Тања МИЛОШЕВСКА **УДК: 327.36:327.88**

ГЛОБАЛНО АНТИТЕРОРИСТИЧКО ВМРЕЖУВАЊЕ

Кратка содржина

Технологиите на информацискатa доба особено им помагаат на мрежните форми на организации чии припадници/групи географски се разместени или се задолжени за спроведување различни, но комплементарни активности.

Во овој труд се укажува дека преминот од хиерархиски кон мрежни организациски форми ќе биде различен, односно неизедначен и постепен, додека резултатите на истражувањата ја потврдуваат еволуцијата на тероризмот кон „мрежно војување" и создавање „нов" тероризам, а соодветно на тоа и антитерористичките активности е потребно да се приспособат на полето на организација, стратегија и технологија.

***Клучни зборови**: ГЛОБАЛЕН ТЕРОРИЗАМ, АНТИТЕРОРИЗАМ, ВМРЕЖУВАЊЕ, РАЗУЗНАВАЧКИ ИНФОРМАЦИИ*

Вовед

Современиот тероризам преку комуникацискатa информациска поврзаност на светот (глобализација и информациска револуција) добива глобален досег и влијание. Всушност, информацискатa револуција го помага создавањето и јакнењето на мрежните форми на терористичките организации кои брзо се приспособуваат на промените. Се менува и карактерот на судирите, кои сега сè повеќе зависат од информацискитe и комуникацискитe можности, а одлучувачки фактор за решавање на конфликтите претставува знаењето, односно поседувањето квалитетни информации.

Од државно спонзориран тероризам, карактеристичен за времето на Студената војна, кој беше познат и како метод на специјалното војување, еволуирањето на тероризмот отиде во насока на премисите на религијата и анархијата. Вмрежувањето на религиозно обоените терористички групи во услови на техничко-технолошки развој и експанзија на глобализацијата претставува сериозна закана за светскиот мир и безбедност.

Информацискатa доба не влијае само на изборот на цели и оружје на терористичките организации, туку и на нивниот начин на функционирање. Потенцијалната предност на мрежните организациски облици во однос на традиционалниот хиерархиски поредок се согледува преку мрежната структура

на латерална контрола, авторитет и комуникација за разлика од вертикалната комуникација.

Информацискатa револуција го помага создавањето и јакнењето на мрежните форми на организација и истовремено овозможува остварување нивни компаративни предности над хиерархиските форми. Тоа особено ќе придонесе за нови можности на недржавните актери кои полесно ќе се трансформираат во мултиорганизациски мрежи во однос на традиционалните хиерархиски државни актери, со оглед на тоа дека недржавните актери побрзо се адаптираат на надворешните влијанија и попродуктивно ги користат информациите за унапредување на процесите за донесување одлуки.

Одговор на државите на терористичкиот предизвик

Функционирањето на мрежните терористички организации најмногу зависи од протекот на информации, односно прекинот на нивниот тек во голема мера ќе го оневозможи функционирањето и координирањето на нивните активности. Интернетот како информациска мрежа овозможува двонасочна комуникација, поточно, нивото на користење информациска инфраструктура во напаѓачки цели е пропорционална на нивото на изложеност на терористичките организации на нападите на противтерористичките сили. Може да се очекува дека терористичките организации често ќе успеваат да остварат предност - фактор на изненадување, но таа тактика може да се приспособи, односно примени во антитерористичката стратегија.

Современата терористичка мрежа се согледува како високорационален и интелигентен креатор на насилство кој планира неколку чекори понапред, со правилно проценување на консеквенциите на своите акции, кој не дејствува импулсивно на принципот на емоции.

Широко инкорпорирани во секоја димензија на јавниот живот, со можни влијанија во глобалната информациска, финансиска, образовна, берзанска, телекомуникациска мрежа, современите терористички мрежи остануваат, главно, невидливи за владините институции. Терористичката мрежа има способност да ги надгледува и попречува комуникациите помеѓу владините институции, способна е да обезбеди перманентни извори од кои може да добие информации за тоа што планира владата да направи во следниот период на прашањето: борба против тероризам. Преку своите спонзори и симпатизери е способна да ги користи сателитските фотографии кои ги покажуваат активностите на државните антитерористички сили и институции, способна е да ги контролира телефонските разговори и електронската пошта, што ѝ овозможува да го идентификува планот и стратегијата кои државата планира да ги преземе на антитерористички план. Нивната терористичка активност останува прикриена под политички програми на големите етнички, верски и социјални групи, што претставува голем проблем за владата, особено ако се користи со класичните методи на антитерористичка активност.

Одговорот на државите на терористичкиот предизвик во новото опкружување мора да биде модернизирано/современо и мора да го вклучи политичкиот и дипломатскиот пристап за креирање нови коалиции со големите маргинализирани социјални, етнички, верски и расни групи. Преку креирање коалиции со маргинализираните групи и отворање нови визии и можности преку вклучување на овие групи во процесот на економска глобализација и модернизација со поголем степен на социјална правда и демократија, државата ќе биде во можност да ја елиминира легитимноста на терористичките групи и на тој начин да ја елиминира нивната голема општествена моќ што ја црпат од тешката економска, социјална и политичка положба на големите маргинализирани општествени заедници. Без елиминација на оваа легитимност, политичкиот кредибилитет на терористичката мрежа не може да биде разорен, ниту терористичката мрежа може да биде елиминирана.

Меѓутоа, меѓународната заедница за да може успешно да формира коалиција со овие значајни фактори на меѓународните односи, неопходно е поголемо разбирање на политичките, економските и културните структури на периферните заедници, нивното чувство на беспомошност и пониженост во новиот светски поредок, што бара донесување нова антитеористичка доктрина и нова стратегија за борба против глобалниот тероризам, кои не би се сведувале исклучително само на преземање воени и полициски мерки.

Мрежно војување

Предностите на мрежните организациски форми во споредба со традиционалните хиерархиски организациски форми се согледуваат во следново.

1. Хиерархиските форми многу тешко се спротивставуваат на мрежните организациски облици. Конкретен пример претставува неуспехот на колумбиските државни структури во борбата против нарко-картелите.
2. Само со новите мрежни организациски структури може ефикасно да се спротивставува на постојните мрежни организациски форми.
3. Онаа страна која прва ќе ја прифати мрежната организациска форма, ќе се здобие со капитална предност (Howard 2004).

Концепцијата на мрежно дејствување - војување се однесува на општествен судир со низок интензитет и невоени операции, во кои актерите на судирот се користат со мрежни облици на организација, односно со соодветни доктрини, стратегии и технологии на информацискатa доба. Во мрежната војна се спротивставени недржавни сили, паравоени и нерегуларни, како и тероризам. Учесниците на мрежното војување ќе бидат помали групи чии начини на комуникација, координација и водење операции се одвиваат вмрежено без јасна утврдена централна заповедна позиција.

Концепцијата на мрежното војување е конзистентна со обрасците на случувања на Блискиот Исток, каде што е очигледно дека новите и активни терористички организации ја усвојуваат децентрализираната флексибилна мрежна структура, која им овозможува преобразба од формално организирани и државно спонзорирани терористички организации кон приватно финансирани неформални мрежи. Ако е повисоко нивото на мрежната организираност на терористичката организација, се јавува поголема веројатност информацискатa технологија да се користи за потпора во процесот на мрежно одлучување. Најновите достигнувања на информациските технологии им овозможуваат на вмрежените терористички организации побрз, поевтин и посигурен проток на информации. Преку прифаќање на информацискатa технологија за одлучување, се зголемува веројатноста дека терористичките организации ќе користат иста технологија како средство за напаѓање (со цел да се попречи нормалното функционирање или уништување).

Од аспект на мрежно војување, вмрежените терористички организации во иднина ќе одбираат активности кои ќе бидат насочени кон попречување на функционирање отколку на уништување. Имено, вмрежените терористички организации и понатаму ќе продолжат да го уништуваат имотот и да убиваат невини луѓе, но нивната стратегија може да се насочи и кон преземање несмртоносни активности, со оглед на тоа дека ранливата информациска инфраструктура овозможува голем дијапазон на цели. Во прилог на оваа теза е мислењето на Брус Хофман дека поради „оперативниот конзерватизам", кој произлегува од терористичкиот императив за постигнување успех, терористичките организации секогаш ќе се обидуваат да бидат чекор пред технолошкото ниво на антитерористичките активности, располагајќи со доволно можности за приспособување и спротивставување на антитерористичките мерки, но истовремено ќе бидат соодветно насочени и кон избор на целите за да бидат сигурни во успехот на самата операција. Така, „наместо да нападнат исклучително добро заштитена цел, односно да преземат високоризична операција, терористичките организации ќе ги истражуваат потенцијалните слабости за на едноставен начин да го приспособат планот на нападот и тактиката..." (Hoffman 2004).

Анализата на терористичките тактики покажува дека терористичките организации сè повеќе се свесни за важноста на информациите и информациско-комуникацискатa технологија за функционирање на демократските институции. Мрежното војување може да го водат многубројни терористички организации, независно од своите доктрини, т.е парадигми, но создавањето на мрежните терористички организации заради водење војна претставува дополнителен проблем од воен аспект. Имено, припадниците на терористичките организации тогаш како војници/борци можат да покажат сè поголем интерес за непријателските воени интереси и цели. Познато е дека сите мрежни организациони форми се многу приспособливи и флексибилни при спроведување напаѓачки операции. Тоа е особено видливо кога група напаѓачи прибегнуваат кон методот „блок на напади". Овој метод настапува кога повеќе распрскани/дисперзирани контакти на мрежата конвергираат кон целта од повеќе насоки со цел да постигнат одржлива сила на

пулсирање. Нападите во информацискатa ера е поверојатно дека ќе се одвиваат „во роеви" отколку традиционално „во бранови" (eds Khalilzad, White & Marshall, 1999).

Службите за спроведување на законот играат клучна улога во справувањето со многу закани кои се појавуваат на просторот на четвртата генерација. Полицијата разви многубројни механизми за справување со насилните терористички мрежи, картелите на дрога, транснационалните криминални организации, милитантните анархисти и до помал степен воените лидери. Она што е забележливо во овој поглед се инструментите за билатерална и мултилатерална полициска соработка преку организации како што се Европол и Интерпол (Wilkinson 1996). Полицијата ги развива своите структури за одговор и разузнавачките врски за да се справи со предизвикувачките реалности на мрежниот конфликт.

Исто така, воените сили се во процес на развивање свои одговори за овој нов континуитет на закани преку заедничка обука на високи полициски и воени офицери на ниво на универзитетски персонал; дискусии за соодветното ниво на воена поддршка на цивилните власти и соработка во спојувањето на напорите на разузнавачките операции.

Војската мора да ги засили своите специјални операции и да ги истражи вештините за собирање/контрасобирање и пулсирање/ контрапулсирање, потребни за ефикасно да ѝ се спротивстават на мрежната војна. Специјалните операции, најверојатно, ќе формираат основа за нашите идни воени одговори со конвенционалните сили кои ќе ги поддржуваат силите за специјални операции (Sullivan 2003).

Спротивставувањето на мрежната војна значително ќе бара единствено спојување на воените, полициските и разузнавачките операции. Овие нови структури треба да бидат хибридни организации што ќе ги спојуваат бенефитите од мрежните структури со оние на постојните организациски хиерархии. Подобреното разузнавање е витално и мора да биде компонента од секој пристап што ќе се избере. На тактичко и оперативно ниво, ова мора да вклучува подлабинско испитување на мрежната војна и развој на контрамрежна војна.

Тероризмот, транснационалниот организиран криминал и военото самоволие на лидерите не се одделни и различни феномени. Тие, всушност, се различните лица на војувањето на четвртата генерација. Приспособениот одговор што вклучува мешавина на сила од конвенционални воени, специјални операции, разузнавачки и безбедносни услуги, полицијата и цивилната заштита ќе бидат неопходни. Оваа мрежа на оператори ќе мора да го синхронизира одговорот преку јурисдикционите граници. За да се справи со овие меѓусебно поврзани закани, националната и меѓународната безбедност мора да развие структура на мрежна сила, заедно со мрежни инструменти и доктрина.

Со анализа на вмрежување на формите на глобалниот тероризам се потврдува тезата за очекувани промени на терористичките организации на организационо ниво, ниво на доктрина и стратегија попрецизно на технолошко ниво, како и промени на спектарот на закани и начините на водење на конфликтите. Со оглед на тоа, оправдано е да се размислува за организациска приспособеност на

институциите задолжени за спречување на тероризмот заради нивно поефикасно спротивставување на постојните мрежни организациски форми на терористички организации.

Деструктивната моќ на новиот тероризам и неговото фокусирање кон информациското војување ќе претставува закана која ќе биде поголема од класичните закани и може да ги надмине и заканите предизвикани од потенцијална употреба на биолошко или хемиско оружје.

Мрежните организации ја забрзуваат одлуката и акцијата во споредба со хиерархиската структура. Мрежите нудат неколку предности, но се претприемачки поради институционалната одбивност за промена на хиерархиското и на тој начин побавно организациско однесување. Владата или институцијата која инвестирала време и напор за развој на ефикасен хиерархиски процес не се префрла лесно на мрежа којашто има распуштена/лабава и децентрализирана контрола. Ова е слабост која асиметричниот опонент, кој не е врзан за слична хиерархиска структура, може да ја искористи. Можно решение е да се направи мрежа за поддршка на оперативното ниво на активност во хиерархиската организација.

Мрежата ги поддржува разузнавачките подготовки за операции на два начина: го поддржува собирањето, откривањето информации и разузнавањето и го забрзува овој процес на мрежниот систем.

Моменталниот терористички конфликт каде што антидржавните актери имаат клучна одлука (и повремено де факто заземаат држави) е дел од оперативниот простор кој еволуира. Бидејќи овој конфликт еволуира и веројатно се шири, следниве предизвици можат да се предвидат:

- ❖ поинтензивно влијание на мрежните форми;
- ❖ потенцијално заземање (или насилно вклучување) на држави;
- ❖ зголемено преклопување на криминалот и тероризмот (Bunker and Sullivan 1998).

Низа актери, како Ал-Каеда и слободните коалиции на криминални актери, герилци и бунтовници ги предизвикаа и може да се очекува да продолжат да ги предизвикуваат капацитетите на националната безбедност што беа дизајнирани да функционираат во рамките на националната државна рамка. Надвор од таа рамка, традиционалните структури имаат големи тешкотии (Bunker 1998).

Опсегот на актери во овој нов простор на четвртата генерација (терористи, транснационални криминални организации, милитантни анархисти и воени лидери) типично оперираат во мали дисперзирани единици. Тие ги користат слабите страни на системот за национална безбедност, флексибилноста и немаат способност да се распоредат во опсег на локации, можеби во истовремени операции. Пулсирајќи и собирајќи се низ географските и политичките граници, тие ги предизвикуваат традиционалните, хиерархиски структури. Тие користат мрежни форми на организација за да се соберат и растурат; пенетрираат и нарушат; повлечат и избегаат (Ronfeldt & Arquilla 2001).

Зголемувањето на мрежите (а оттука и мрежните противници) резултира од миграцијата на моќта на антидржавните актери што можат да се организираат во мултиорганизациски мрежи (особено мрежи со сите канали каде што сите контакти се меѓусебно поврзани) поподготвено отколку хиерархиските државни актери. Како резултат на тој тренд, криминалот и конфликтот засновани врз мрежи претставуваат растечка закана. Хиерархиите - полицијата, војската и безбедносните служби за да се борат против мрежи, прво мора да ја разберат природата на мрежната закана и потоа да создадат соодветна рамнотежа меѓу мрежите и хиерархиите за да се борат против овие нови закани.

Современите безбедносни сили можат да очекуваат соочување со мрежни противници во различни ситуации, повеќето во урбани средини. Тоа вклучува брзи напредувања во системот на информации и комуникации, подобрени сензори, системи на прецизно насочување и способноста за новини во широкодостапните технологии.

„Ќе оперираме на многу комплексно борбено поле што ги комбинира предизвиците на тежок и непознат терен, терористи и парамилитанти, како и бегалци и непријателски цивилни организации (од кои некои веројатно имаат врски со транснационален мрежен организиран криминал)" (Meigs 2001).

Иако често се потенцира дека е потребна мрежа за да се нападне мрежа, може да се забележи дека антитерористичкото вмрежување обично се потпира врз хибрид на хиерархија и мрежи. Во кој било случај, страната која ги раководи мрежите (и нивните односи со други организациски форми) веројатно ќе преовлада во сегашниот и иден конфликт.

Заклучок

Во суштина, не е само предизвикот од соочување со мрежните противници, туку предизвикот да се одреди со кој вид мрежа се соочуваме, а потоа да се одреди фактичкиот состав и врските во рамките на таа мрежа.

Сериозно внимание треба се посвети на ревизија на целата национална безбедносна структура на САД, Велика Британија, Европската унија и на меѓународните структури за да се преминат бирократските бариери за акција.

Антитерористичките активности мора да се насочат кон идентификација на мрежните форми на терористички организации, од организационо и технолошко гледно поле, кое опфаќа дополнителна едуцираност на кадрите, како и опременост со најсовремена технологија. Антитерористичката стратегија треба да ги земе предвид следниве препораки:

- континуирано следење на начините на користење информациски технологии на терористичките организации и разликување на влијанието на нивните организациски и офанзивни можности;

- противмерките и соодветните анти/контратерористички активности мора да бидат насочени кон текот на информации (попречување, прекин на текот, дезинформации и др.);
- неопходна е заштита на информатичката структура, бидејќи нејзината солидна заштита резултира со успешно одвраќање на нападите.

Новите пристапи на спојување на разузнавањето и разузнавачките операции се суштински елементи на структурата на мрежната сила. Новите инструменти и пристапи мора да имаат способност да ги сортираат релевантните информации и да ги идентификуваат задачите што се суштински за мисијата со цел да им се спротивстават на потенцијалните противници. Ова може потенцијално да се постигне со користење на традиционалните инструменти и современата информациска структура.

Литература

Bunker, RJ & Sullivan, JP 1998, Cartel Evolution: Potential and Consequences, *Transnational Organized Crime*, 4/2, pp. 55-74.

Bunker, RJ, 1998, *Five-Dimensional Cyber War fighting: Can the Army after next be defeated through complex concepts and technologies*, Carlisle: PA: US Army War College, Strategic Studies Institute.

Hoffman, B 1994, *Responding to terrorism across the technological spectrum*, RAND Corporation.

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

Khalilzad, Z, White, J & Marshall, A (eds.) 1999, *Strategic appraisal: The changing role of information in warfare,* RAND.

Meigs, MC 2001, Operational At in the New Century. *Parameters* 31/1, pp. 4-14.

Ronfeldt, D & Arquilla, J 2001, Networks, Netwars and the Fight for the Future, *First Monday*. Available from: http://firstmonday.orgissues/issues6_10/ronfeldt/index.html.

Sullivan, J 2003, 'Structure of network forces and C4I', in *Non-State Threats and Future Wars,* ed. R.J. Bunker, Frank Cass & Co. Ltd. p.153.

Wilkinson, P 1996, The role of the Military in Combating Terrorism in a Democratic Society, *Terrorism and Political Violence* 8/3.

Tanja MILOSHEVSKA

GLOBAL ANTI-TERRORIST NETWORKING

Summary

The technologies of the information age in particular help network forms of organizations whose members/groups are geographically detached or carry-out different but complementary actions.

In this paper emphasis is put on the shift from hierarchical to networked organizational forms which will be different specifically gradual and uneven, although the results of the research confirm the evolution of terrorism to "network warfare" and creating a "new" terrorism. Consequently anti-terrorism activities need to be adapted to the field of organization, strategy and technology.

Key words: *GLOBAL TERRORISM, ANTI-TERRORISM, NETWORKING, INTELLIGENCE INFORMATION.*