Pregledni rad
323.28:004
Primljeno: 14. travnja 2007.

Paradigma "novoga" terorizma informacijskoga doba

ANITA PEREŠIN*

Sažetak

U radu se predstavljaju rezultati istraživanja promjena značajki terorizma u informacijskom dobu, koji se odnose na utjecaje mrežnih tehnologija, kao posljedice informacijske revolucije na paradigmu terorizma. Promatrajući terorizam u širem kontekstu kao sukob, Arquilla, Ronfeldt i Zanini uočili su dva osobito zanimljiva aspekta utjecaja informacijske revolucije na njegovu narav: prvo, informacijska revolucija pospješuje nastajanje i jačanje mrežnih oblika organizacije te istodobno omogućuje ostvarenje njihovih komparativnih prednosti nad hijerarhijskim oblicima i drugo, načini vođenja i rezultati sukoba sve će više ovisiti o informacijama i informacijsko-komunikacijskim tehnologijama. Pritom su, istražujući njezin utjecaj na organizacijske oblike, postavili hipotezu o evoluciji hijerarhijskih u mrežne organizacijske oblike: lančanu mrežu, zvjezdastu mrežu i svekanalnu mrežu, što pospješuje i evoluciju terorizma ka vođenju "mrežnoga ratovanja", društvenoga sukoba u kojemu se sudionici koriste mrežnim oblicima organizacije te odgovarajućim doktrinama, strategijama i tehnologijama informacijskoga doba. Odabir načina vođenja mrežnoga ratovanja terorističkih organizacija ovisi o doktrinama koje oblikuju njihove ciljeve i strategije, a koje se mogu definirati kao paradigma prinudnoga pregovaranja, ratna paradigma i paradigma novoga svijeta. Osobit je problem što sve tri paradigme podupiru izvođenje *cyber* sabotaža sa svrhom ometanja funkcioniranja i/ili uništavanja informacijske infrastrukture. Temeljem navedenoga istražili smo značajke "novoga" terorizma na organizacijskoj razini, razini doktrine i strategije te na tehnološkoj razini. Rezultati provedenoga istraživanja potvrdili su evoluciju terorizma ka "mrežnom ratovanju" i nastajanje "novoga" terorizma pa će se sukladno tome i antiterorističke aktivnosti morati prilagoditi na organizacijskoj, strategijskoj i tehnološkoj razini. Prikazana metodologija ujedno je model istraživanja fenomena terorizma koji bi se mogao primijeniti u multidisciplinarnom pristupu antiterorističkim aktivnostima.

Ključne riječi: terorizam, globalizacija, informacijska revolucija, mrežni oblici organizacije, antiteroristička strategija

* *Anita Perešin*, Ured Vijeća za nacionalnu sigurnost.

Uvod: terorizam (definicije, značajke i utjecaj globalizacije)

Terorizam je danas jedna od najvećih prijetnji suvremenom društvu. Suvremeni ili megaterorizam posljedica je informacijske revolucije. Njegova su se obilježja mijenjala tijekom povijesti, neprekidno usklađujući svoje djelovanje s aktualnim društvenim političkim procesima, dostignućima u znanosti i tehnici te s razvojem tehnologije.

No, poseban je problem nepostojanje općeprihvaćene definicije terorizma te različita, a često i suprotstavljena stajališta najpoznatijih svjetskih stručnjaka, vlada, međunarodnih organizacija i institucija, čelnika država involviranih u terorizam, kao i istaknutijih vođa terorističkih organizacija o tome što je to zapravo terorizam, odnosno koja se djela, s obzirom na motive, način izvođenja i odabir ciljeva, smatraju terorističkima.

U povijesti se mnogo puta kroz najviše međunarodne institucije i organizacije pokušavala utvrditi općeprihvaćena definicija terorizma. Još se u Konvenciji Lige naroda iz 1937. godine navodi kako terorizam čine "... sva kaznena djela usmjerena protiv neke države i počinjena s namjerom da se stvori stanje straha kod određenih osoba, skupina osoba ili javnosti u cjelini ...".[1] No, suglasnost oko definicije terorizma bilo je teško postići ponajprije stoga što je za neke zemlje terorizam legitimno pravo na obranu te stoga teroriste smatraju borcima za slobodu. Potom, prema Laqueuru: "... nema definicije koja može u potpunosti definirati sve inačice terorizma, koje su se pojavile kroz povijest ..." (Laqueur, 1997.: 7).

U stručnoj literaturi postoji više od stotinu različitih definicija terorizma, a mi ćemo izdvojiti definiciju koju su predložili Schmid i Jongman, koja se smatra jednom od sveobuhvatnijih (ujedno i preciznijih) definicija: "... terorizam je metoda izazivanja straha poduzimanjem ponavljajućih nasilnih djela od strane ilegalnih grupa ili organizacija (moguće i pod pokroviteljstvom ili u organizaciji nekih država) zbog kriminalnih, političkih ili ideoloških razloga. Za razliku od klasičnoga ubojstva, ciljevi nasilja nisu ujedno i glavni ciljevi tih organizacija. Neposredne ljudske žrtve nasilja najčešće se biraju nasumično (ciljevi prilike) ili selektivno (ciljevi predstavnici/simboli) iz ciljane populacije te služe kao poslužitelji/generatori poruke. Komunikacijski proces prijetnjom ili nasiljem između žrtve i glavnih ciljeva ima za svrhu manipulaciju glavnoga cilja (u ovom slučaju glavni cilj je i u ulozi publike/promatrača) teroriziranjem, postavljanjem zahtjeva ili privlačenjem pozornosti ..." (Schmid, P. A.; Jongman, 1988.: 28).

[1] http://www.undcp.org/terrorism_definitions.htm.

Znatniji napredak postignut je donošenjem Rezolucije 1566 Vijeća sigurnosti Ujedinjenih naroda 8. listopada 2004. godine[2] i to zbog dvaju razloga. Najprije, jer ju je Vijeće sigurnosti donijelo jednoglasno, a onda i zato što se njome prvi puta zabranjuju svi oblici nasilja osobito usmjereni prema civilima, bez obzira na njihove motive. Tako u 3. poglavlju Rezolucije stoji da "kriminalne radnje počinjene nad civilima s ciljem izazivanja smrti ili ozbiljnih tjelesnih ozljeda, kao i uzimanje talaca s ciljem izazivanja straha kod cjelokupne populacije ili kod određene grupe ljudi, zastrašivanje javnosti, prisiljavanje vlade ili međunarodne organizacije na činjenje ili suzdržavanje od poduzimanja neke radnje, kao i sva ostala djela koja su kao kažnjiva definirana međunarodnim konvencijama i protokolima koji se odnose na terorizam, ni u kojem slučaju ne mogu biti opravdani razlozima političke, filozofske, ideološke, rasne, etničke, religijske ili bilo koje druge prirode te se pozivaju sve države da preventivno djeluju na sprječavanju takvih radnji i da se pobrinu za njihovo kažnjavanje sukladno težini njihova karaktera".[3] No, treba naglasiti da ova Rezolucija ne propisuje nikakve sankcije za države koje ne surađuju u borbi protiv terorizma, koje ne procesuiraju teroriste ili im pružaju utočište. [4]

Stručnjaci za terorizam i države koje se bore protiv terorizma suglasni su u ocjeni da će biti vrlo teško odrediti definiciju terorizma koju bi priznale sve zemlje svijeta, ali su također suglasni u tome da se bez nje ne može voditi uspješna internacionalna borba protiv terorizma. Terorizam više nije lokalni problem ili problem pojedine države, on je danas internacionalni fenomen te stoga i odgovor na terorizam moraju zajednički uskladiti sve države svijeta, što se danas čini nemogućim. No, bez odgovora na pitanje što je terorizam ne može se povesti uspješna borba protiv terorističkih organizacija i njihovih pomagača, ne može se tražiti odgovornost država koje ga podupiru, niti se mogu donijeti potrebni međunarodni sporazumi, čije je nepostojanje dosad pokazalo brojne otežavajuće okolnosti u borbi protiv terorizma.

Pri sagledavanju terorizma u suvremenim uvjetima, prema Javoroviću, treba uočiti i istražiti njegove značajke:

- *Globalizaciju.* Terorizam se može pojaviti na bilo kojem mjestu/zemlji, a njegove su posljedice globalne. Suvremeni je terorizam prijetnja cijelom svijetu, čovječanstvu, materijalnim dobrima, odnosno vrijednostima ljudske zajednice, pa se globalizira i strah od terorizma.

[2] Njezino je donošenje uslijedilo nakon terorističkog napada u Beslanu, Osetija, kad su čečenski separatisti u školi zatočili na stotine učenika i osoblja, od kojih je veliki broj stradao u sukobima uslijed akcije njihova oslobađanja.

[3] "Rezolucija 1566 Vijeća sigurnosti UN-a", http://www.mideastweb.org

[4] http://www.mideastweb.org

- *Univerzalizaciju i djelovanje logikom "cilj opravdava sredstvo"*. Očituje se u ciljevima, sredstvima i metodama, s obzirom na to da ne postoje ograničenja te će se odabrati i uporabiti sve ono što terorističke organizacije ocijene korisnim.
- *Veliki učinak i teške posljedice*. Odabiru se objekti čije će razaranje izazvati teške posljedice i ostvariti velik učinak s globalnim odjekom.
- *Stradavanje nevinih ljudi.*
- *Prilagođivanje promjenama i novim uvjetima.* Terorističke organizacije neprekidno usklađuju svoja djelovanja sa suvremenim procesima, dostignućima u znanosti i tehnici, osobito s internetskim i komunikacijskim tehnologijama.
- *Profesionalizaciju specijalnih izvršitelja i fanatizaciju pojedinaca, grupa i organizacija te povezivanje terorističkih organizacija i grupa.* Terorističke organizacije sve se više povezuju radi lakšega osposobljavanja, pripremanja i provođenja akcija (Javorović, 2001.: 23-24).

Dok neki autori pod globalizacijom terorizma podrazumijevaju proces kojim se terorizam nameće kao svjetska pojava, prijetnja i problem, Javorović globalizaciju terorizma vidi u[5]:

- stavljanju terorizma u funkciju internacionalizacije rata,
- najavi mogućnosti legalizacije terorizma/opravdanju terorizma kao oblika borbe za "opravdane/pravedne" ciljeve,
- stvaranju međunarodnih terorističkih skupina te
- ozbiljenju terorizma kao nuklearne, biološke i kemijske prijetnje (Javorović, 2001.: 35).

Istražujući čimbenike terorizma nedvojbeno je da postojanju i razvoju terorizma pridonosi i komunikacijsko-informacijska povezanost svijeta koja omogućuje da o terorističkom činu i zahtjevima terorista bude gotovo istoga trena obaviještena cjelokupna svjetska javnost. Tomu, ponajprije, pridonosi globalizacija masovnih medija i jačanje njihova utjecaja na sve sfere društva. Terorističke organizacije danas za svoje potrebe koriste sve funkcije masovnih medija, što je dokaz da su prepoznale značenje i ulogu masovnih medija u suvremenom društvu te da modele i tehnike komuniciranja uključuju u strategije svoga djelovanja sa svrhom postizanja što većega utjecaja na efekte koje masovno komuniciranje ima na društvo u cjelini.

[5] Ovdje nedostaje informacijsko-komunikacijska prijetnja (više o toj temi u nastavku rada, nap. a.).

Naime, bez pomoći medija, teroristička bi retorika imala utjecaj samo na one koji su izloženi terorističkom nasilju ili su se nalazili u njegovoj neposrednoj blizini. No, uz pomoć medija doseg je terorizma mnogo širi, tj. postaje globalan. Dakle, možemo reći da terorizam danas ima globalni dohvat i utjecaj koji nije imao prije globalizacije i informacijske revolucije.

Vezano uz korištenje masovnih medija, teroristi, prema Wilkinsonu, imaju četiri glavna cilja:

1. promicati djelo i stvoriti ekstremno snažan strah u ciljanim grupama,
2. mobilizirati širu potporu za svoj cilj među stanovništvom i međunarodnom javnom mnijenju, naglašavajući teme poput pravednosti svoga cilja i neizbježnosti pobjede,
3. frustrirati i omesti reakciju vlasti i snaga sigurnosti te
4. mobilizirati, potaknuti i povećati tijelo svojih stvarnih i potencijalnih pristaša te time povećati regrutiranje, prikupiti nova sredstva i potaknuti daljnje napade (Wilkinson, 2002.: 192).

Terorističke organizacije pritom, zbog njegove sveprisutnosti i anonimnosti, za potrebe propagande, regrutiranja, indoktrinacije, prikupljanje sredstava i vođenje psihološkoga rata, najviše se koriste internetom (Howard, 2004.: 289). Stoga danas sve više govorimo o "*e-jihadu*" i "*google* teroristima".

Analizirajući navedene značajke terorizma, postavlja se pitanje koje promjene možemo očekivati u području antiterorističke borbe. Sudeći prema stajalištima citiranih autora, promjene možemo očekivati na razini:

- samih protivnika/suprotstavljenih strana (u ovom slučaju terorističkih organizacija na organizacijskoj razini, razini doktrine i strategije te na tehnološkoj razini),
- u raznolikostima njihovih prijetnji te
- u načinima vođenja sukoba.

Također se postavlja pitanje u kojem će se smjeru razvijati terorizam, s obzirom na izbor načina ratovanja i nastajanje novih organizacijskih oblika.

Definicija i značajke mrežnoga ratovanja[6]

Informacijska revolucija utječe na narav sukoba u svijetu i mijenja ih te su Arquilla, Ronfeldt i Zanini (2004.) istražili utemeljenost sljedećih tvrdnji:

[6] Engl. Netwar = network + war.

1. informacijska revolucija pogoduje nastajanju i jačanju mrežnih oblika organizacije te istodobno omogućuje ostvarenje njihovih komparativnih prednosti nad hijerarhijskim oblicima;
2. načini vođenja te rezultati sukoba sve će više ovisiti o informacijama i informacijsko-komunikacijskim tehnologijama.[7]

To će osobito pridonijeti novim mogućnostima nedržavnih aktera koji će se tada lakše transformirati u multiorganizacijske mreže u odnosu na tradicionalne hijerarhijske državne aktere, s obzirom na to da su nedržavni akteri pristupačniji i primljiviji vanjskim utjecajima te učinkovitije koriste informacije pri unapređenju procesa donošenja odluka. Širenjem informacijske revolucije sukobi će sve više ovisiti o informacijskim i komunikacijskim mogućnostima te će, više nego ikada prije, znanje i sposobnost korištenja "mozgova", odnosno tzv. "meka snaga", postati odlučujućim čimbenikom rješavanja sukoba.

Prijetnje informacijskoga doba vjerojatno će biti raširene i raspršene te multidimenzionalne i višeznačne, a sukobi će se odvijati u rasponu od informacijskoga rata do *cyber* i mrežnoga ratovanja. Najveće razlike između informacijskoga rata (engl. *information warfare*), cyber ratovanja (engl. *cyberwar*) i mrežnoga ratovanja (engl. *netwar*) jesu:

- Informacijski rat podrazumijeva široko primjenjivanje destruktivne sile protiv informacijskih sustava, računalnih sustava i sustava koji podržavaju četiri ključna infrastrukturalna područja: energetiku, komunikacije, financije i transport. U svom članku pod nazivom "Information Warfare: What and How?" M. Burns definira informacijsko ratovanje kao "kategoriju tehnika, uključujući prikupljanje, prijenos, zaštitu, manipulaciju, prekid i uništenje informacija kojima se održava prednost pred protivnicima"[8]. Treba naglasiti da zbog kompleksnosti područja informacijskoga ratovanja ne postoji jedinstvena, sveobuhvatna i općeprihvaćena definicija tog pojma. U tom kontekstu Martin Libicki u svojoj knjizi "What is Information Warfare?" navodi da je "poimanje problema informacijskoga ratovanja isto kao dati slijepcu da prepozna slona: ako mu dotakne nogu kaže da je drvo, ako ga uhvati za rep kaže da je uže itd.", te na taj slikoviti način pokazuje brojne aspekte informacijskoga ratovanja.[9]

[7] Arquilla, J., Ronfeldt D.: The Advent of Netwar, RAND, 1996., str. 1, u pdf. formatu, preuzeto s http://www.rand.org

[8] Burns, M.: Information Warfare: What and How?, http://www-2.cs.cmu.edu/~burnsm/InfoWarfare.html

[9] Isto.

- Koncepcija *cyber* ratovanja odnosi se na informacijski usmjeren vojni sukob, uglavnom visokoga intenziteta, dok se koncepcija mrežnoga ratovanja odnosi na društveni sukob niskoga intenziteta i nevojnih operacija.
- Dok se u *cyber* ratu suprotstavljaju vojne snage, u mrežnom su ratu suprotstavljene nedržavne snage, paravojne i neregularne, kao u terorizmu (Howard, 2004.: 90).

Nijedna se od navedenih koncepcija ne odnosi samo na tehnološki aspekt, nego ih treba sagledavati na razini doktrine, taktike i strategije te na tehnološkoj razini primjene inovacija pri obrani i napadu. S druge strane, sve su tri koncepcije u suglasju s paradigmom "transformacije ratovanja"[10].

Koncepcija mrežnoga ratovanja odnosi se na društveni sukob u kojemu se sudionici sukoba koriste mrežnim oblicima organizacije te odgovarajućim doktrinama, strategijama i tehnologijama informacijskoga doba. Sudionici mrežnoga rata u najvećoj će mjeri biti raspršene manje grupe čiji se načini komunikacije, koordinacije i vođenja operacija odvijaju umreženo bez jasno utvrđenoga središnjeg zapovjednog mjesta. Sukobi i kriminalne aktivnosti temeljene na mrežnim strukturama postat će središnjim fenomenom u nadolazećem vremenu (Lesser, i dr., 1999.: 47). Arquilla, Ronfeldt i Zanini preobrazbu u tom smjeru sagledavaju kroz usporedbu značajki djelovanja (na organizacijskoj razini te na razini strategije, doktrine i tehnologije) Hamasa i PLO-a. (Howard, 2004.: 90).

Umrežavanje terorizma u informacijskom dobu

Informacijsko doba ne utječe samo na odabir vrste ciljeva i oružja terorističkih organizacija, nego i na njihov način funkcioniranja i strukturiranja (Arquilla/Ronfeldt, 2001.: 30). Potencijalna učinkovitost mrežnih organizacijskih oblika u odnosu na tradicionalni hijerarhijski ustroj privukla je pozornost teoretičara menadžmenta već 1961. godine, kad su se istraživači Burns i Stalker (1961.) referirali na organski oblik kao mrežnu strukturu kontrole, autoriteta i komunikacija s lateralnim, prije nego okomitim smjerom komunikacije.

Tri su osnovne značajke mrežnih organizacija:

1. Komunikacija i koordinacija nije unaprijed formalno određena vodoravnim ili okomitim vezama/odnosima izvješćivanja, nego se ostvaruje i mijenja prema potrebi.
2. Unutarnje se mreže (npr. dijelovi mrežne organizacije unutar jedne zemlje ili mrežna organizacija koja je dio veće mreže) najčešće nadopunjuju

[10] Više o tome u Van Creveld, 1991.

vezama s pojedincima izvan organizacije (često prelazeći nacionalne granice). I unutarnje i vanjske veze stvaraju se i gase ovisno o životnom ciklusu pojedinoga projekta/zadatka.

3. I unutarnje i vanjske veze ne definiraju "birokratska" pravila/zapovijedi, nego zajedničke vrijednosti i norme, kao i međusobno povjerenje. Veći dio aktivnosti obavljaju "samoupravljajući" timovi, dok vanjske veze čine "… organizirani skup koji uključuje kompleksnu mrežu tvrtki i grupa …" (Monge/Fulk, 1999.: 71-72).

Može se zaključiti da lateralni koordinacijski mehanizmi olakšavaju poduzimanje operacija mrežnih terorističkih organizacija, a podržani su napretkom informacijske tehnologije.

Razlozi zbog kojih nove informacijske i komunikacijske tehnologije podržavaju, odnosno pospješuju nastajanje mrežnih oblika organizacije su:

1. *Povećanje brzine komuniciranja* (uz povećanje propusnosti mreže i široke umreženosti). Nove tehnologije umnogome su smanjile vrijeme prijenosa, omogućujući učinkovitu komunikaciju i koordinaciju među raspršenim pripadnicima (grupama) terorističke organizacije.

2. *Smanjenje cijene komunikacije.* Nove su tehnologije znatno smanjile troškove komuniciranja, omogućujući tako održivost mrežnoga oblika organizacije (s obzirom na potrebu za intenzivnom komunikacijom).

3. *Integracija komunikacijskih i računalnih tehnologija*. Integracija komunikacijskih i računalnih tehnologija rezultirala je znatnim povećanjem opsega i složenosti informacija koje se mogu dijeliti putem mreže (Monge/Fulk, 1999.: 84).

Tehnologije informacijskoga doba osobito pogoduju mrežnim oblicima organizacije čiji su pripadnici/grupe zemljopisno raspršeni ili su zaduženi za provođenje različitih, ali komplementarnih aktivnosti. To ne znači da tradicionalne hijerarhijski organizirane terorističke organizacije neće prihvatiti i koristiti informacijsku tehnologiju sa svrhom poboljšanja internih zapovjednih, kontrolnih i komunikacijskih funkcija. Primjerice, sekta Aum Shinrikyo bila je organizacijski visoko centralizirana oko ličnosti vođe Shokoa Asahare s vrlo kohezijskom i strogom hijerarhijskom strukturom, no istodobno su se u znatnoj mjeri koristili informacijskom tehnologijom unutar grupe (Cameron, 1999.: 283).

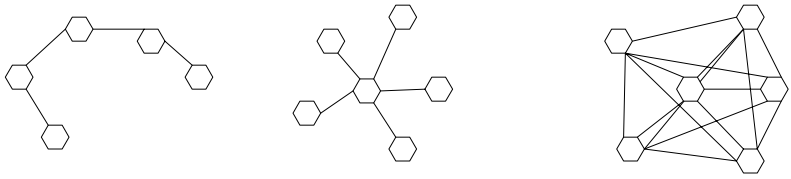
Mrežni oblici organizacije

Organizacijska struktura kakva već postoji u poslovnom svijetu sve se više počinje primjenjivati i među strukturama sudionika mrežnih ratova.

William M. Evan je definirao tri osnovna mrežna organizacijska oblika (Arquilla/Ronfeldt, 2001.: 7-8):

1. *Lančana mreža* – komunikacija između krajeva mreže odvija se preko posrednika, odnosno čvorova. Primjer: krijumčarski lanac u kojemu ljudi, roba i informacije putuju linijom koja se sastoji od odvojenih kontakata/čvorova i gdje komunikacija s jednoga na drugi kraj linije mora proći kroz sve dijelove lanca.
2. *Zvjezdasta mreža* – komunikacija i koordinacija među sudionicima mreže odvija se preko središnjega čvora. Primjer: organizacija kartela gdje su sudionici vezani uz središte ili glavnog organizatora te preko njega moraju komunicirati i koordinirati sve svoje djelatnosti.
3. *Svekanalna mreža* – suradnička mreža više međusobno povezanih manjih grupa. Primjer: mreža militantnih grupa.

Slika 1: Osnovni mrežni organizacijski oblici



Izvor: Arquila, J.; Ronfeldt, D.; Zanini, M.: Networks, Netwar, and Information-Age Terrorism, u: Howard, 2004.: 92.

Arquilla, Ronfeldt i Zanini objašnjavaju kako svaki ovaj oblik mrežne organizacijske strukture prema potrebi može biti prilagođen različitim uvjetima i namjenama. Čvor može biti pojedinac, grupa i/ili institucija (ili njihov dio), pa i država, dok "granice mreže mogu biti jasno određene, ali mogu biti i nedefinirane, odnosno nevidljive i porozne u odnosu na vanjsko okruženje. Čvorovi mreže mogu biti više ili manje povezani te biti ili ne biti uključeni u određeno članstvo (sve su kombinacije moguće)" (Howard, 2004.: 92).

Isti autori upućuju i na mogućnost kombiniranja njihove primjene te ističu kako tada nastaju hibridni oblici. Primjeri hibridnih oblika jesu:

1. mrežni akter može organizirati svoju jezgru kao svekanalnu te se istodobno koristiti lančanim i zvjezdastim mrežama za taktičke operacije,
2. hijerarhijski organizirani akter može se koristiti mrežnim organizacijskim oblicima za provođenje taktičkih operacija,

3. mrežni akter organiziran u obliku svekanalne mreže može se koristiti hijerarhijski organiziranim timovima za provođenje taktičkih operacija (Howard, 2004.: 92).

Konkretan je primjer hibridnoga oblika mreža Al-Qa'ide, odnosno komunikacija među pripadnicima te mreže. Simon i Benjamin navode da se "… komunikacija među pripadnicima Al-Qa'ide ostvaruje kombinacijom zvjezdaste mreže (kad čvorovi, operativci komuniciraju s bin Ladenom i njegovim bliskim suradnicima u Afganistanu) i svekanalne mreže (kad čvorovi mreže međusobno komuniciraju bez pozivanja bin Ladena) …" (Simon/Benjamin, 2000.: 70).

Prednosti mrežnih organizacijskih oblika nad tradicionalnim hijerarhijskim organizacijskim oblicima očituju se u sljedećem:

1. Hijerarhijski se oblici vrlo teško suprotstavljaju mrežnim organizacijskim oblicima. Konkretan primjer je neuspjeh kolumbijskih državnih tijela u borbi protiv narko-kartela.
2. Samo se novim mrežnim organizacijskim oblicima može učinkovito suprotstaviti postojećim mrežnim organizacijskim oblicima.
3. Tko prvi prihvati mrežni organizacijski oblik, stekao je kapitalnu prednost. (Howard, 2004.: 94-95).

Najteže je organizirati i održavati svekanalnu mrežu, koja zahtijeva učestalu komunikaciju, ali ona pruža najveće mogućnosti provođenja zajedničkih operacija te je "ujedno i mrežni oblik koji će najviše prosperirati informacijskom revolucijom" (Howard, 2004.: 92). U svekanalnoj mreži hijerarhija nije izražena ili je uopće nema, a unutar strukture može biti više vođa pa je stoga donošenje odluka, a katkad i samo djelovanje decentralizirano. To ponajprije omogućuje autonomiju te potiče inicijativu manjih skupina. No, Arquilla, Ronfeldt i Zanini upozoravaju na opasnost da upravo takva organizacija katkad može ostaviti kontradiktorne dojmove koji se kreću od anarhičnosti do višestruke organiziranosti. Pritom ističu kako učinkovito funkcioniranje ovakvoga mrežnog oblika "treba sagledati u njegovoj ovisnosti o postojanju zajedničkih interesa i ciljeva, tj. o postojanju doktrine ili ideologije čije neke značajke/stajališta prihvaćaju svi čvorovi" (Howard, 2004.: 92). Unatoč njihovoj raspršenosti i različitim zadaćama, pripadnicima mreže, tj. čvorovima, upravo zajednički prethodno usklađena i prihvaćena stajališta omogućuju usklađeno funkcioniranje (kao da su pobornici iste ideologije i doktrine). Tako je omogućena središnja ideološka i strategijska usklađenost koja istodobno podupire taktičku decentraliziranost. Ostvarenje svekanalne mreže ovisi o infrastrukturi koja omogućuje učestalo komuniciranje, odnosno protok funkcionalnih informacija. Arquilla, Ronfeldt i Zanini stoga ističu kako "ne trebaju nužno svi čvorovi stalno komunicirati (to ujedno znatno otežava konspirativnost), ali kad je komunikacija potrebna, pripadnici

mreže, čvorovi, moraju biti u mogućnosti proslijediti informaciju pravodobno i u potrebnu širinu (pripadnicima mreže, ali i vanjskoj publici)".[11]

Takav mrežni oblik organizacije odgovara nekadašnjoj SPIN[12] koncepciji, koju su šezdesetih godina 20. stoljeća osmislili Gerlach i Hine (1970.) pokušavajući opisati socijalne pokrete u SAD-u. Prema njima, karakteristike SPIN koncepcije su segmentiranost (znači da ima staničnu strukturu, sastavljenu od mnogo različitih grupa), policentričnost (znači da postoji više vođa ili različitih centara) te ideološka integriranost mreže.

Sagledavajući prednosti i primjenu mrežnih organizacijskih oblika, moramo uzeti u obzir sljedeće:

1. Iako mrežni akteri imaju koristi od povećanja brzine komuniciranja, povećanja propusnosti mreže, široke umreženosti, smanjenja cijene komunikacije te integracije komunikacijskih i računalnih tehnologija, ipak je učinkovita primjena potrebnih tehnologija problem za zemljopisno široko raspršene pripadnike mreže. Također, ne treba previdjeti da prihvaćanje potrebnih tehnologija, koje će omogućiti evoluciju ka mrežnim organizacijskim oblicima, nisu jedine i kritično potrebne tehnologije. Za mrežno funkcioniranje mogu biti dovoljni i "stari" načini komunikacije poput, primjerice, posredstvom kurira ili kombinacijom "novih" i "starih" načina komunikacije.
2. Također je potrebno naglasiti da mrežni rat nije internetski rat, tj. on se ne odvija isključivo u *cyber* prostoru, a način vođenja i ukupni rezultat mrežnoga rata ovise o događanjima u stvarnom svijetu.

Informacijska tehnologija, mrežno ratovanje i bliskoistočni terorizam

Koncepcija mrežnoga ratovanja konzistentna je i s obrascima događanja na Bliskom istoku, gdje je očito da novije i aktivnije terorističke organizacije usvajaju decentraliziranu fleksibilnu mrežnu strukturu, koja im omogućuje preobražaj iz formalnije organiziranih i državno sponzoriranih terorističkih organizacija ka privatno financiranim neformalnijim mrežama. Upravo takve mreže omogućuju pojedincima i grupama da, uz zajedničko vodstvo na strategijskoj razini, na taktičkoj razini mogu biti posve neovisni. Kad se govori o utjecaju informacijske tehnologije na djelovanje terorističkih organizacija, treba istaknuti sljedeće: ona omogućuje njihovu evoluciju k mrežnim

[11] Više o tome Gerlach, P. L. U: Johnson/Covello, (urednici), 1987. i Gerlach, i dr., 1970.

[12] Engl. *segmented, polycentric, ideologicaly integrated network* – SPIN.

organizacijskim oblicima i vođenju mrežnoga ratovanja, može im služiti kao oružje te kao potpora u vođenju i koordiniranju aktivnosti.

U prilog tome govore istraživanja Arquille, Ronfeldta i Zaninija (2004.) koji su na primjeru bliskoistočnih terorističkih organizacija dokazali sljedeći međuodnos informacijske tehnologije i mrežnog ratovanja:

1. Što je viša razina mrežne organiziranosti terorističke organizacije, to je veća vjerojatnost da se informacijska tehnologija koristi za potporu u procesu mrežnoga odlučivanja.
2. Najnoviji napredak informacijske tehnologije pomaže umreženim terorističkim organizacijama s obzirom na brži, jeftiniji i sigurniji protok informacija.
3. Prihvaćanjem informacijske tehnologije za potporu u odlučivanju i u druge organizacijske svrhe, raste vjerojatnost da će se terorističke organizacije koristiti istom tehnologijom kao napadačkim oružjem (u svrhu ometanja normalnoga funkcioniranja ili uništavanja) (Howard, 2004.: 98).

Već su 1999. godine rezultati istraživanja obrazaca i trendova aktivnosti na Bliskom istoku potvrdili hipotezu da "novi" terorizam evoluira ka mrežnom ratovanju s obzirom na to da:

1. sve veći broj terorističkih organizacija prihvaća mrežne oblike organizacije te se pritom sve više koristi informacijskom tehnologijom;
2. su terorističke organizacije (one koje su osnovane osamdesetih i devedesetih godina 20. stoljeća) umreženije od terorističkih organizacija s duljom tradicijom;
3. između stupnja aktivnosti terorističke organizacije i stupnja prihvaćanja mrežnoga oblika organizacije postoji pozitivna korelacija. U prilog toj tvrdnji Zanini i Edwards (Arquilla/Ronfeldt, 2001.) navode novije i manje hijerarhijski organizirane terorističke organizacije kao što su Hamas, Palestinski islamski džihad, Hezbollah i bin Ladenova teroristička mreža Al-Qa'ida, koje su ujedno postale i najaktivnijim terorističkim organizacijama;
4. je jednaka vjerojatnost da će se informacijska tehnologija koristiti kao organizacijska potpora i kao napadačko oružje pri ratovanju;
5. je veća vjerojatnost da su novoregrutirani pripadnici terorističkih organizacija osposobljeniji za korištenje informacijske tehnologije, što implicira da će terorističke organizacije u budućnosti biti umreženije te da će se više koristiti računalnom tehnologijom nego što to čine danas (Ian i dr., 1999.: 67).

Terorističke doktrine, mrežno ratovanje i informacijski terorizam

Evolucija terorizma prema mrežnom ratovanju stvorit će dodatne poteškoće antiterorističkim aktivnostima i djelovanjima. Ozbiljnost i veličina prijetnje ovisit će o doktrinama terorističkih organizacija. Naime, odabir načina vođenja mrežnoga ratovanja terorističkih organizacija ovisi o doktrinama koje oblikuju njihove ciljeve i strategije, a koje Arquilla, Ronfeldt i Zanini (Lesser, i dr., 1999.: 68-91) definiraju kao:

- *Paradigmu prinudnoga pregovaranja.* Metodu uvjeravanja ili nagovaranja drugih da nešto učine, da nešto prestanu činiti ili da poništе radnju koju su već učinili, George i William Simons (1994.) definirali su kao pregovaranje pod prinudom ili prinudno pregovaranje. Ako je namjera postizanje točno određenoga cilja uz ograničenu razinu nasilja, proporcionalnu željenom cilju, tada govorimo o terorizmu paradigme prinudnoga pregovaranja.

- *Ratnu paradigmu.* Strategijski cilj terorizma ratne paradigme jest nanošenje štete, odnosno uništavanje u kontekstu aktivnosti koje se poduzimaju u ratu koji je u tijeku. Ako, na primjer, uzmemo slučaj Osame bin Ladena i njegove objave rata Sjedinjenim Američkim Državama, vidimo da se kod ratne paradigme, za razliku od paradigme prinudnoga pregovaranja, ne teži uspostavljanju proporcionalnosti između razine nasilja, tj. primijenjene sile i ciljeva koji se žele ostvariti. Taj je primjer ujedno i potvrda Jenkinsove hipoteze (1974.) da se terorističke aktivnosti pojavljuju kad se slabija strana u sukobu ne može izravno suprotstaviti protivniku, pa pribjegava asimetričnim metodama (Jenkins, 1974.).

- *Paradigmu novoga svijeta.* Cilj terorizma paradigme novoga svijeta upravo je stvaranje novoga svijeta rušenjem političkoga, društvenog i ekonomskog poretka. Primjer je međunarodna vjerska sekta Aum Shinrikyo[13] koju je u Japanu osnovao Shoko Asahara. Ta se sekta pripremala za apokaliptični rat gomilajući velike zalihe kemijskih tvari, a njezini su pripadnici izveli napad plinom sarinom 1995. godine u vlaku podzemne željeznice koji se kretao prema središtu Tokija.

Osobit je problem što sve tri paradigme podupiru izvođenje *cyber* sabotaža (engl. *cybotage* = *cyber* + *sabotage*). Cyber sabotaža je "aktivnost/djelo ometanja funkcioniranja i/ili uništavanja informacijske infrastrukture koju poduzimaju pripadnici terorističkih organizacija koji su savladali, odnosno naučili vještine cyber terorizma" (engl. *cyberterrorism* = *cyber* + *terrorism*) ili "neprijateljski nastrojeni pojedinci koje su privukle ili angažirale terori-

[13] Vidi, Harmon, 2002.: 286., odnosno više o tome u: Horgan/Taylor, 2003.: 152-161.

stičke organizacije" (Howard, 2004.: 102). No, treba napomenuti da ne postoji jedinstvena definicija pojma cyber terorizma, najvećim dijelom zbog nepostojanja jedinstvene definicije terorizma (Embar-Seddon, 2002.: 1034).

Prema Denningu (1999.), cyber terorizam odnosi se na unaprijed smišljene i politički motivirane napade subnacionalnih grupa ili "tajnih agenata" usmjerene na informacijske sustave, računalne programe i podatke koji rezultiraju nasiljem prema civilnim (nevojnim) ciljevima. Devost, Houghton i Pollard (1997.) umjesto pojma *cyber* terorizma, definiraju informacijski terorizam kao svjesnu zlouporabu digitalnoga informacijskog sustava, mreže ili komponente sa svrhom omogućivanja ili podupiranja terorističke akcije.

Panarin i Panarina informacijski terorizam definiraju kao "novu vrstu terorističke djelatnosti pod kojom se podrazumijeva ciljani utjecaj na informacijsku infrastrukturu da bi se stvorili uvjeti koji rezultiraju katastrofalnim posljedicama po različite strane života i djelatnosti društva i države" (Panarin/Panarina, 2003.: 317). U tom kontekstu treba razjasniti i uporabu pojma "informacijskog ratovanja". Istraživanja informacijskoga ratovanja najčešće se odnose na sukobe među državama, odnosno na operacije država – država, pa je subdržavne fenomene i fenomen "sivoga područja", osobito informacijskoga terorizma tek potrebno istražiti (u okviru paradigme informacijskoga ratovanja). Fenomen "sivoga područja" odnosi se na političko nasilje za koje nije jasno vidljivo je li sponzorirano ili povezano s nekom državom ili nekom postojećom organizacijom (Devost, 1996.).

U današnjem društvu "trećega vala"[14] dvije su vrste napada koje terorističke organizacije mogu poduzeti, a koje možemo definirati kao informacijski terorizam:

1. Informacijska tehnologija je cilj napada, tj. cilj terorističke organizacije je informacijski sustav. Poduzimaju se sabotaže, elektroničke ili fizičke, sa svrhom uništavanja ili ometanja/prekidanja funkcioniranja informacijskoga sustava i pripadajuće informacijske infrastrukture (napajanja, komunikacija i dr.).
2. Informacijska je tehnologija oruđe/oružje u većoj operaciji. Terorističke će organizacije pokušati manipulirati informacijskim sustavom i/ili iskoristiti njegove slabosti mijenjajući ili otuđujući podatke, ili će pokušati "natjerati" sustav na izvođenje funkcije/akcije za koju nije namijenjen.

Panarin i Panarina ta dva oblika informacijskoga terorizma nazivaju *informacijsko-tehničkim,* odnosno *informacijsko-psihološkim terorizmom*. Posebnom vrstom informacijsko-psihološkoga terorizma ukrajinski stručnjak

[14] Za poduzimanje fizičkoga nasilja terorističke se organizacije koriste tehnologijom "drugoga vala", dok se informacijski napadi ubrajaju u paradigmu "trećega vala". Više o tome u: Toffler, 1980.

za pitanja nacionalne sigurnosti Viktor Cyganov smatra medijski terorizam. On se, objašnjava taj autor, može pojaviti u otvorenom i zatvorenom obliku. Otvoreni oblik obuhvaća propagandu, reklamu, agitaciju i informacijsko priopćenje, a zatvoreni audiosugestiju i videosugestiju, tj. zvučno i vizualno utjecanje, čak i hipnozu, neurolingvističko programiranje i druge psihološke tehnologije (Cyganov, 2004.: 25). Na strateškom planu medijski je terorizam namijenjen izazivanju straha, panike i kaosa, osjećaja nesigurnosti i nepovjerenja u vlast te destabiliziranju funkcioniranja vlasti (Han, 1993.: 210).

U *tablici 1*., koja prikazuje moguće varijante odabira sredstva napada i cilja napada (fizički vs. digitalni), *ćelija a)* se odnosi na tradicionalni terorizam, dok se *ćelije b), c) i d)* odnose na informacijski terorizam. No, "pravi" informacijski terorizam odnosi se samo na *ćeliju d)*.

Tablica 1. Moguće varijante odabira sredstva napada i cilja napada teroristička organizacije

		Cilj	
		Fizički	**Digitalni**
Sredstvo	**Fizičko**	a) konvencionalni terorizam, podmetanje eksplozivne naprave u Oklahoma Cityju	b) napad IRA-e na financijsku četvrt Londona, Square Mile 4. listopada 1992.
	Digitalno	c) izmišljeni scenarij, radio smetnje kao uzrok pada zrakoplova	d) trojanski konj u javnoj digitalnoj mreži

Izvor: Devost, M. G./Houghton/Pollard, *Information Terrorism: Can You Trust Your Toaster?***,** The terrorism research center, 1996.: 11., http://www.terrorism.com

Brojni stručnjaci iz područja terorizma u svojim radovima navode da će terorizam postati još opasnijim i smrtonosnijim, no s gledišta mrežnoga ratovanja umrežene bi terorističke organizacije mogle prije odabrati aktivnosti usmjerene na ometanje funkcioniranja nego na uništenje. Naime, umrežene će terorističke organizacije, bez sumnje, nastaviti uništavati imovinu i ubijati nevine ljude, ali bi se njihova strategija mogla usmjeriti i prema poduzimanju nesmrtonosnih aktivnosti, s obzirom na to da ranjiva informacijska infrastruktura omogućuje velik odabir ciljeva. U prilog toj tezi ide i Hoffmanovo mišljenje (Hoffman, 1994.: 29-30) da će zbog "operativnoga konzervatizma" koji proizlazi iz terorističkoga imperativa za postizanjem uspjeha "… terorističke organizacije uvijek pokušavati biti korak ispred tehnološke razine antiterorističkih aktivnosti[15], raspolažući s dovoljnim mogućnostima

[15] Neki autori razlikuju antiterorističku od protuterorističke djelatnosti, i to tako da se antiteroristička djelatnost odnosi na one aktivnosti koje imaju cilj prevenirati teroristično djelova-

prilagođivanja i suprotstavljanja antiterorističkim mjerama, ali će istodobno biti razmjerno umjerene pri odabiru ciljeva, kako bi bili sigurni u uspjeh operacije. Naime, "umjesto da napadnu osobito dobro zaštićeni cilj, odnosno poduzmu visokorizičnu 'visoko isplativu' operaciju, terorističke će organizacije radije istraživati potencijalne ranjivosti te tada jednostavno na odgovarajući način prilagoditi plan napada i taktiku …"(Hoffman, 1994.: 29-30).

Analiza terorističke taktike pokazuje da su terorističke organizacije sve više svjesne važnosti informacija i informacijsko-komunikacijske tehnologije za funkcioniranje demokratskih institucija. (Howard, 2004.: 102). Mrežni rat mogu voditi mnogobrojne terorističke organizacije, neovisno o svojim doktrinama, tj. paradigmama, ali nastajanje mrežnih terorističkih organizacija s ciljem vođenja rata dodatni je problem i to problem s vojnoga stajališta. Naime, pripadnici terorističkih organizacija tada bi kao vojnici/ratnici mogli pokazati i sve veći interes za neprijateljske vojne interese i ciljeve. Poznato je da su mrežni organizacijski oblici vrlo prilagodljivi i fleksibilni pri provođenju napadačkih operacija. To je osobito vidljivo kad skupina napadača pribjegne metodi skupnoga napada.[16] Skupni napad ili rojenje nastupa kad više raspršenih čvorova mreže konvergira cilju iz višestrukih smjerova sa svrhom postizanja održivoga pulsiranja sile. Vrlo malo analitičara proučava metode skupnoga napada, a to bi mogao biti ključ sukoba informacijskoga doba. U prilog toj tezi govori i mišljenje nekih autora da bi se napadi informacijskoga doba mogli ubuduće prije odvijati "u rojevima" nego tradicionalno "u valovima" (Khalilzad i dr., 1999.: 88).

Umjesto zaključka: nove antiterorističke strategije?

Paradigma "novoga" terorizma informacijskoga doba uključuje promjene koje su terorističke organizacije ostvarile na organizacijskoj i tehnološkoj razini, razini doktrine i strategije, kao i promjene u raznolikostima njihovih prijetnji te promjene u načinima vođenja sukoba.

Komunikacijsko-informacijska povezanost svijeta suvremenom terorizmu daje globalni domet i utjecaj kakav nije imao prije globalizacije i informacijske revolucije. Upravo informacijska revolucija pogoduje nastajanju i jačanju mrežnih oblika organizacije, čemu su se vrlo vješto prilagodile terorističke organizacije uvođenjem navedenih promjena.

nje. S druge strane, protuteroristička djelatnost odnosi se na one aktivnosti koje se poduzimaju kad je terorističko djelovanje već ostvareno. Riley/Hoffman, 1995.: 2.

[16] Više o tome u: Kelly, 1994.

Mijenja se i karakter sukoba, koji sada sve više ovise o informacijskim i komunikacijskim mogućnostima, a odlučujući čimbenik rješavanja sukoba postaje znanje, odnosno posjedovanje kvalitetnih informacija.

Tehnologije informacijskoga doba osobito pogoduju mrežnim oblicima organizacije čiji su pripadnici/grupe zemljopisno raspršeni ili su zaduženi za provođenje različitih, ali komplementarnih aktivnosti. Povećanje brzine komuniciranja, smanjenje cijene komunikacije te integracija komunikacijskih i računalnih tehnologija razlozi su zbog kojih nove informacijske i komunikacijske tehnologije pospješuju nastajanje mrežnih oblika organizacije. Uz to, organizacijska struktura kakva već postoji u poslovnome svijetu, sve se više počinje primjenjivati i među strukturama sudionika mrežnih ratova.

Prelazak s hijerarhijskih na mrežne organizacijske oblike bit će različit, odnosno neujednačen i postupan, ali rezultati provedenoga istraživanja potvrđuju evoluciju terorizma prema "mrežnom ratovanju" i nastajanje "novoga" terorizma te će, sukladno tome i antiterorističke aktivnosti trebati prilagoditi na području organizacije, strategije i tehnologije.

Funkcioniranje mrežnih terorističkih organizacija umnogome ovisi o protoku informacija te bi prekid njihova toka u znatnoj mjeri onemogućilo funkcioniranje i koordiniranje njihovih aktivnosti. Internet kao informacijska mreža omogućuje dvosmjernu komunikaciju te je razina korištenja informacijske infrastrukture u napadačke svrhe proporcionalna razini izloženosti terorističkih organizacija napadima protuterorističkih snaga. Može se očekivati da će terorističke organizacije nerijetko uspjeti ostvariti prednost uvjetovanu čimbenikom iznenađenja, ali tu taktiku možemo prilagoditi te primijeniti i u antiterorističkoj strategiji.

Antiterorističke aktivnosti moraju se usmjeriti na identificiranje mrežnoga oblika terorističke organizacije i to s organizacijskoga i tehnološkog gledišta, koje obuhvaća dodatnu educiranost kadrova, kao i opremljenost najsuvremenijom tehnologijom. Antiteroristička bi strategija trebala uzeti u obzir sljedeće preporuke:

1. kontinuirano praćenje načina korištenja informacijske tehnologije terorističkih organizacija te pritom obvezno razlikovanje utjecaja njihovih organizacijskih i napadačkih mogućnosti;
2. protumjere i odgovarajuće anti/protuterorističke aktivnosti moraju biti usmjerene prema "toku" informacija (ometanje, prekid toka, dezinformacije i dr.);
3. potrebno je poboljšati zaštitu informacijske infrastrukture jer njezina učinkovitija zaštita rezultira i uspješnijim odvraćanjem od napada.

Provedenim istraživanjem došli smo do potvrde teze o očekivanim promjenama terorističkih organizacija na organizacijskoj razini, razini doktrine i

strategije te na tehnološkoj razini, kao i o promjenama u raznolikostima njihovih prijetnji i načinima vođenja sukoba. S obzirom na to, opravdano je razmišljati i o organizacijskoj prilagodbi institucija zaduženih za suzbijanje terorizma radi njihova učinkovitijega suprotstavljanja postojećim mrežnim organizacijskim oblicima terorističkih organizacija.

Međunarodni stručnjaci suglasni su u ocjeni da će destruktivna moć novoga terorizma, usmjeri li on svoje djelovanje prema informacijskom ratu, biti jača od dosadašnjih klasičnih metoda, a šteta po čovječanstvo mogla bi nadmašiti onu uzrokovanu biološkim ili kemijskim oružjem.

Literatura

Arquilla, J./Ronfeldt, D., 1996: *The Advent of Netwar,* RAND, 1996., http://www.rand.org

Arquilla, J./Ronfeldt, D. (ur.), 2001.: *Networks and Netwars: The Future of Terror, Crime, and Militancy,* RAND

Burns, T./Stalker, G.M., 1961.: *The Management of Innovation,* Tavistock, London

Cameron, G., 1999.: Multi-Track Microproliferation: Lessons from Aum Shinrikyo and Al Qaeda*, Studies in Conflict & Terrorism,* Vol. 22.

Cyganov, V., 2004.: *Media-terorizm: Terorizm i sredstva massovoj informaciyi*, Nika-Centr, Kijev

Denning, D., 1999.: *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Nautilus Institute, Washington D.C., http://www.nautilus.org

Derenčinović, D., 2002.: *Novi antiterorizam na razmeđu depolitizacije i dejuridizacije*, Zbornik Pravnog fakulteta u Zagrebu 7 2002/3-4, Zagreb

Devost, M. G./Houghton/Pollard, 1996.: *Information Terrorism: Can You Trust Your Toaster?***,** The terrorism research center, http://www.terrorism.com

Devost, M. G./Houghton/Pollard, 1997.: *Information Terrorism: Political Violence in the Information Age*, Terrorism and Political Violence 9(1), 1997.

Embar-Seddon, A. 2002.: *Cyberterrorism: Are You Under Siege?*, American Behavioural Scientist 45(6)

Gerlach, P. L./Hine, V., 1970.: *People, Power, Change: Movements of Social Transformation*, The Bobbs-Merrill Co., New York

Han, H. H. (ur.), 1993.: *Terirism and Political Violence: Limits and Possibilities of Legal Control*, Oceana, New York

Harmon, C. C., 2002.: *Terorizam danas*, Golden marketing, Zagreb

Hoffman, B., 1994.: *Responding to Terrorism Across the Technological Spectrum,* RAND Corporation

Horgan, J./Taylor, M. (ur.), 2003.: *Terorizam u budućnosti*, Golden marketing, Zagreb

Howard, D.R., 2004.: *Terrorism and Counterterrorism*, The McGraw-Hill/Dushkin, Connecticut

Javorović, B., 1997.: Terorizam, *Policija i sigurnost*, godina 6, br. 1-2

Javorović, B., 2001.: O terorizmu, *Defendologija*, br. 1-4, Vol. 4, DEFIMI, Zagreb

Jenkins, B., 1974.: *International terrorism: A New Kind of Warfare*, RAND, P-5261

Johnson, B. B./Covello, V. T. (ur.), 1987: *The Social and Cultural Construction of Risk***,** D. Reidel Publishing Co., Boston

Kelly, K., 1994.: *Out of Control: The Rise of Neo-Biological Civilization*, A William Patrick Book – Addison-Wesley Publishing Company, New York

Khalilzad, Z./White, J. P./Marshall, A.W., 1999.: *Strategic Appraisal: The Changing Role of Information in Warfare*, RAND

Kopal, R., 2002.: *Značaj kriminalističke obavještajne analitike u antiterorističkoj djelatnosti*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Vol. 23, br. 2, Rijeka

Laqueur, W., 1996.: Postmodern Terrorism**,** *Foreign Affairs*, Vol. 75, br. 5

Laqueur, W., 1997.: *Terrorism*, Weidenfeld & Nicolson, London

Lesser, I. O. i dr., 1999.: *Countering the New Terrorism*, RAND

Monge, G./Fulk, J. (ur.), 1999.: *Shaping Organizational Form: Communication, Connection, and Community*, Thousands Oaks, Sage

Panarin, I./Panarina, L., 2003.: *Informacionnaja vojna i mir*, OLMA-PRESS, Moskva

Riley, K. J./Hoffman, B., 1995.: *Domestic Terrorism: A National Assessment of State and Local Preparedness*, RAND, Santa Monica

Schmid, P. A./Jongman, J. A., 1988.: *Political Terrorism***,** North-Holland Publishing Company, Amsterdam

Simon, S./Benjamin, D., 2000.: America and the New Terrorism, *Survival*, Vol. 42, br. 1

Simons, G./Simons, W., 1994.: *The Limits of Coercive Diplomacy*, Westview Press, Boulder

Toffler, A., 1980.: *The Third Wave*, William Morrow&Co., Inc., New York

Tuite, M./Chisholm, R./Radnor, M. (ur.), 1972.: *Interorganizational Decisionmaking*, Aldine Publishing Company, Chicago

Van Creveld, M., 1991.: *The Transformation of War*, Free Press, New York

Wilkinskon, P., 2002.: *Terorizam protiv demokracije***,** Golden marketing, Zagreb

Internetski izvori

http://www.undcp.org/terrorism_definitions.html

http://www.2.cs.cmu.edu/~burnsm/InfoWartare.html

http://www.mideastweb.org

Anita Perešin

NEW TERRORISM PARADIGM IN THE INFORMATION AGE

Summary

In this paper we are presenting the results of a scientific research on the changes in the characteristics of terrorism in the information age, relating to the influences of network technologies, results of the information revolution, the paradigm of terrorism. Perceiving the terrorism in a wider context as a conflict, Arquilla, Ronfeldt and Zanini have found two particularly interesting aspects of the influence of the information revolution on its characteristics: one, information revolution is favouring and strengthening network forms of organization, and is at the same time enabling the realization of their comparative advantages over hierarchical forms and two, the conduct and outcome of conflicts will increasingly depend on information and communication technologies.

Exploring the influence on organizational forms, they have formulated a hypothesis on evolution of the hierarchical forms into network forms of organization; chain network, star network and all-channel network, substantiating the evolution of terrorism towards netwar. Netwar refers to an emerging mode of conflict at societal level, in which the protagonists use network forms of organization and related doctrines, strategies and technologies of the information age. The choice of the opus operandi of the netwar by the terrorist organization depends on the doctrinal paradigms that formulate their goals and strategies, which can be defined as the coercive diplomacy paradigm, the war paradigm and the new-world paradigm. The particular problem is that all three paradigms offer room for cybotage with the goal of disruption and destruction of information infrastructure.

Based on the above stated premises we have researched "new" terrorism characteristics at organizational, doctrinal, strategic and technological levels. The study has confirmed the evolution of terrorism towards netwar and the emerging of "new terrorism", hence the counter terrorism activities will needed to be adapted at the organizational, strategic and technological levels respectively. Given methodology also represents a research model for the terrorism phenomenon which could be applied at a multidisciplinary approach to the antiterrorist activities.

Key words: terrorism, globalisation, information revolution, network forms of organization, antiterrorist strategy

Mailing address: Ured Vijeća za nacionalnu sigurnost, Jurjevska 34, HR 10 000 Zagreb. *E-mail:* aperesin@gmail.com