 507–515.

202. Simeunović D. (1991). *Državni udar ili revolucija*, Beograd: Studio plus.

203. Simeunović, D. (1989). *Političko nasilje*, Beograd: Radnička štampa.

204. Simeunović, D. (1993). *Nasilje. Enciklopedija političke kulture*, Beograd: Savremena administracija.

205. Simeunović, D. (2009). *Terorizam: opšti deo*, Beograd: Pravni fakultet Univerziteta u Beogradu.

206. Sinai, J. (2011). Terrorism on the Internet and Effective Countermeasures, *The Intelligencer: Journal of U.S. Intelligence Studies* Vol. 18, 21–24.

207. Skakavac, Z. (2010). *Terorizam - savremeni fenomenološki oblici ispoljavanja i karakteristike*. U: M, Kreća (ur.). Međunarodni naučni skup Terorizam i ljudske slobode, Vol. IX. (331-345), Beograd: Udruženje za međunarodno krivično pravo.

208. Sklair, L. (2013). Globalization. Capitalism and its Alternatives. Oxford University Press.

209. Sklair, L. (2001): *The Transnational Capitalist Class*, Oxford: Blackwell Publishers.

210. Smelser, N. J. (2003). Pressures for Continuity in the Context of Globalization. *Current Sociology* 51(2), 101–112.

211. Smit, D. A. (1998). *Nacionalni identitet*, Beograd, Biblioteka XX vek.

212. Sofaer, A. D. (2010). *The Best Defense? Legitimacy and Preventive Force*, Stanford, CA: Hoover Institution Press.

213. Solange G.H. (2009). *Cybersecurity Guide for Developing Countries*, Geneva: International Telecommunication Unione.

214. Sommestad, T. (2012). *A framework and theory for cyber security assessments*. Doctoral dissertation, Stockholm, Sweden: KTH, Royal Institute of Technology.

215. Soros, Dž. (2003). *O globalizaciji*, Beograd: Samizdat B92.

216. Srole, L. (1956). Social Integration and Certain Corollaries: An Exploratory Study. *American Sociological Review* XXI, 709-716.

217. Stallings, W. & Brown L. (2015). *Computer security : principles and practice*, Harlow : Pearson Education Limited.

218. Stamenković, B., Živanović, S., Paunović, B., Stevanović, I. (2017). *Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Republici Srbiji*, Sarajevo: Save the Children in North West Balkans.

219. Stavrou V, Kandias, M., Karoulas G., Gritzalis, D. (2014). Business process modeling for insider threat monitoring and handling. In: *Proccedings of the 11th international conference on trust, privacy &security in digital business* (119-131). Germany: Springer.

220. Stoll, C. (2005). *The Cuckoo's Egg*, New York: Gallery Books.

221. Stytz, M. (2006). Cyberwarfare Distributed Training, *Military Technology* (MILTECH) Vol. 11, 95-96.

222. Šikman, M. (2011). Terorizam kao kriminalni fenomen – kriminološko, kriminalističko, krivičnopravno gledište. U: M. Šikman, G. Amidžić (ur.)., *Suprotstavljanje terorizmu – međunarodni standardi i pravna regulativa* (43-63). Banja Luka: Visoka škola unutrašnjih poslova.

223. Škulić, M. (2003). *Organizovani kriminalitet. Pojam i krivično procesni aspekti*, Beograd: Dosije.

224. Škulić, M. (2014). Odnos organizovanog kriminalitet u krivičnopravnom smislu i saučesništva, *Nauka, bezbednost, policija: časopis Policijske akademije* 19 (3), 1-26.

225. Talbot, J. & Welsh D. (2006). *Complexity and Cryptography: an introduction*, Cambridge: Cambridge University Press.

226. Talijan, M. (2004). *Terorizam i antiterorističke snage*, Beograd: Generalštab Vojske Srbije i Crne Gore.

227. Tasić, V. & Bauer I. (2003). *Rečnik kompjuterskih termina*, Beograd: Mikro knjiga.

228. Tavani H. T. (2003). *Ethics and Technology: Ethical Issues in an Age of Information and Communications Technology*, Hoboken, John Wiley & Sons Inc.

229. Todd, E. (2003). *After the Empire: The Breakdown of the American Order,* New York: Columbia University Press.

230. Tomaševski, K. (1983). *Izazov terorizma*, Beograd: NIRO Mladost.

231. Tomlinson, John (1999): *Globalization and Culture*, Cambridge: Polity Press.

232. Tong, Y. -Y., Hui, P. P. -Z., Kwan, L., Peng, S. (2011). National feelings or rational dealings? The role of procedural priming on the perceptions of cross-border acquisitions. *Journal of Social Issues* 67, 743–759.

233. Torelli, C. J., Chiu, C. -Y., Tam, K. -P., Au, A. K. -C., & Keh, H. T. (2011). Exclusionary reactions to foreign culture: Effects of simultaneous exposure to culture in globalized space. *Journal of Social Issues* Vol. 67, 716–742.

234. Townsend, P. (1979).*Poverty in the United Kingdom*. Harmondsworth: Penguin Books.

235. Townsend, P. (1987). Deprivation. *Journal of Social Policy,* 16(2), 125–146.

236. Trager F. R & Zagorcheva, P. D. (2005-2006). Deterring Terrorism, *International Security* 30 (3), 87-123.

237. Trask, B. S. (2010). *Globalization and Family: Accelerated Systemic Soccial Change*, New York: Springer.

238. Tsakloglou,P. & Papadopulos,F.(2002). Aggregate Level and Determining Factors of Social Exclusion u Twelve European Countries.*Journal of European Social Policy* 12(3), 211–225.

239. Urošević, V. (2009). „Nigerijska prevara" u Republici Srbiji, *Bezbednost* Vol.3, 1-12.

240. Vandermoortele, J. (2002). *Are we really reducing global poverty*. New York: UNDP.

241. Vernotte, A., Dadeau, F., Lebeau, F., Legeard, B., Peureux, F, Piat, F. (2014). Efficient Detection of Multi-step Cross-Site Scripting Vulnerabilities, *10th International Conference on Information Security Systems*, Indija: ICISS 2014.

242. Vidanage, H. R. (2006). *Apparition of the predator*. The Lanka Academic, 6 (281), p. 3.

243. Vodinelić, V. (1984). *Kriminalistika*, Beograd: Savremena administracija.

244. Volerstin Imanuel (2005). *Uvod u analizu svjetskog sistema*, Cetinje: Otvoreni kulturni forum.

245. Volerstin, I. (2003). Globalizacija ili period tranzicije? Pogled na dugoročno kretanje svetskog sistema. U: V. Vuletić (prir.), *Globalizacija – mit ili stvarnost* (92-111), Beograd: Zavod za udžbenike i nastavna sredstva.

246. Vujaklija, M. (1975). *Leksikon stranih reči i izraza*, Beograd: Prosveta.

247. Vuletić, D. (2011). *Odbrana od pretnji u sajber prostoru*, Beograd: Institut za strategijska istraživanja.

248. Vuletić, V. (2006). *Globalizacija-aktuelne debate*, Beograd: Biblioteka Polis.

249. Wagner, R. Abraham (2005). Terrorism and the Internet: Use and Abuse. In: *Fighting Terror in Cyberspace, Terrorism and the internet*; (Eds.) Mark Last, Abraham Kandel, World Scientific.

250. Wagner-Pacifici, R. & Hall, M. (2012). Resolution of Social Conflict. *Annual Review of Sociology* Vol. 38, 181-199.

251. Walsh E. L. (1997). *Firewall : the Iran-contra conspiracy and cover-up*, New York: W. W. Norton & Company.

252. Walsh, J. I. (2007). Do States Play Signaling Games? *Cooperation and Conflict: Journal of the Nordic International Studies Association* 42 (4), 441.

253. Weaver, L.R., Abramson, W.L. & Bacigal, R. (2007). *Criminal Procedure, cases, Problem and Exercises*, USA: Gale Cengage.
254. Weimann, G. (2006). *Terror on the Internet: Tne New Arena, The New Challenges*, Washington: United States Institute of Peace Press.
255. Weimann, G. (2015). *Terrorism in Cyberspace. The Next Generation*, New York: Columbia University Press.
256. Weinstock N.N. (2000). Cyberspace self-Governance, *California Law Review* Vol. 88.
257. Williams, K. (2008). Using Tittle's control balance theory to understand computer crime and deviance, *International Review of Law Computers & Technology* 22 (1-2), 145-155.
258. Wong, P. T (2011). *Active cyber defense: enhancing national cyber defense*, Calhoun: The NPS Institutional.
259. Yang, D. Y-J., Chen, X., Cheng, S. Y. Y., Kwan, L., Tam, K. -P., & Yeh, K. -H.(2011). The lay psychology of globalization and its social impact. *Journal of Social Issues* Vol. 67, 677–695.
260. Yeates, N. (2001). *Globalization and Social Policy*, London: SAGE Publications.
261. Yergin, D., Stanislaw, J. (2002). *The Commanding Heights: The Battle for the World Economy*, New York: Simon & Schuster.
262. Yılmaz, E. N., Gönen S. (2018). Attack detection/ prevention system against cyber attack in industrial control systems, *Computers & Security* Vol. 77, 98.
263. Žoa, D., Šuler, M. (2005). Nejednakosti, teritorije i pokretljivosti: obnovljena perspektiva urbane sociologije. U: S., Vujović, M. Petrović (prir.), *Urbana sociologija* (248-262). Beograd: Zavod za udžbenike i nastavna sredstva.

Dokumenti (zakonska akta, odluke, akcioni planovi, uredbe, pravilnici, strateški dokumenti, agende)

1. European Commission (2015, 28 April). *European Agenda on Security: Questions & Answers*. Retrieved from: http://europa.eu/rapid/press-release_MEMO-15-4867_en.htm (16.5.2017)
2. Krivični zakonik, Službeni glasnik RS, br. 85/05, 88/05- ispravka, 107/05 – ispravka, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/85/6/reg (15.9.2019)

3. Ministarstvo unutrašnjih poslova (2015). *Akcioni plan za poglavlje 24*. Preuzeto s www.mup.gov.rs [preuzeto u pdf formatu] (30.4.2017)
4. Nacionalna strategija održivog razvoja, Službeni glasnik RS br. 57/08. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2008/57/1/reg (17.7.2017)
5. Nacionalna strategiju za borbu protiv pranja novca i finansiranja terorizma, Službeni glasnik RS, broj 3/15. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2015/3/1/reg (14.3.2017)
6. Nacionalna strategija za sprečavanje i borbu protiv terorizma za period od 2017-2021. godine, Službeni glasnik RS, broj 94/17. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/94/1/reg (30.12.2017)
7. Odluka o usvajanju Strategije nacionalne bezbednosti Republike Srbije, Službeni glasnik RS, broj 88/09. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/odluka/2009/88/1/reg (18.3.2017)
8. Odluka o usvajanju Strategije odbrane Republike Srbije, Službeni glasnik RS br. 107/15. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/odluka/2009/88/2/reg (7.8.2017)
9. Pakt stabilnosti inicijativa za Jugoiastočnu Evropu (2002, 27 Septembar). *eSEE Agenda za razvoj informacionog društva. Zajedničko zalaganje za implementaciju Informacionog društva u region Jugoistočne Evrope.* Retrieved from: http://www.mkt.gov.ba/dokumenti/informatizacija/ostali_propisi/default.aspx?id=3544&langTag=bs-BA (12.11.2017)
10. Pravilnik o uslovima koje mora da ispunjava kvalifikovano sredstvo za kreiranje elektronskog potpisa odnosno pečata i uslovina koje mora da ispunjava imenovano telo, Službeni glasnik RS, br. 34/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/34/4/reg (20.3.2019)

11. Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati, Službeni glasnik RS, br. 34/18 i 81/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/34/3/reg (21.1.2019)
12. Pravilnik o Registru pružalaca kvalifikovanih usluga od poverenja, Službeni glasnik RS, br. 31/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/31/8/reg (1.12.2018)
13. Pravilnik o Registru kvalifikovanih sredstava za kreiranje elektronskih potpisa i elektronskih pečata, Službeni glasnik RS, br. 31/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/31/7/reg (16.12.2018)
14. Pravilnik o Registru pružalaca usluga elektronske identifikacije i šema elektronske identifikacije, Službeni glasnik RS, br. 67/18. Preuzeto s http://pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/67/1/reg (7.12.2018)
15. Pravilnik o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u informaciono-komunikacionim sistemima, Službeni glasnik RS, br. 12/17. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2017/12/2/reg (23.12.2018)
16. Pravilnik o izboru programa od javnog interesa u oblasti razvoja informacionog društva koje realizuju udruženja, Službeni glasnik RS, br. 47/13 i br. 88/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2013/47/3/reg (21.12.2018)
17. Pravilnik o zahtevima za uređaje i programsku podršku za zakonito presretanje elektronskih komunikacija i tehničkim zahtevima za ispunjenje obaveze zadržavanja podataka o elektronskim komunikacijama, Službeni glasnik RS, br. 88/15. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2015/88/1/reg (18.12.2017)
18. Pravilnik o tehničkim i drugim zahtevima pri izgradnji prateće infrastrukture potrebne za postavljanje elektronskih komunikacionih mreža, pripadajućih sredstava i elektronske komunikacione opreme prilikom izgradnje poslovnih i stambenih objekata, Službeni glasnik RS, br. 123/12. Preuzeto s

http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2012/123/4/reg (7.2.2018)

19. Pravilnik o protokolu postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemarivanje, Službeni glasnik RS", br. 46/19. Preuzeto s https://www.paragraf.rs/propisi/pravilnik_o_protokolu_postupanja_u_ustanovi.html (18.9.2019)

20. Republika Srbija, Ministarstvo prosvete nauke i tehnološkog razvoja (2018). Informator *o radu Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije*. Preuzeto s http://www.mpn.gov.rs/wp-content/uploads/2018/04/Informator-o-radu-MPNTR-april-2018-latinica.pdf (8.9.2019)

21. Republika Srbija, Komisija za zaštitu konkurencije (2017). *Izveštaj o analizi uslova konkurencije na tržištu softvera i računarske opreme u Republici Srbije u periodu od 2014 - 2016. godine*. Preuzeto s http://www.kzk.gov.rs/kzk/wp-content/uploads/2018/01/Analiza-softveri-i-racunari-2017.pdf (28.8.2018)

22. Republika Srbija (2017). *Nacrt - Strategija nacionalne bezbednosti Republike Srbije*. Preuzeto s: http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/javna%20rasprava/strategije/Nacrt%20Strategije%20nacionalne%20bezbednosti.pdf (14.9.2018)

23. Republika Srbija (2017). *Nacrt – Strategija odbrane Republike Srbije*. Preuzeto s http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/javna%20rasprava/strategije/Nacrt%20Strategije%20odbrane.pdf (14.9.2018)

24. Stability Pact – eSEEurope Initiative (2002). eSEEurope Agenda for the Development of the Information Society. Retrieved from: http://www.eseeinitiative.org/file/2017/08/eSEEurope_Agenda.pdf (12.1.2012)

25. Strategija razvoja industrije informacionih tehnologija za period od 2017. godine do 2020. godine, Službeni glasnik RS, broj 95/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2016/95/1/reg (12.1.2017)

26. Strategija razvoja elektronske uprave u Republici Srbiji za period od 2015 – 2018. i Akcioni plan za sporovođenje Strategije za period 2015-2016. godine, Službeni glasnik RS br. 107/15. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2015/107/1/reg (4.4.2017)

27. Strategija naučnog i tehnološkog razvoja Republike Srbije za period od 2016. do 2020. godine, Službeni glasnik RS br. 25/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2016/25/1/reg (9.10.2017)

28. Strategija razvoja mreža nove generacije do 2023. godine, Službeni glasnik RS, br. 33/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/33/1 (3.4.2019)

29. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine, Službeni glasnik RS, br. 51/10. Preuzeto s https://www.paragraf.rs/propisi/strategija_razvoja_informacionog_drustva_u_republici_srbiji.html (8.11.2017)

30. Strategije razvoja trgovine u Republici Srbiji, Službeni glasnik RS, br. 15/09. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/reg/viewAct/85576edb-a45f-4292-b682-9668d4f8d5e4 (9.10.2017)

31. Strategije razvoja trgovine u Republici Srbiji do 2020. Godine, Službeni glasnik RS, br. 100/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2016/100/1/reg (7.10.2017)

32. Strategija zaštite podataka o ličnosti, Službeni glasnik RS, br. 58/10. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2010/58/1 (17.10.2017)

33. Strategija za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine, Službeni glasnik RS, br. 71/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg (8.5.2019)

34. Strategija razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine, Službeni glasnik RS, broj 68/10. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/reg/viewAct/df3fb65a-6acc-4e90-bd0f-f69066f6e0aa (19.11.2017)

United Nations (2006). *UN Global Counter-Terrorism Strategy*. Retrieved from: https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy (12.2.2017)

35. Uredba o uslovima za pružanje kvalifikovanih usluga od poverenja, Službeni glasnik RS, br. 37/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2018/37/2/reg (1.11.2018)

36. Uredba o bližem uređenju uslova koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti, Službeni glasnik RS, br. 60/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2018/60/1/reg (12.12.2018)
37. Uredba o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja, Službeni glasnik RS, br. 94/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/1/reg (12.1.2017)
38. Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenta i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, Službeni glasnik RS, br. 94/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/4/reg (16.3.2017)
39. Uredba o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja, Službeni glasnik RS, br. 94/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/2/reg (21.5.2017)
40. Uredba o utvrđivanju liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja, Službeni glasnik RS, br. 94/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/3/reg (23.6.2017)
41. Uredba o upravi za zajedničke poslove republičkih organa, Službeni glasnik RS, br. 63/13, 73/17 – dr. uredba, 76/17. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2013/63/4/reg (4.1.2018)
42. Uredba o bezbednosti i zaštiti dece pri korišćenju informaciono-komunikacionih tehnologija, Službeni glasnik RS, br. 61/16. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/61/1/reg (28.5.2017)
43. Uredba o Kancelariji za informacione tehnologije i elektronsku upravu, Službeni glasnik RS, br. 73/17, 8/19. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2017/73/2/reg (4.9.2019)

44. Zakon o ministarstvima, Službeni glasnik RS br. 62/17. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2014/44/1/reg (15.8.2018)
45. Zakon o elektronskom dokumentu, elektronskoj identifikaciji i ulugama od poverenja u elektronskom poslovanju, Službeni glasnik RS, br. 94/17. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2017/94/4/reg (15.8.2018)
46. Zakon o informacionoj bezbednosti, Službeni glasnik RS, br. 6/16, 94/17. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg (26.6.2018)
47. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Službeni glasnik RS, br. 61/05 i 104/09. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/61/7/reg (7.10.2017)
48. Zakon o elektronskim komunikacijama, Službeni glasnik RS, br. 44/10, 60/13 – US, 62/14 i 95/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2010/44/1/reg (14.10.2017)
49. Zakon o elektronskoj trgovini, Službeni glasnik RS, br. 41/09, 95/13, 52/19. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2009/41/4/reg (31.8.2019)
50. Zakon o zaštiti podataka o ličnosti, Službeni glasnik RS, br. 87/18. Preuzeto s https://www.paragraf.rs/propisi/zakon-o-zastiti-podataka-o-licnosti.html (8.2.2019)
51. Zakon o elektronskoj upravi, Službeni glasnik RS, br. 27/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/27/4/reg (14.3.2019)
52. Zakon o platnim uslugama, Službeni glasnik RS, br. 139/14, 44/18. Preuzeto s https://www.paragraf.rs/propisi/zakon_o_platnim_uslugama.html7 (15.2.2019)
53. Zakon o oglašavanju, Službeni glasnik RS, br. 6/16, 52/19 – dr. zakon. Preuzeto s https://www.paragraf.rs/propisi/zakon_o_oglasavanju.html (30.8.2019)
54. Zakon o javnom tužilaštvu, Službeni glasnik RS, br.116/08, 104/09, 101/10, 78/11– dr. zakon, 101/11, 38/12- US, 121/12, 101/13, 111/14- US, 117/14, 106/15, 63/16-US. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2008/116/4/reg (30.10.2017)

55. Zakon o upravnim sporovima, Službeni glasnik RS, br.111/09. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2009/111/6 (28.4.2017)
56. Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica, Službeni glasnik RS, br. 85/05. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/85/7/reg (31.1.2017)
57. Zakon o policiji, Službeni glasnik RS, br. 6/16, 24/18, 87/18. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/1/reg (9.7.2019)
58. Zakonik o krivičnom postupku, Službeni glasnik RS, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14 i 35/19. Preuzeto s https://www.paragraf.rs/propisi/zakonik_o_krivicnom_postupku.html (28.8.2019)
59. Zakon o potvrđivanju Sporazuma o operativnoj i strateškoj saradnji između Republike Srbije i Evropske policijske kancelarije, Službeni glasnik RS – Međunarodni ugovori, br. 5/14. Preuzeto s http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/mu/skupstina/zakon/2014/5/6/reg (7.12.2017)

Internet izvori

1. Awan, I. (2014). Debating the term cyber-terrorism, issues and problems, *Internet Journal of Criminology* [Online]. Retrieved from: https://pdfs.semanticscholar.org/1806/6b03bef29209009b55bfd6301f88a0e0f949.pdf?_ga=2.155224251.1203613720.1503162643-246278333.1503162643 (9.10.2017)
2. Bar, S. (2008, 2 June). *Deterring Terrorists*, Hoover Institution. Retrieved from: https://www.hoover.org/research/deterring-terrorists (17.2.2017)
BBC News World Edition (2003, 25 January). *Virus - like Attack Hits Web Traffic*. Retrieved from: http://news.bbc.co.uk/2/hi/technology/2693925.stm (27.4.2017)
3. Bogdanovski, M. & Petreski, D. (2016). Cyber Terrorism – Global Security Threat, *International Scientific Defence, Security and Peace Journal*. Retrieved from: https://www.academia.edu/11151330/CYBER_TERRORISM_GLOBAL_SECURITY_THREAT (15.2.2017)

4. CCDCOE (no date). *Tallin Manual 2.0*. Retrieved from: https://ccdcoe.org/research/tallinn-manual/ (10.1.2017)

5. Clay, W. (2007). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress, Congressional Research Service. Retrieved from: https://fas.org/sgp/crs/terror/RL32114.pdf (17.3.2017)

6. Council of Europe (2005). *Organised crime situation report 2005. Focus on the threat of economic crime*, Octopus Programme. Retrieved from: https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Report2005E.pdf (16.4.2017)

7. Davis, A. (1. februar 2002). The Afghan files: Al-Qaeda Documents from Kabul. *Jane's Intelligence Review*. Preuzeto s https://www.janes.com/security/janes-intelligence-review (7.2.2017)

8. Denning, D. (2000, 24 August). *Cyberterrorism.* [Prepublication version of a paper that appeared in Global Dialogue, Autumn, 2000]. Retrieved Aprile 4, 2018 from: http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf (8.5.2017)

9. Deutsch, J. (1996, 25 June). Statement before the US Senate Governmental Affairs. 1996 Conressional Hearings Intelligence and Security. Retrieved from: https://fas.org/irp/congress/1996_hr/s960625d.htm (23.9.2017)

10. Dewar, R. S. (2014). The Triptych of Cyber Security: A Classification of Active Cyber Defence. In: P. Brangetto, M. Maybaum, J. Stinissen (Eds.). *6th International Conference on Cyber Con ict* Retrieved from: https://www.academia.edu/6412868/_The_Triptych_of_Cyber_Security_A_Classification_of_Active_Cyber_Defence (8.4.2017)

11. Dougherty, C., Schwartz & Norris, F. (2008, 5 October). Financial Crises Spread in Europe, *The New Yourk Times*. Retrieved from: https://www.nytimes.com/2008/10/06/business/06markets.html?_r=1&hp&oref=slogin (19.3.2017)

12. Enisa (2018, 7 November). *EU cybersecurity organisations agree on 2019 roadmap*. Retrieved from: https://www.enisa.europa.eu/news/enisa-news/eu-cybersecurity-organisations-agree-on-2019-roadmap (12.12.2018)

13. European Parliament (no date). Fact Sheets on the European Union. Retrieved from: http://www.europarl.europa.eu/factsheets/en/home (17.3.2017)

14. Europol (no date). *European Cybercrime Centre – EC3*. Retrieved from: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (8.9.2017)

15. Eurostat Statistic Exiplained (2019, June). *Digital economy and society statistics – households and individuals*. Retrieved from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals (3.8.2019)

16. Fallico, M. (2013, 24 October). *Cyber terrorism*. Computer Crimes. Retrieved from: https://www.coursehero.com/file/8455402/Cyber-Terrorism-Essay/ (9.8.2018)

17. Farnsworth, T. (2011, June). China and Russia Submit Cyber Proposal, *Arms Control Association*. Retrieved from: http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal (6.5.2017)

18. Fischer E. A. (2005, 22 February). *CRS Report for Congress, Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, Congressional Research Service. The Library of Congress. Retrieved from: https://fas.org/sgp/crs/natsec/RL32777.pdf (25.4.2018)

19. Gercke, M. (2012, September). *Understanding cybercrime: phenomena, challenges and legal response,* Cibercrime: ITU. Retrieved from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (19.6.2017)

20. Glazer, Ilsa M. (Spring 2006). Armies of the Young: Child Soldiers in War and Terrorism (review). [Online] *Anthropological Quarterly*, 79 (2), 373-384. DOI:10.1353/anq.2006.0021. Retrieved from: https://muse.jhu.edu/ [Project Muse Database] (4.9.2017)

21. Goodman, S. E. (2007). Chapter 5: Cyberterrorism and Security Measures. In: National Academy of Sciences, *Science and Technology to Counter Terrorism Proceedings of an Indo US Workshop* (43-54). Retrieved from: https://www.nap.edu/read/11848/chapter/6#54 (7.11.2017)

Healey, J. (2012). *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council. Retrieved from: http://www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF (18.8.2017)

22. High-level Conference on Counter-Terrorism (2018, June 28-29). *High-level Conference of Heads of Counter-Terrorism Agencies of Memmber States*. Retrieved from: http://www.un.org/en/counterterrorism/hlc/index.shtml (17.12.2018)

23. Hutchins, E. M., Cloppert, M. J., Amin R. M. (2011). Intelligence - driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. In: *Proceedings of the 6th annual international conference on information warfare and security*, Washington DC. Retrieved from: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (18.12.2017)

24. Iasiello, E. (2012). *Identifying Cyber-Attackers to Require High-Tech Sleuthing Skills*, National Defense Industrial Association. Retrieved from: http://www.academia.edu/3680849/Identifying_Cyber-Attackers_to_Require_High-Tech_Sleuthing_Skills_Iasiello (30.11. 2017)

25. Iasiello, E. (2018, 1st Quarter). Is Cyber Deterrence an Illusory Course of Action? *ASPJ Africa & Francophonie* 9 (1), 35-51. Retrieved from: https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue-1/2018_1_e.pdf (19.5.2018)

26. ICT (2018). *Imagine Digital - Connect Europe*. Retrieved from: https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe (12.1.2019)

27. International Telecommunications Union (ITU) (2018, 29 October - 16. November). *ITU Plenipotentiary Conference Dubai UAE*. Retrieved from: https://www.itu.int/web/pp-18/en/ (17.12.2018)

28. Jalil, S. A. (2003, June). *Countering Cyber Terrorism Effectively: Are We Ready To Rumble?* Giac Security Essentials Certification (GSAC): Global Information Assurance Certification Paper. Retrieved from: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 (19.11. 2017)

29. Klein, J.J (2018). Deterring and Dissuading Cyberterrorism, *ASPJ Africa & Francophonie* 9 (1), 21-34. Retrieved from: https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue-1/2018_1_e.pdf (19.5.2018)

30. Knopf, W. J. (2013, 11 June). Use with Caution: The Value and Limits of Deterrence Against Asymmetric Threats, *World Politics Review*. Retrieved from: http://www.worldpoliticsreview.com/articles/13006/use-with-cautionthe-value-and-limits-of-deterrence-against-asymmetric-threats (18.7.2017)

31. Kronja, J. (2011). *Vodič kroz Strategiju Evropa 2020*, Beograd: Evropski pokret u Srbiji. Preuzeto s http://www.mpn.gov.rs/wp-content/uploads/2015/08/EU-2020.pdf (10.5.2017)

32. Lachow, I. (2013, February). *Active Cyber Defense. A Framework for Policymakers*, Policy Brief: Center for a New American Security. Retrieved from: https://s3.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf?mtime=20160906080446 (11.11.2017)

33. Lee, M., R. (2015). *Activecyber defense cycle: Asset identification and network security monitoring***.** Retrieved from: https://www.csemag.com/single-article/active-cyber-defense-cycle-asset-identification-and-network-security-monitoring/b69ad17203697864e47a8f5fec24fedb.html (21.10.2017)

34. Lewis, A. J. (2002, December). *Assessing the Risks of Cyber Washington DC, Terrorism, Cyber War and Other Cyber Threats*. Washington DC: Center for Strategic and International Studies. Retrieved from: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (10.1.2018)

35. Libicki, M. (2009). *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corp. Retrieved from: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (8.9.2017)

36. Mandt, E & Lee, R. (2016). *Leveraging Threat Intelligence in an Active Defense*. [Power Point Presentation]. Retrieved from: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492180823.pdf (23.9.2017)

37. Menn, J. (2013, May 18). *Cyber attacks against banks more severe than most realize*. Reuters. Retrieved from: https://www.reuters.com/article/us-cyber-summit-banks/cyber-attacks-against-banks-more-severe-than-most-realize-idUSBRE94G0ZP20130518 (5.8.2017)

38. Mitrović, Đ. (2017). *Na putu ka blagostanju 4.0 – Digitalizacija u Srbiji*. Beograd: Friedrich Ebert Stiftung. Preuzeto s http://library.fes.de/pdf-files/bueros/belgrad/13415.pdf (10.4.2018)

39. Mohsin, Saima; Khan, Shaan. (March 14, 2013). *Police: Kids young as 8 used as bombers in Pakistan*. CNN [Online] Retrieved from: https://edition.cnn.com/2013/03/14/world/asia/pakistan-child-bombers/index.html (15.3.2013)

40. Mulvenon, C. J. & Rattray, J. G. (2012). *Addressing Cyber Instability: Executive Summary*, Cyber Conflict Studies Association. Retrieved from: http://static1.1.sqspcdn.com/static/f/956646/19193589/1341880349257/CCSA+-+Addressing+Cyber (5.10.2015)

41. Murray, Rebecca (2010, October 29). *Scarred by Sri Lanka's war with Tamil Tigers, female exfighters build new lives*. The Christian Science Monitor. Retrieved from: http://www.csmonitor.com/World/Asia-South-Central/2010/1029/Scarred-by-Sri-Lanka-s-war-with-Tamil-Tigers-female-ex-fighters-build-new-lives (17.4.2017)

42. NATO (2002, 21-22 November). *Prague Summit*. Retrieved from: https://www.nato.int/docu/comm/2002/0211-prague/ (21.3.2017)

43. NIAS18 (2018, 16-18 October). Cyber Security Simposium. Retrieved from: https://www.cisco.com/c/m/en_emear/training-events/2018/nias/index.html (30.10.2018)

44. OSCE (2014). *Sprječavanje terorizma i suzbijanje nasilnog ekstremizma i radikalizacije koji vode ka terorizmu: Pristup kroz rad policije u zajednici*. Preuzeto s: https://www.osce.org/bs/secretariat/119226?download=true (17.1.2017)

45. OSCE (no date). FSC - Forum for Security Co-operation. Retrieved from: https://www.osce.org/forum-for-security-cooperation (18.2.2017)

46. Othman, E. S. (2012, September-October). Hide and Seek: Embedding Audio into RGB 24-bit Color Image Sporadically Using Linked List Concepts, *IOSR Journal of Computer Engineering (IOSRJCE)* 4 (1), 37-44. Retrieved from: http://www.iosrjournals.org/iosr-jce/papers/Vol4-issue1/G0413744.pdf (17.10.2017)

47. Rauscher, K. (2013, 27 November). *It's Time to Write the Rules of Cyberwar*, IEEE Spectrum. Retrieved from: https://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar (24.2.2017)

48. Rollins, J., Wilson, C. (2007, 22 January). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, CRS Report for Congress. Retrieved from: https://fas.org/sgp/crs/terror/RL33123.pdf (19.1.2018)

49. Saint-Claire, Steve (2011). *Overview and Analysis on Cyber Terrorism*, Retrieved from: http://www.oalib.com/paper/2690062#.W4Pa9V4zbIU (7.1.2017)

50. Scaparrotti, M. C (2014). Information Operations, *Joint Publication* 3-13. Retrieved from: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (18.1.2018)

51. Schmitt, M. N. (1999). Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework, *Columbia Journal of Transnational Law* Vol. 37, 885-937. Retrived from: http://www.dtic.mil/dtic/tr/fulltext/u2/a471993.pdf (14.3.2017)

52. Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington D.C.: The National Academies Press, 151-178. Retrieved from: http://wpressutexas.net/cs378h/images/f/fe/DeterringCyberAttacksWorkshop2010.pdf (19.3.2017)

53. Schneier, Bruce (2003, 16 December). *Blaster and the Great Blackout*, SALON. Schneier on Security. Retrieved from: https://www.schneier.com/essays/archives/2003/12/blaster_and_the_grea.html (23.11.2017)

54. Shielding (2003, 15 February). Shielding Cyber-Space, *Los Angeles Times.* Retrieved from: http://articles.latimes.com/2003/feb/15/opinion/ed-cyber15 (15.11.2017)

55. Smith, Tony (2001, 31 October). Hacker Jailed for Revenge Sewage Attacks. Job rejection caused a bit of a stink, *The Register. Biting the hand that feeds IT*. Retrived from: https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ (11.10.2017)

56. Sproles, J., Byars, W. (1998). *Statistics on Cyber-terrorism. Computer Ethics Course at ETSU*. Retrieved from: http://csciwww.etsu.edu/gotterbarn/stdntppr/stats.htm (14.3.2017)

57. Stalings, William (2011). *Cryptography and Network Security Principles and Practices*. Prentice Hall. Retrieved from: https://wanguolin.github.io/assets/cryptography_and_network_security.pdf (31.4.2017)

58. Swanson, J. (2012, 25 July). *Looking into the minds of killers*. Special to CNN [Online] Retrieved from: https://edition.cnn.com/2012/07/24/opinion/swanson-colorado-shooting/index.html (21.4.2017)

59. Taylor, A. M. (2002). *Globalization, Trade and Development: Somme Lessons from History*. NBER Working Paper Series, No. 9326. Retrieved from: http://www.nber.org/papers/w9326.pdf (23.10.2017)

60. Tikk, E., Kaska, K. & Vihul L. (2010). *International Cyber Incidents: Legal Considerations*. Cooperative Cyber Defence Centre of Excellence. Retrieved from: https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/ (6.8.2018)

61. United Nations (2008). *International Instruments related to the Prevention and Suppression of International Terrorism*. Retrieved from: https://www.unodc.org/documents/terrorism/Publications/Int_Instruments_Prevention_and_Suppression_Int_Terrorism/Publication_-_English_-_08-25503_text.pdf (30.8.2017)

62. Verbić, S. (2016). *ISTRAŽIVANJA za inovacije: strategija naučnog i tehnološkog razvoja Republike Srbije za period 2016 do 2020. god*. Beograd: Ministarstvo prosvete nauke i tehnološkog razvoja Republike Srbije. Preuzeto s http://www.mpn.gov.rs/wp-content/uploads/2015/08/Strategija-srpski.pdf (20.7.2018)

63. Vidojković, M. (2015). *Kompjuterski kriminalitet*. Master rad. Univerzitet u Nišu: Pravni fakultet. Preuzeto s: http://www.prafak.ni.ac.rs/files/master-radovi/milos-vidojkovic.pdf (23.9.2017)

64. Warren Axelrod, C. (2002, 27 February). *Security Against Cyber Terrorism.* Pershing Division of Donaldson, Lufkin & Jenrette Securities Corp 2002. Preuzeto s: http://www.sia.com/iuc2002/pdf/axelrod.pdf (6.7.2003)

65. Wasielewski, Philip G. (2007, 1st Quarter). Defining the War on Terror. [Online] *Joint Force Quarterly*, Issue 44, 13-18. Retrieved from: http://www.ndu.edu/press/lib/pdf/jfq-44/JFQ-44.pdf (26.2.2017)

66. Weigant, C. (2013, 28 October). *We Need a Geneva Convention on Cyber Warfare*, Huffington Post: The Blog. Retrieved from: https://www.huffpost.com/entry/we-need-a-geneva-conventi_b_4171853?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnJzLw&guce_referrer_sig=AQAAADlD2CIt4Wur3r4w3YYrl7IbJF3srq7aYRael71ZRPvqmhTirTeehGDNDs4yp8xFDJRKSC5hWSY-8VveoXq_7lK1Wy_oXLPqxGGuVf_tMWBFKMHg_hM4fcPvm4Ugz9hgcZTuiERtSHXTnD3iwKDbUk5AJkNnhutGDnfgO0zSD6QF (6.12.2017)

67. Weimann, G. (2004, March). *How Modern Terrorism Uses The Internet*. Special Report 116. Washington, DC: United States Institute of Peace. Retrieved from: https://www.usip.org/sites/default/files/sr116.pdf (24.12.2018)

68. Weimann, G. (2008, December). How Terrorists Use the Internet to Target Children. *InSite*: *The Official Newsletter of SITE Intelligence Group* 1(8), 14–16. Retrieved from: http://sitemultimedia.org/docs/inSITE_December_2008.pdf (15.10.2017)

69. Weimann, G. (2009, January). Virtual Sisters: How Terrorists Target Women Online. *InSite: The Official Newsletter of SITE Intelligence Group* 2(1), 19–22. Retrieved from: http://sitemultimedia.org/docs/inSITE_January_2009.pdf (27.11.2017)

70. Wilke, A. Clifford. (1999, 5 March). *Infrastructure Threats from Cyber-Terrorists*. Retrieved from: https://www.occ.gov/news-issuances/bulletins/1999/bulletin-1999-9.pdf (8.6.2018)

71. Wilson, C. (2003, 17 October). *Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress. Retrieved from: https://fas.org/irp/crs/RL32114.pdf (27.7.2018)

72. WSIS forum (2018, 19-23 March). Retrieved from: https://www.itu.int/net4/wsis/forum/2018/ (16.5.2018)

73. WSIS forum (2019, 8-12 April). Retrieved from: https://www.itu.int/net4/wsis/forum/2019/ (30.4.209)

74. Yagli, S., Dal, S. (2014). Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures, *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering* 8 (4). Retrieved from: https://pdfs.semanticscholar.org/959c/817cd8d725a3e37feb3b251b18a1c951e1cf.pdf (29.11.2017)

Biografija

Ivana Luknar, osnovno obrazovanje stekla je u OŠ "Milica Pavlović" u Čačku kao dobitnik Vukovog priznaja za postignut odličan uspeh i izvanredne rezultate na takmičenjima iz geografije i biologije. Srednju školu „Gimnaziju" takođe je završila u Čačku sa odličnim uspehom. Kao mladi istaknuti istraživač tokom srednje škole bila je polaznik naučno-istraživačkog centra „Petnica". Zvanje diplomirani sociolog stekla je na Filozofskom fakultetu u Beogradu sa izvanrednim rezultatima i prosečnom ocenom preko 9. Tokom studija radila je kao saradnik u nastavi na Filozofskom fakultetu u Beogradu na predmetu „Uvod u sociologiju". Učestvovala je u brojnim nevladinim projektima, međunarodnim konferencijama i humanitarnim akcijama za decu, kao i projektima pod pokroviteljstvom Instituta za sociološka istraživanja Filozofskog fakulteta. Pri kancelariji za ljudska i manjinska prava radila je na brojnim projektima vezanim za decu i dečja prava. Učesnik je projekta „Inkluzivno obrazovanje" pod pokroviteljstvom Saveta Evrope i Ministarstva obrazovanja Italije. Takođe je bila i učesnik međunarodne naučne konferencije održane 2014. godine na pomenutu temu. Autor je nekoliko objavljenih radova i knjige „Tebi-poučne priče za decu", izdavač Prosveta. Tečno govori engleski jezik i poseduje sertifikat B1+ English for Business Communication. Poseduje osnovno znanje nemačkog i kineskog jezika. U oblasti uspešnog poslovanja takođe poseduje sertifikat za izradu biznis plana dodeljen od strane Republičke Agenicije za razvoj malih i srednjih preduzeća i preduzetništva RS; sertifikat za upravljanje rizicima u realnom sektoru, kao i za efektivnu komunikaciju u poslovanju. Ivana je takođe odabrani dobitnik stipendije 30 mladih istaknutih istraživača iz celog sveta od strane SOU Open University u Šangaju, gde je boravila dve nedelje.

SPISAK OBJAVLjENIH RADOVA

Ivana (Luknar) Vasiljević (2011, 1. decembar). Intervju prof. dr Lesli Skler Transnacionalna kapitalistička klasa, *Geopolitika* br. 47, Dostupno na: http://www.geopolitika.rs/index.php/sr/intervju/360-intervju-prof-dr-lesli-skler-transnacionalna-kapitalisticka-klasa

Ivana (Luknar) Vasiljević (2015). Vuk Karadžić, nacionalni identitet i savremeni problemi obrazovanja u Srbiji, *Nacionalni interes*, br. 2, god. XI, Vol. 23, str. 9-30. Dostupno na: http://www.nacionalniinteres.rs/CD-NI%202-2015.pdf)

Ivana (Luknar) Vasiljević (2016). Challenges for inclusion of women in police profession. U: D. Kolarić (ur.), *Međunarodni naučni skup „Dani Arčibalda Rajsa“: Vol. 2. Tematski zbornik radova međunarodnog značaja* (p.280-291). Beograd: Kriminalističko-policijska akademija. Dostupno na: http://www.nsar.org.rs/sites/default/files/docs/Rajs_2016_Tom_2.pdf

Ivana (Luknar) Vasiljević, Dane Subošić (2017). Migranatska kriza kao izazov za očuvanje nacionalnog identiteta članica Evropske unije, *Vojno delo*, god. 69, br. 3, str. 72-88.

Ivana Luknar, Dane Subošić, Slaviša Krstić (2017, 4-5 June). Police subculture and potential stress risk. In: M Gjurovski (ed.), *Security concepts and policies - new generation of risks and threats: Vol. 2. International scientific conference Ohrid* (p.146-154). Skopje: Faculty of security.

Ivana Luknar (2017, 7-9 novembar). Organizational Behavior in Police. U: B. Simeunović-Patić (ur.), *Međunarodni naučni skup „Dani Arčibalda Rajsa“:Vol. 2. Tematski zbornik radova međunarodnog značaja* (p.151-159). Beograd: Kriminalističko-policijska akademija. Dostupno na: http://www.nsar.org.rs/sites/default/files/docs/Rajs_2017_Tom_2.pdf

Ivana Luknar (2018, 4 - 6 June). Terrorism and human rights. In: M Gjurovski (ed.), *Security System Reforms as Precondition for Euro-Atlantic Integrations. Vol. 2. International scientific conference Ohrid* (p. 94-99). Skopje: Faculty of security.