УДК : 343.533::004

ЗЛОУПОТРЕБА КИБЕР ПРОСТОРА КАО СРЕДСТВА МАСОВНЕ КОМУНИКАЦИЈЕ

Ненад Путник
Универзитет у Београду, Факултет безбедности
Милан Миљковић
Министарство одбране Републике Србије

Безбедносне претње информационим системима могуће је груписати у одређене врсте. Класификација се може спровести у односу на начин изазивања претњи, тј. техника и инструмената који се користе ради њиховог остваривања, као критеријума класификације. У досадашњим истраживањима у подручју кибер безбедности, безбедносне претње у кибер простору најчешће су поистовећиване са кибер нападима техничког типа (напади засновани на употреби малициозних програма − malware и напади усмерени на опструкцију услуга − distributed denial of service) и оним нападима у кибер простору који се заснивају на обмањивању других корисника кибер простора и злоупотреби њиховог поверења (социјални инжењеринг − social engineering и фишинг − phishing).

Осим различитих врста кибер напада који, свакако, представљају један вид злоупотребе кибер простора, евидентно је и специфично злоупотребљавање овог простора у односу на његову функцију средства за масовну комуникацију. У том смислу, категорији безбедносних претњи у кибер простору, осим већ поменута два аспекта кибер напада, приписујемо и „злоупотребе кибер простора као средства масовне комуникације“, као посебну врсту претњи, с обзиром на њихов деструктивни потенцијал у односу на појединце и друштво у целини. У раду је представљена детаљна класификација безбедносних претњи у кибер простору, а тежиште је на идентификацији, класификацији и дескрипцији оних феномена који се могу подвести под поткатегорију „злоупотреба кибер простора као средства масовне комуникације“. У том смислу, детаљно су описани и објашњени феномени злоупотребе кибер простора за информационо ратовање и за подршку тероризму.

Кључне речи: *информациони системи, кибер простор, претња, информационо ратовање, кибер операције, пропаганда, тероризам*

Увод

Информациони системи данас су изложени многобројним и разноврсним безбедносним претњама. Њихову функционалност могу угрозити све класичне претње, као што су ватра, вода, експлозија и друге, али и специфичне, релативно но-

ве претње, попут електронских и кибер напада. Један број нових претњи или, прецизније речено, оне претње за чије је манифестовање неопходно постојање рачунарске мреже (попут кибер напада) према парадигми *кибер безбедности* (енгл. *cyber security*) називају се кибер претњама, тј. безбедносним претњама у кибер простору. Под појмом *кибер претња* експлицитно се подразумева злонамерна употреба технологија које припадају кибер простору као инструмената претње, али и као циљева великог броја актера – криминалаца, терориста, организација и држава.[1]

Дакле, постоји једна специфична категорија претњи са префиксоидом „кибер". Оне су, као и традиционалне претње, усмерене против информационо-комуникационих система и информација које су садржане у њима, али су извори ових претњи и средства неопходних за њихову експликацију везани за кибер простор. Другим речима, њихово манифестовање омогућено је стварањем глобалне рачунарске мреже. То је, дакле, њихово дистинктивно обележје.

Проблему научне класификације претњи информационим системима, историјски посматрано, приступало се фрагментарно. Најстарији и најзаступљенији приступ јесте техничко-технолошки, са позиција информационих и математичких наука и њихових посебних дисциплина (као што су криптографија и криптоанализа). Умножавање врста претњи и повећање учесталости напада на рачунарске и мрежне системе, уз раст свести о могућим последицама за све аспекте друштвеног живота, утицали су на то да претње кибер простору постану предмет изучавања и других научних дисциплина. Безбедносне претње информационим системима, дакле, почињу да се изучавају и са других аспеката – војних, правних, криминалистичких и криминолошких. До делимичне, али не и потпуне унификације приступа дошло је са настанком концепта кибер безбедности. Делимична унификација омогућена је заузимањем једног ширег, обухватнијег приступа, који је настао као последица промењене перспективе у перцепцији претњи информационим системима. Страх од могућих последица за безбедност државе услед угрожавања информационих система довео је, дакле, до настанка концепта кибер безбедности.

Према томе, можемо констатовати да је концепт кибер безбедности проистекао из страха од могућег угрожавања националне безбедности. Овај приступ, данас прихваћен на наднационалном нивоу, захтева синергијску активност свих субјеката у међународној заједници, уз примарну улогу експерата на пољу информатичких наука, ради достизања безбедног кибер простора. Превентивне активности на усвајању хардверских и софтверских стандарда, оснивању националних и наднационалних експертских тела, побољшању међународне сарадње у овој области и усаглашавању националних закона у области кибер криминала јесу неопходни кораци у побољшању безбедности кибер простора, али никако не и довољни.

Безбедносне претње усмерене на информационе системе јесу, и свакако треба да буду, предмет изучавања свих наведених наука и њихових научних поддисциплина, на првом месту информационих наука. Ипак, с обзиром на комплексност овог феномена и на могуће последице које могу произаћи из угрожавања кибер простора за безбедност државе и становништва, сматрамо да је овај проблем и легитимно питање безбедносних наука, без обзира на тренутно непостојање јасно де-

[1] Fischer, E., CRS Report for Congress, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, http://csrc.nist.gov

финисаног појмовног апарата и чврстог теоријског оквира. Чини нам се логичним да информационе науке треба да имају примат у подручју безбедности и заштите информационих система, али, исто тако, и да безбедносне науке не треба да пренебрегавају други аспект феномена – последице за безбедност државе и становништва које могу произаћи из угрожавања информационих система.

Може ли се проблем решити уколико не познајемо његове суштинске узроке? Ко су актери безбедносних претњи, какви су њихови циљеви и који их мотиви покрећу? Јесу ли то појединци, организације или државне структуре? Да ли је угрожавање безбедности кибер простора последица само супротстављених и противречних интереса актера у кибер простору или је оно последица и њихових различитих вредносних перцепција? Није ли кибер простор постао универзално доступно бојно поље, поприште сукоба, које предочава сву комплексност односа проистеклих из процеса глобализације и њених последица?

Приступ овом сложеном проблему са позиција наука безбедности захтевао би идентификацију, класификацију и исцрпну анализу не само претњи усмерених ка кибер простору, већ и субјеката претњи, тј. њихових актера, са становишта различитих безбедносних парадигми, као што су: хумана, корпоративна, национална, регионална и глобална безбедност. На садашњем степену тематизације овог проблема то, међутим, није могуће учинити. Управо због тога, уважавајући основна епистемолошка начела, у овом раду смо се усредсредили на исцрпну дескрипцију и класификацију појавних облика овог феномена са аспекта безбедносних наука, ради формирања полазне грађе за будућа истраживања.

Класификација безбедносних претњи у кибер простору

Констатовали смо да се са позиција безбедносних наука у први план постављају оне претње кибер простору које могу угрозити безбедност информационог друштва. Овај аспект би, свакако, морао да узме у разматрање све до сада идентификоване претње информационим системима, али и да у центар пажње постави безбедносне претње са атрибутом намерности и њихове старе и нове појавне облике (схема 1).

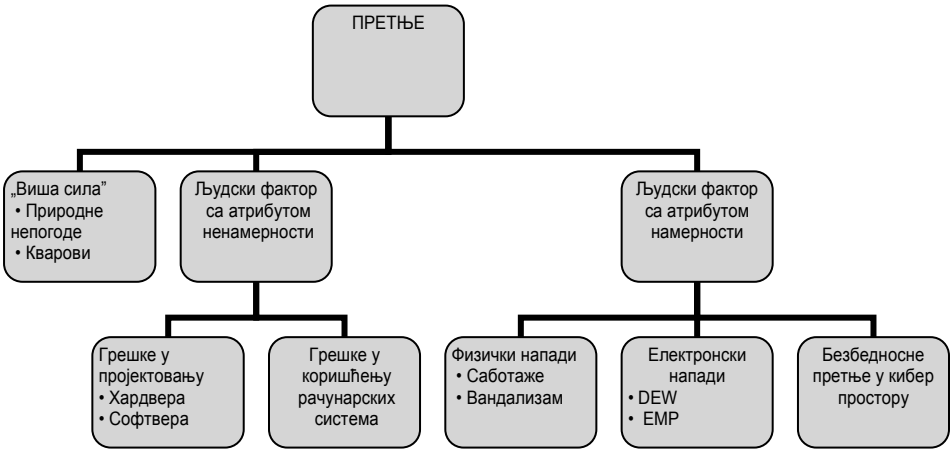

Схема 1 – *Класификација претњи информационим системима*

Класични појавни облици претњи информационим системима, сврстани у категорије „виша сила“, „људски фактор са атрибутом ненамерности“ и део скупа „људски фактор са атрибутом намерности“, који обухвата „физичке“ и „електронске“ нападе, историјски посматрано, познати су творцима безбедносних сценарија. За разлику од њих, нови појавни облици претњи, названи „безбедносне претње у кибер простору“ (или краће „кибер претње“), још нису чак ни идентификовани у потпуности. Тако, на пример, када се говори о актерима кибер претњи који користе кибер простор као циљ напада, а њему својствене технологије као средство за извршење напада, учестало се разматра проблем кибер тероризма, иако се на основу доступних података још не може тврдити да се иједан такав акт догодио. При томе, сматра се да ће управо претња кибер тероризмом представљати највећи безбедносни изазов у XXI веку. Свакодневно повећање начина злоупотребе кибер простора не само да представља тешкоћу у изналажењу адекватних мера за заштиту информационог друштва, већ и приморава на размишљање о могућим облицима угрожавања у будућности.

У најопштијем смислу, безбедносна претња у кибер простору може се рашчланити на две компоненте: начин изазивања (технике и инструменти) и субјект (актер) претње. Начин изазивања претње представља прави механизам претње, док је субјект претње особа или организација која иницира настанак претње или извршава акцију.

У односу на начин изазивања кибер претњи, тј. технике и инструменте који се користе ради њиховог остваривања, претње је могуће груписати у одређене врсте. У досадашњим истраживањима у подручју кибер безбедности, безбедносне претње у кибер простору најчешће су поистовећиване са кибер нападима техничког типа и оним нападима у кибер простору који се заснивају на обмањивању других корисника кибер простора и злоупотреби њиховог поверења.[2]

Осим различитих врста кибер напада, који, свакако, представљају један вид злоупотребе кибер простора, евидентно је и специфично злоупотребљавање овог простора у односу на његову функцију средства за масовну комуникацију. У том смислу, категорији безбедносних претњи у кибер простору, осим већ поменута два аспекта кибер напада, приписујемо и „злоупотребе кибер простора као средства масовне комуникације“, као посебну врсту претњи, с обзиром на њихов деструктивни потенцијал у односу на појединце и друштво у целини. У следећем схематском приказу покушали смо да, на основу увида у досадашња истраживања, али и властитих запажања, графички представимо једну, по нашем мишљењу, систематичнију класификацију безбедносних претњи у кибер простору.

Кибер напади који се базирају на употреби разноврсних малициозних софтверских апликација, али и они што се користе специфичним методима обмане појединаца који опслужују информационе системе, представљају значајну претњу не само складном функционисању информационих система већ и, посредно, целокупном друштву које се

[2] Под нападима техничког типа подразумевају се напади засновани на употреби малициозних програма (*енгл.* malware) као што су: вируси, црви, тројанци, итд., као и напади усмерени на дистрибуирану опструкцију услуга (*енгл.* distributed denial of service − DDoS). У категорију напада који се заснивају на обмањивању других корисника кибер простора и злоупотреби њиховог поверења уобичајено се сврставају тзв. социјални инжењеринг (*енгл.* social engineering) и фишинг (*енгл.* phishing). О врстама напада и њиховим карактеристикама видети детаљније у: Путник, Н., *Сајбер простор и безбедносни изазови*, Факултет безбедности, Београд, 2009.

на њима темељи. Можемо констатовати да су ове врсте претњи специфичне по томе што су усмерене на дестабилизацију инфраструктуре која је у основи кибер простора. Другим речима, кибер напад превасходно је усмерен на сâм кибер простор.

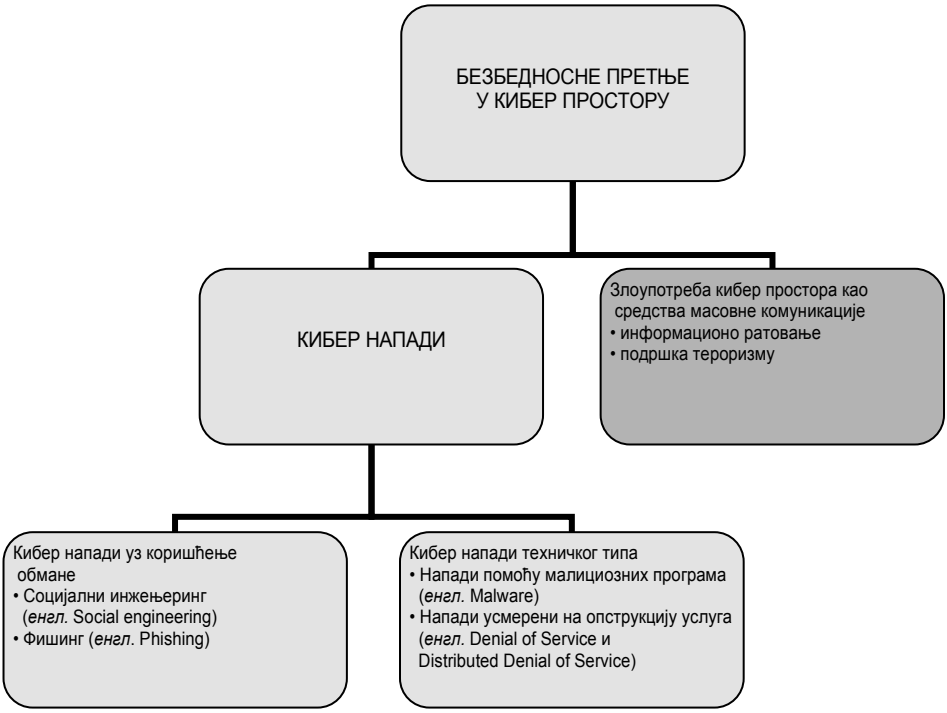

Схема 2 – *Класификација безбедносних претњи у кибер простору*

За разлику од њих, постоји и она категорија претњи информационом друштву која кибер простор злоупотребљава у једном ширем смислу – не као циљ, већ као средство. Реч је о специфичној злоупотреби кибер простора као средства за масовну комуникацију. Субјекти (актери) ове врсте претњи јесу националне армије, обавештајне службе, привредне корпорације, као и најразличитије мотивисане друштвене групе, међу којима се, по субверзивној активности, посебно истичу терористи.

Злоупотреба кибер простора за информационо ратовање

У информационој епохи, информациона револуција трансформише ратовање, тј. изазива промене у томе како друштва долазе у конфликт и како њихове оружане снаге воде оружани сукоб. Савремени сукоб је незамислив без великог броја релевантних информација о противнику, сопственим снагама, простору и времену. Сагласно томе, савремени сукоби су наглашено окарактерисани и као борба у сфери

информација. Са војног гледишта, информациони простор већ дуже време се посматра као борбени простор савременог глобалног друштва.[3] За разлику од индустријског доба, где су земље које су имале превласт на мору и у ваздушном простору „владале“ светом, у информационом добу земље које доминирају информационим простором остварују важан предуслов за доминацију у свету.

Нова друштвено-економска формација друштва повлачи за собом и нове претње безбедности, које, са друге стране, иницирају нове приступе у борби против нових претњи. Императив информационог друштва је информациона доминација у животно важним областима. Ако ово запажање пренесемо на војну сферу и сферу безбедности, можемо рећи да је једна од основних карактеристика „сукоба“ у информационом друштву сукоб у могућности приступа информацијама, тј. сукоб информацијама, које се данас назива „информационо ратовање“.

Информационо ратовање није нова појава. Историја људске цивилизације сведочи о бројним примерима информационог ратовања који указују на значај информације у постизању информационе супериорности у односу на противника. Израз „информација у рату“ претходио је изразу „информационо ратовање“. Први израз односи се на тактичко и стратешко заваравање, ратну пропаганду и уништавање командних и контролних система. Пример информације у рату представља употреба пропагандних форми разгледница, памфлета, говора и постера, које су растурали Американци и Немци током оба светска рата.[4]

Пракса и искуство из савремених сукоба такође показују да се сукоби у сфери информација појављују као претходница војних операција, током операција као њихов део и у експлоатацији њихових резултата. Свим војним сукобима у свету, после осамдесетих година прошлог века, претходили су сукоби у сфери информација или друге акције тог карактера којима су припремане војне операције. Неоружана дејства трају непрекидно, док се оружана, ако до њих дође, догађају повремено и ациклично.[5] Када је реч о сукобу неоружаним средствима, они се, такође, врло често воде у сфери комуникација. Такође, имајући у виду неке од изнетих карактеристика информационог друштва, као и искуства из савремених сукоба, у савременим војним теоријама и актуелним трансформацијама оружаних снага, преовлађују концепти ратовања засновани на информацијама и, као такви, спроводе се у сфери комуникације.[6] Тако у савременим концептима ратовања наилазимо на појмове *информационог ратовања*, *мрежноцентричног* ратовања и сл. Информациона технологија, као кључни аспект глобализације, има веома важну улогу претварајући, у модерном рату, информацију у све важнији и кључни ресурс. То је место где концепт информационог ратовања добија посебан значај. Основна предност је у томе што се применом информационог ратовања, односно

[3] Вулетић, Д., „Шта је информационо ратовање“, *Безбедност*, 3/'05, 2005, стр. 491.

[4] О појму пропаганде, али и о терминима са сродним појмовним значењем (агитација, индоктринација, „испирање мозга“, психолошки рат, субверзија, итд.), видети шире у: Милашиновић, Р., Милашиновић, С., *Увод у теорије конфликата*, Факултет цивилне одбране, Београд, 2004, стр. 289–314.

[5] Форца, Б., „Нове форме сукоба“, *Војни информатор*, 4/01, 2001, стр. 14.

[6] Комуникациону сферу, посматрано не само са војног аспекта, чине измешане цивилне и војне информационе мреже и технологије, са електронским линковима и другим везама које повезују појединце, групе, организације и нације широм планете, омогућујући им да готово непојмљивим брзинама размењују огромне количине најразноврснијих података и информација.

контролом информација, стварају предуслови за савладавање противника уз минималне губитке на људском, финансијском, друштвеном и политичком плану.

Од Другог светског рата до данас, у међународној војној теорији непрекидно се мењао назив за делатности коју данас називамо *информационо ратовање* (IW). У прошлој деценији она је носила назив *психолошко-пропагандно деловање* (ППД), а након тога била је позната под именом *психолошке операције* (PSYOP). Циљ поменуте делатности и термина који је денотирају је, током историје, суштински остао исти − утицај на промену ставова и понашања противника, пријатеља и неутралне јавности на начин који одговара постизању националних, политичких и војних циљева организатора информационог ратовања. Основна специфичност информационог ратовања јесте да бојиште није физички, већ виртуелни свет, а потенцијални учесници на овом бојишту могу бити државни органи, обавештајне службе, војне организације, терористичке организације и други. Победник у информационом рату требало би да буде она страна која може брже да експлоатише информације, односно да их анализира, процењује ситуацију и на њу реагује. Осим тога, шанса за победу увећава се код оне стране која успе да противнику пласира убедљиве информације или дезинформације, на основу којих би противничко руководство требало да донесе погрешне закључке и лоше одлуке.

Постоје бројне дефиниције информационог ратовања. Према дефиницији Института за проучавање информационог рата (Institute for Advanced Studies on Information Warfare), информациони рат представља „офанзивну и дефанзивну употребу информације и информационих система да би се искористиле, поткупиле, искварили и уништиле информације и системи информисања противничке стране, истовремено штитећи властите информације и системе“.[7] Према овом одређењу, вођење информационог рата заснива се на три принципа:

- сазнати;
- спречити другога да дође до сазнања;
- навести друге да дођу до неистинитог сазнања. У овом трећем аспекту реч је о дезинформацији и утицају на мишљење и ставове.

Са друге стране, „Intelco“, филијала Међународне асоцијације савета одбране (International Association of Defense Counsel – IADC), као видове информационог рата разликује:

- рат *за* информацију;
- рат *кроз* информацију (помоћу дезинформације);
- рат *против* информације.[8]

Према Арквили и Ронфелду, информационо ратовање обухвата: 1) настојање да се о противнику сазна све и спречавање противника да зна много о вама; 2) окретање „баланса информација и знања“ у сопствену корист, посебно ако не постоји баланс снаге; 3) коришћење знања тако да мањи капитал и рад могу бити проширени (увећани).[9]

---

[7] Greenberg, L., Goodman, S., Soo Hoo, K., *Information Warfare and International Law*, National Defense University, Washington DC, 1998.

[8] International Association of Defense Counsel, http://www.iadclaw.org/books.cfm

[9] Arquilla, J., Ronfeldt, D. „Cyberwar is Coming!“ RAND corporation, published in the Journal of Comparative Strategy Vol 12 No. 2 Summer 1993. pp.141–165.

Стеван Синковски наводи да је информационо ратовање могуће дефинисати и као облик конфликта којим се директно нападају информациони системи, а тиме и системи знања и убеђења противника.

Шлехер, амерички експерт за електронско ратовање, под информационим ратовањем подразумева:„акције предузете да би се остварила информациона супериорност, као подршка националној војној стратегији, утицајем на противничке информације и информационе системе, док се истовремено штите сопствене информације и информациони системи“.[10]

Радна дефиниција информационог ратовања Универзитета националне одбране (National Defense University)[11] САД је следећа: информационо ратовање је приступ оружаном конфликту којим се усмерава менаџмент и користе информације у свим облицима и на свим нивоима да би се остварила одлучујућа војна предност, посебно у интервидовском и комбинованом окружењу. Информационо ратовање је, по природи, и офанзивно и дефанзивно и *креће се од мера којима се противник спречава да експлоатише информације* до одговарајућих мера којима се обезбеђује интегритет, расположивост и интероперабилност пријатељских информационих ресурса. Мада је у крајњем случају војно по својој природи, информационо ратовање се води и у политичкој, економској и друштвеној сфери и применљиво је преко читавог скупа области националне безбедности од мира до рата и од „главе до пете“.[12]

Сматрамо да је најпотпунија и најприхватљивија дефиниција Ричарда Шафранског, према којој је „информационо ратовање активност уперена против било којег дела система знања и веровања противника. Без обзира на то да ли се води против спољњег противника или унутрашњих група, информационо ратовање има крајњи циљ да употреби информационо оружје да би променило (утицало, манипулисало, напало) системе знања и веровања неког спољњег противника.“[13]

Војни аспект информационог ратовања

У контексту америчке војне доктрине појам *информационо ратовање* сведен је и на оперативном нивоу означен као *информациона операција* (Information operation – IO). Информационе операције подразумевају предузимање потеза да би се деловало на непријатељске информације и информационе системе, док се у исто време штите сопствене информације и информациони системи. Информационе операције захтевају софистицирани развој, повезаност и ослањање на информационе технологије.

[10] Schleher, C., *Electronic Warfare in the information age*, Artech House, 1999.

[11] *National Defense University* је највиша војно-политичка школа САД и њени слушаоци су, поред официра и високих службеника администрације САД, и официри других земаља.

[12] Група аутора, *Информациони и математички модели у процесима командовања*, Лабораторија за примењену математику, Београд, 1969.

[13] Col Richard Szafranski: „A Theory of Information Warfare“, Published Airpower Journal - Spring 1995; извор – интернет: http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm.; приступљено 16. јануара 2011. године.

Примарни циљ информационих операција је противничко руководство (политичко, војно, социјално, културно), као и процес доношења одлука противничког руководства. Међу остале, не мање значајне мете напада могу се подвести: војна инфраструктура, цивилне инфраструктуре (телекомуникације, транспорт, енергетски систем, финансијски систем, производни систем) и оружани системи (авијација, бродови, артиљерија, прецизно вођена муниција и ПВО системи).

Документ Министарства одбране САД из 2003. године дефинише информационе операције као заједничке активности електронског ратовања, компјутерских мрежних операција, психолошких операција, војног обмањивања и „заштите операција" ради утицаја, прекидања или наношења неисправности противничком „људском" или аутоматизованом систему за руковођење. Према томе, америчка војна теорија идентификује пет централних координираних активности (способности), када говори о садржају информационих операција.

Руски приступ информационим операцијама и класификацији активности које се подводе под овај појам разликује се у односу на амерички приступ. Информационо ратовање, из руског угла, реализује се у периоду мира, фази припреме за рат и током самог вођења рата, и то на три нивоа: 1) на стратегијском нивоу (државни ниво који укључује ангажовање различитих министарстава и агенција у операцијама на два фронта или више њих), 2) оперативном нивоу (изводи се на армијском и корпусном нивоу), и 3) на тактичком нивоу (ниво који изводе комбиноване јединице и њихови састави).[14]

У време мира, информационо ратовање односи се на информациону безбедност друштва и државних институција и укључује широки спектар активности које имају везе са заштитом државе.[15] Информационо ратовање у миру води се и тајним средствима, уз помоћ обавештајне делатности, политике и психолошких операција. У време рата информационо ратовање доводи се у везу са намером да се постигне информациона супериорност над непријатељем, да се оствари и одржи информациона предност, али исто тако и да се заштите сопствене информације и информациони системи.[16] Информационо ратовање током оружаног сукоба много је отвореније него у време мира и може да подржи традиционалне форме ратовања, укључујући и обавештајне активности. Оне обухватају физичко уништавање војних информационих система, електронске контрамере, специјално програмиране хардвере и софтвере (вируси, тројанци и логичке бомбе), „извртање" информација, обмањивање и манипулације информацијама, укључујући и психолошке операције.

У руским оружаним снагама, информационо ратовање обухвата електронско ратовање, психолошке операције, обавештајни рад, обмањивање и примену математичких програма.[17] Важно је нагласити да наведена дефиниција не помиње експлицитно компјутерско-мрежне операције (CNO), али израз „примена математичких програма" вероватно укључује примену офанзивних и дефанзивних способности за ком-

[14] Limno, A. N., Krysanov, M. F., „Information Warfare and Camouflage, Concealment and Deception", *Military Thought*, vol. 12, no. 2, 2003.

[15] Pirumov, V. (1996) 'Nekotorye aspekty informatsionnoi voiny' (Certain aspects of information warfare). Conference speech in Brussels in May 1996, наведено у R Heickerö, ''Emerging Cyber Threats and Russian Views on Information warfare and Information operations'', 2010.

[16] *Ibid*.

[17] *Ibid*.

пјутерску и мрежну експлоатацију, напад и одбрану. Може се закључити да већина руских експерата, као и званична документа, наводе да су кибер операције, заједно са електронским ратовањем, обавештајним и контраобавештајним радом, обмањивањем, дезинформисањем, психолошким операцијама и уништавањем противничких компјутерских способности – основни елементи информационих операција.

Када је у питању кинеска војна теорија, изнећемо ставове водећег кинеског стручњака за информационо ратовање, генерала Dai Qingmina. Он је током 2002. године, у престижном листу *Кинеска војна наука,* изнео шест форми информационог ратовања које развија Народноослободилачка армија Кине (НОАК): оперативна безбедност, обмана, компјутерско-мрежни напади, електронско ратовање, обавештајни рад и физичка деструкција.[18]

Из наведених америчких, руских и кинеских дефиниција може се закључити да компјутерско-мрежне операције представљају интегрални и најмодернији вид информационих операција.

У савременом добу, активностима информационих операција придодате су, прво, активности електронског ратовања (EW), а онда и компјутерско-мрежне операције, које су замениле физичко уништење као елеменат информационих операција. До енормног повећања могућности за вођење информационог рата, односно увођења компјутерско-мрежних операција, како у сфери војних активности, тако и у сферама економије, политике и културе, дошло је са настанком кибер простора или, прецизније речено, појавом интернета. Иако представља откриће америчких војних стручњака, интернет је увелико превазишао своју војну функцију. Данас је постао поприште *par excellence* на којем се слободно може водити информациони рат. Као и физички простор, и кибер простор припада ономе ко га се најпре домогне. Било која стратегија за успостављање контроле над интернетом, једним од главних попришта информационог рата, морала би, као императив, да усвоји следеће максиме: загосподарити каналима за проток информације, што је могуће више емитовати властите погледе и ставове да би се што ефикасније наметнули и без престанка усавршавале методе и средства за обраду информације.

У складу са развојем интернета и информационо-комуникационе технологије, компјутерско-мрежне операције су једне од најсавременијих и најмодернијих способности развијених за потребе подршке војних операција. Значај тих операција порастао је са наглим порастом коришћења умрежених компјутерских система и телекомуникационе инфраструктуре од стране војних и цивилних структура и организација. Компјутерско-мрежне операције, заједно са електронским ратовањем, користе се за напад, ометање, прекид и уништење противничких информационих и компјутерских система. У војним операцијама, компјутерско-мрежне операције деле се на нападне (CAN) и одбрамбене (CND) и повезане компјутерске операције за експлоатацију (CNE). Компјутерске операције за експлоатацију омогућавају обавештајно прикупљање података преко компјутерских мрежа и из противничких база података.

Компјутерсконападне операције су врста операција офанзивне намене, у којима се акције спроводе коришћењем компјутерске мреже ради стварања поремећаја, одбијања, деградирања, манипулисања или уништавања информација које су сме-

[18] Dai, Qingmin, „On Integrating Network Warfare and Electronic Warfare," *China Military Science*, Feb 2002, pp 112–117.

штене у противничком информационом систему или компјутерској мрежи. Основни циљ напада не мора да буде противнички информативни систем, већ и подршка некој широј операцији, као што су информационе операције за подршку противтерористичкој борби или мењање и фалсификовање специфичних комуникација.[19] Компјутерсконападне операције тежишно се фокусирају на поверљивост, интегритет и доступност информација.

Према Столингсу (Stallings), компјутерско-мрежне нападне операције могу се класификовати на основу процеса који се примењују при нападу. То су:

1. прекидање – ресурси система су уништени или недоступни корисницима;
2. пресретање – неовлашћено лице приступа ресурсима система;
3. модификација − неовлашћено лице не само да приступа ресурсима система већ и мења садржај података у њима, и
4. фабрикација – неовлашћено лице уноси фалсификоване објекте у систем.

Пресретање представља пасиван напад, док су остала три процеса активни напади.

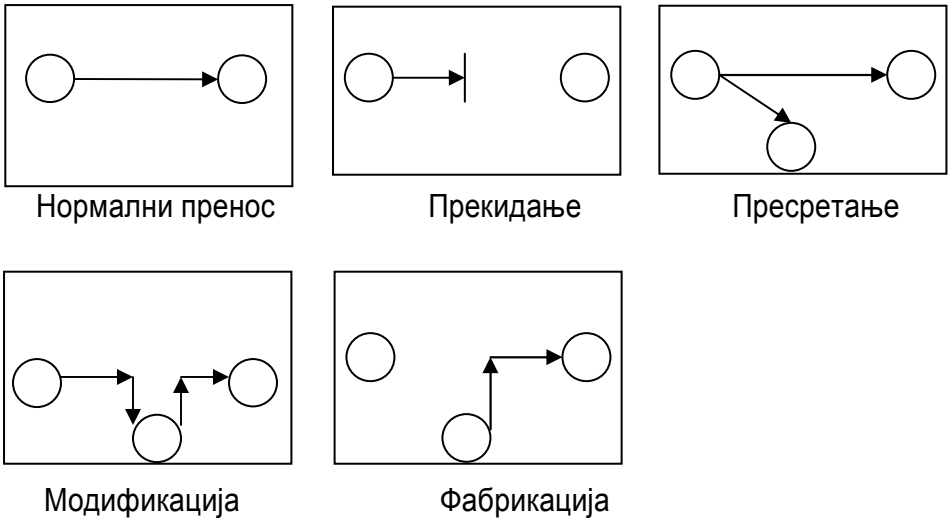

Схема 3 – *Класификација напада на рачунарске системе по Столингсу*

Класификација компјутерско-мрежних нападних операција може се извршити и на основу ефеката напада као критеријума деобе.[20] У том смислу, могу се издвојити четири основне врсте компјутерско-мрежних нападних операција:

[19] J. Cartwright, Vice Chairman of the Joint Chiefs of Staff, Cyberspace Operations Lexicon, 2010. Retrieved at http://www.nsci-va.org/CyberReferenceLib/201011 Joint%20Terminology%20for%20Cyberspace%20Operations.pdf

[20] Bayles, William J., *The Ethics of Computer Network Attack*, http://www.totse.com/en/hack/legalities_of_hacking/excerpt4.html

1. Операције одбијања (Deny). Главна намена операција одбијања јесте спречавање приступа информацијама. Ове операције јављају се у различитим формама. Једна од најосновнијих форми је опструкција услуга (Denial-of-Service − DoS), која се фокусира на одбијање доступности информација за одређено време ауторизованим корисницима.

2. Операције прекидања (Disrupt). Ова врста напада фокусирана је на стварање поремећаја, на такав начин да нападачи могу тајно да репрограмирају компјутерски систем противника и тако поремете процес контроле у неком систему или институцији. На пример, то може бити прекидање снабдевања електричном енергијом применом операција којима се репрограмирају компјутери који контролишу дистрибуцију електричне енергије.[21]

3. Операције деградирања (Degrade). Намена ових операција је умањивање протока информација код противника, као и да се противник натера да користи мање ефикасна комуникациона средства, што треба да успорити његов процес правилног одлучивања и доношења одлука.[22] Овај процес је сличан борбеним операцијама на копну, у којима се користе разни природни и вештачки предмети као препреке ради ометања и успоравања напредовања противничких копнених снага. Напад ради деградирања доводи до тога да се информације противника каналишу кроз рањивије канале за проток и достављање информација. Овакву ситуацију, тј. „каналисање" противничких информација може да користи савезничка страна да усмерава или води противника у жељеном правцу када су у питању предстојећа борбена дејства.

4. Операције уништавања (Destroy). Кинетичка муниција може да буде коришћена за уништавање компјутерских система противника. Будући да ова муниција представља конвенционално средство, такве операције се не могу подвести под компјутерско-мрежне нападне операције. Уместо тога, компјутерско-мрежне нападне операције уништавања подразумевају коришћење вируса и/или неких других малициозних програма за уништавање компјутерских мрежа, софтверских програма и хардверских компоненти.

Економски, културни и политички аспект

Једна од најраспрострањенијих врста информационог ратовања, коју је у својој класификацији дао Швартау (Schwartau), јесте тзв. корпорацијско информационо ратовање.[23] Велике привредне корпорације користе интернет да би се обавестиле о пословним кретањима, али, исто тако, и да би дезинформисале своје конкуренте. У конкурентским секторима прикупљање података и избор тражених профила противника од изузетног су значаја. Кибер простор представља један неисцрпан и свима доступан извор за такве активности. С обзиром на то да ће у скорој будућности

[21] *Ibid.*

[22] *Ibid*.

[23] Осим корпорацијског, поменута класификација садржи још персонално и глобално информационо ратовање. Према: Петровић, С., *Компјутерски криминал*, МУП Србије, Београд, 2001, стр. 337.

све врсте знања постати стратешка тајна, може се, према Петровићу, очекивати драстичан пораст ове врсте ратовања.

Из доступне литературе може се утврдити да је до сада на интернету покренут велики број програмираних кампања ширења дезинформација, економског карактера, чији је циљ био опањкавање противника. Такве акције дезинформисања представљају утолико мањи ризик за покретача што он, генерално посматрано, не учествује директно у акцији, већ, најчешће, преко неке од приватних агенција специјализованих за пружање овакве врсте услуга. Развој информационе технологије и жестина у суочавању са конкурентима доводе до умножавања активности ове врсте, до стварања правог тржишта дезинформација.

Сваки корисник глобалне информационе мреже може постати жртва различитих техника информационог рата. Чест је случај да особа која се обавештава преко интернета верује да су обавештења која прима објективна. Напротив, велики број обавештења је тенденциозно пристрастан, национално, религиозно, политички, социјално или професионално обојен. Интернет се мање ослања на квалитет информације, а више на могућност да искристалише распрострањена мишљења. Тако се, уз помоћ глобалне рачунарске мреже, формирају „заједнице веровања“, које карактерише некритичко прихватање онога што се нуди у информационом галиматијасу – прихватање дела истине подметнутог као целина.

Отворени политички маневар дезинформисања у кибер простору, на пример, покренуо је запатистички покрет у Мексику, 11. фебруара 1995. године. Овај покрет је успео да „мобилише штампу у САД, а преко ње и међународно јавно мњење тако што је, на Интернету, лансирао апел са захтевом за помоћ у супротстављању офанзиви мексичке владе, откривајући наводне покоље у селима у зони Морелија-Гамача. Новинари, који су неколико дана касније, као и обично, дотрчали на лице места, могли су констатовати само да нема никаквих покоља, да се ништа заправо није догодило. Ипак, ефект је био постигнут, било каква акција мексичке армије у тој зони постала је немогућа, јер је све било под будним очима јавности. Штавише, популарност мајора Маркоса није престајала да се даље шири и расте брижљиво развијеном психолошком акцијом у којој су веома широко коришћене могућности Интернета“.[24]

Могућности дезинформисања путем кибернетике технички су неограничене, посебно помоћу слике и звука. Такве могућности се у огромној мери већ користе у области рекламе. Својеврсну дезинформацију спроводе и развијене државе света, које промовишу властите вредности и властити стил потрошње, две области које су у међувремену постале нераскидиво повезане и измешане. Оне то чине из економских, али и политичких побуда. Идеја је једноставна – промовисањем властитих вредности извозе и властити стил потрошње, чиме повећавају продају својих производа.

Повезивање вредносног система и производа објашњава перманентно инсистирање САД на извозу америчког начина живљења у све друге делове света. Да парафразирамо Волкова – можда не постоји директна узрочно-последична веза између светског поретка и потрошње кока-коле, али је сигурно да превласт информа-

[24] Волков, В., *op. cit.*, стр. 211.

ције отвара могућност за остваривање значајних профита. Средства којима се, при том, служе транснационалне компаније под покровитељством матичних држава по дефиницији су заобилазна, посредна, будући да нико нема осећај да се потчињава Америци тиме што једе у ресторану „Мекдоналдс".

Злоупотреба кибер простора за подршку тероризму

Недостатак правила и граница, могућност достизања широког медијског ефекта, брза размена информација и готово апсолутна гаранција анонимности карактеристике су кибер простора које га чине идеалним пољем за прикривене организације и покрете. Кибер простор је за терористичке организације постао једна врста виртуелне оперативне базе коју је немогуће опколити и неутрализовати. Практично су све светске терористичке организације било које политичке или религиозне оријентације показале да имају жељу и способност да искористе карактеристике кибер простора, колико год то звучало парадоксално, у односу на групе које се традиционално сматрају антимодернистичким.

Према подацима Стејт дипартмента, 1998. године 15 од 30 организација које су САД прогласиле терористичким имало је своје *web*-сајтове, а од 2000. године све оне су присутне на светској комуникационој мрежи. Вајман (Weimann) констатује да готово све активне терористичке организације, њих преко четрдесет, имају по један или више интернет-сајтова, и то, углавном, доступних на неколико језика.[25] Организације из свих делова света заступљене су на интернету. Ипак, и само присуство на мрежи говори да су многе од њих, како тврди Вајман, не само транснационално, већ и трансрегионално усмерене и профилисане. Овај аутор класификује терористичке организације присутне на мрежи по једноставном, географском критеријуму поделе:

• Блиски исток: Хамас, Хезболах, ПЛО, Фатах танзим, Палестински исламски џихад, покрет „Кахан живи", Курдистанска радничка партија, Ирански муџахедини (PMOI), Партија народног демократског ослободилачког фронта и Велики источни фронт исламских одметника (IBDA-C);

• Европа: ETA, ИРА и Корзиканска армија;

• Латинска Америка: Тупак амару, Сендеро луминозо (Перу); FARC и Колумбијска национална ослободилачка партија (Колумбија);

• Азија: Ал каида, Хизб-ул муџахедини Кашмира, Ансар ал ислам, Јапанска црвена армија, LTTE, Исламски покрет Узбекистана, Исламски ослободилачки фронт Моро (Филипини), Јапанска супериорна истина (Aum Shinrikyo), Laskhar-e-Taiba (Пакистан) и чеченски побуњенички покрет.

Набројане организације користе интернет веома активно и имају, углавном, по неколико сајтова које контролишу и уређују.

[25] Weimann, G., *How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report, New York, p. 3, http://www.usip.org/pubs/specialreports/sr116.pdf

Табела 1 – *Преглед интернет-адреса појединих терористичких организација*

Хамас	http://www.hamas. org http://www.palestine-info. net/hamas/index. html http://www.qassam. org/ http://www.palestine-info. com/index_e. htm
Хезболах	http://www.Hizbollah. org http://www.moqawama. org http://www.moqawama. tv/ http://www.almanar. com. lb/
Aum Shinrikyo	http://Aum-internet. org/ http://Aum-shinrikyo. com/english/ http://info. aleph. to/index_en. html
Тамилски тигрови	http://www.eelam. com/ http://www.eelamweb. com/
FARC	http://www.contrast. org/mirrors/farc/ingles. htm http://www.farc-ep. org/pagina_ingles/
ИРА	http://www.utexas. edu/students/iig/archive/ira/history/irahist. html. http://www.sinnfein. org/
Курдистанска радничка партија	http://www.pkk. org/
Исламски покрет Узбекистана	http://www.ummah. net/uzbekistan/
Палестински исламски џихад	http://www.jihadislami. com/
„Ал каида“	http://www.alneda. com http://www.jihadunspun. net http://www.aloswa. org http://www.drasat. com http://www.jehad. net http://www.islammemo. com http://www.qassam. net http://www.assam. com

(Извор: Weimann, G., *How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report, New York, p. 11, http://www.usip. org/pubs/specialreports/sr116.pdf)

И овај сумарни преглед интернет-страница које служе ширењу терористичке идеологије, сматрамо, довољан је да прикаже њихову распрострањеност на мрежи и могућности за одашиљање жељених порука у свет. На мрежи су, дакле, присутне све најзначајније светске терористичке организације, како оне глобалног, трансрегионалног типа, тако и оне са уским, етничко-сепаратистичким или левичарским, револуционарним циљевима. Речју, терористичка идеологија је „преплавила“ интернет, који је, очигледно, због свих погодности које пружа, постао водеће медијско средство терориста. Поменуте терористичке организације, путем мрежних сајтова, износе јавне прогласе, претње или врше психолошке притиске на противнике, врбују и индоктринирају нове чланове и одржавају везе са географски удаљеним ћелијама или члановима.

Употреба интернета за терористичку пропаганду и психолошки рат

Пре појаве интернета могућности терориста за привлачење пажње широке јавности биле су уско повезане са добијањем визибилитета путем традиционалних медија (телевизија, радио, новине, итд.). Представа коју поменути медији пружају аудиторијуму, међутим, увек има негативну конотацију за терористе. Став јавности према терористичкој активности формира се под утицајем приказаних трагичних слика или информација пуштених у етар, које успут бивају филтриране, промењене или чак цензурисане према избору уредника средстава информисања.[26]

Комуникација путем кибер простора, пак, омогућава слање нецензурисаних информација (чији садржај може бити намењен одређеној циљној групи), без обзира на то да ли је реч о пласирању истинитих или неистинитих информација. Ову погодност користе субверзивне друштвене групе ради изграђивања одређеног имиџа у јавности и пред противницима. Са могућностима мултимедијалне комуникације, интернет функционише у исто време и као радио-станица, телевизија и новине, омогућавајући доступност информација свуда у свету, са незнатним логистичким трошковима и без могућности да националне владе врше цензуру. Није случајност да се, на пример, политичка расправа у Саудијској Арабији и земљама Залива, половином деведесетих година прошлог века, постепено преместила са традиционалних медија (који су у овом региону изложени оштрој контроли држава) у кибер простор.[27]

Путем кибер простора терористи, у основи, теже да допру до три различита аудиторијума:

1) постојећих и потенцијалних бораца и подржавалаца;

2) међународног јавног мњења, које није директно умешано у конфликт и упознато са разлозима терористичких активности, али које може бити заинтересовано за кључна питања конфликта;

3) непријатељске, тј. противничке јавности.

У ове сврхе првенствено се користе *web*-сајтови.[28] Сајтови терористичких организација обично су подељени у секције у којима су представљени разноврсни садржаји: историјат организације, политичко-социјалне идеје и идеолошки и политички циљеви организације, најзначајније иницијативе и спроведене акције, као и биографије лидера организације, оснивача и заслужних чланова, тј. „хероја“. Често је у структури сајта присутна и „информативна секција“, у којој се посетиоци могу упознати са актуелним вестима и прочитати политичке коментаре уредника.

Ради допирања до широке међународне јавности, многи сајтови нуде могућност приказа интегралног текста на више светских језика. Интересантно је поменути да се текстуални садржај на домицилном језику разликује од верзије намењене међународном аудиторијуму по томе што је, у другој верзији, изостављена насилничка реторика из оригинал-

[26] Putignano, D. S., *La criminalità informatica: cyberterrorismo*, Facoltà di Giurisprudenza, Università degli Studi di Bari, 2002, стр. 63.

[27] Eedle, P., „Al Qaeda takes fight for 'Hearts And Minds' to the web“, *Jane's Intelligence Review*, 2002, http://www.freerepublic.com

[28] Putignano, D. S., *op. cit.*, стр. 64.

не верзије. Иако се често употребљавају изрази „оружана борба“ и „отпор“, не емфатизују се и не помињу насилничке активности организације, иако је доста простора посвећено аргументисању моралне исправности и легалности коришћења насиља.

Властита употреба насилних средстава представљена је као нужност, као једини инструмент који стоји на располагању слабијем у супротстављању моћном и потлачавајућем непријатељу. Али, непријатељево коришћење насилних средстава, дакле, оружани одговор на терористичку активност, дефинише се терминима „масакр“, „убиство“ и „геноцид“. Терористичка организација описује се као константно надзирана, спутавана у својој тежњи да се слободно изрази, док су њени лидери у сталној животној опасности. Чланови организације приказани су као борци за слободу или за Бога (као у случају исламског џихада), принуђени да користе силу како би се одбранили од непријатеља који подјармљује права и понос групе или народа који претендују да заступају.

Ова врста комуникације, која настоји да евоцира слику слабе организације, принуђене на избеглиштво од немерљиво надмоћније силе, настоји да представи терористе као жртве и да пребаци одговорност за почињено насиље на противника. Додатно оснаживање овакве поруке постиже се реторичким коришћењем језика ненасиља и наводном расположеношћу за мирно решење сукоба дипломатским средствима. Постоје и изузеци, нарочито у погледу група и организација исламског џихада, које су обично одлучније да убеђивачком реториком утичу на јавност која их фаворизује, али и да непријатеља подвргну притиску.[29]

Последњих година евидентиран је велики пораст броја *web*-сајтова којима управљају исламске групе и симпатизери. Тешко је одредити тачан број, али се процењује да их има неколико стотина. Садржаји који су на њима заступљени обухватају теме од информативних до теолошких, уз реторику која промовише идеје „праведног рата“ и „мучеништва“. Сајтови који припадају признатим организацијама израђени су професионално и приказују фундаменталистичку верзију догађаја који се тичу Блиског истока и света уопште. Сајтови садрже чланке и коментаре идеолошких лидера, а прате их фотографије западњачких злодела. Поједини сајтови нуде детаљне описе насилних акција, а на почетној страници приказују, видно истакнут, електронски бројач палих бораца („мученика“), погинулих непријатеља, као и колаборациониста. Најчешће се користи арапски језик, мада многи сајтови укључују и секције на енглеском језику, унутар којих се разматрају филозофска и теолошка питања, ради преобраћања посетилаца у ислам.

Можемо констатовати да тероризам, у својој суштини, садржи елементе психолошког рата.[30] Савремени терористи су, за разлику од „традиционалних“, у стању да користе технолошка достигнућа трећег миленијума ради успешног вођења својих активности. Интернет, као средство комуникације које је тешко цензурисати и којим се могу ширити мултимедијални садржаји независно од њихове веродостојности, терористи користе као психолошко оружје у кампањама психолошког рата ради увећања властите моћи и ефеката спроведених дејстава.

---

[29] Piccitto, D., *Terrorismo: dal fondamentalismo religioso ad Internet*, Facoltà di lettere e filosofia, Facoltà di Scienze Politiche, Università degli Studi di Perugia, 2005, стр. 140.

[30] Према дефиницији Министарства одбране САД, психолошки рат (*psychological warfare*) јесте планирано коришћење пропаганде и осталих психолошких операција са циљем да се утиче на мишљење, емоције, понашање и деловање страних противничких група, у функцији достизања националних циљева.

Међу различитим начинима за спровођење психолошких операција најчешћи су коришћење дезинформација[31] или претњи, ради ширења осећања страха, немоћи или безнађа. Случај ликвидације америчког држављанина Николаса Берга (Nicholas Berg)[32] један је од препознатљивих примера такве праксе. Видео-снимак обезглављивања америчког грађанина прво се појавио у кибер простору, на *web*-сајту „Muntada al Ansar"-а, чије је седиште било у Малезији.[33] Пре него што је сајт укинут, снимак погубљења преузела је телевизија „Ал џазира" и јавно га емитовала. У финалним сценама снимка који носи наслов *„Абу Мусаб ал-Заркави*[34] *приказан док маскира америчког војника"* могао се видети један од пет терориста како чита следећи текст: „Мајкама и супругама америчких војника поручујемо да смо понудили да разменимо овог таоца са заробљеницима Abu Ghraib-а[35] и да је Бушова администрација то одбила...", „Част људи и жена затвора Abu Ghraib не може се наплатити крвљу".[36]

„Ал каида" обједињава мултимедијалну пропаганду са напредним комуникационим технологијама ради организовања софистицираног психолошког рата. Без обзира на бројне ударе које је претрпела након 11. септембра 2001. године и растурање њених оперативних база у Авганистану и Далеком истоку, организација је и даље у стању да води импресивну психолошку кампању преко својих *web*-сајтова. Са ових сајтова она стално упућује претње новим нападима на америчке циљеве. Велика пажња коју медији посвећују овим претњама доприноси порасту осећања страха и несигурности не само у Америци, већ и широм света.

И уништење Светског трговинског центра „Ал каида" је пропратила честим слањем порука са својих *web*-сајтова и тако проузроковала не само психолошку већ и конкретну штету америчкој економији. У прилог наведеној тврдњи говори и слабљење долара, пад берзанског тржишта и губитак поверења Американаца и света у америчку економи-

[31] Термин *дезинформација*, у контексту шпијунаже, војних обавештајних служби и пропаганде, означава намерно ширење лажних информација ради обмане противника у вези са сопственом позицијом или акцијом. Док пропаганда има за циљ утицање на емоционалну димензију личности, дезинформација манипулише на рационалном нивоу.

[32] Америчког бизнисмена Николаса Берга заробила је, и пред видео-камером убила, терористичка група повезана са „Ал каидом" у Ираку, маја 2004. године. Његово убиство осудиле су многе исламске вође, наводећи да је противно исламу и штетно за муслиманску ситуацију.

[33] Сајт „Muntada al Ansar"-а словио је за центар разврставања порука „Ал каиде" и осталих исламских терористичких група. Адреса сајта била је: http://www.al-ansar.biz/

[34] Абу Мусаб ал-Заркави (Abu Musab al-Zarqawi, 20. 10. 1966–7. 6. 2006) био је вехабијски милитант, родом из Јордана, командант ирачких герилаца и вођа „Ал каиде" у Ираку. Заркави је преузео одговорност за низ терористичких напада, укључујући бомбашке нападе на цивиле, као и одрубљивање главе заробљеном америчком таоцу Николасу Бергу. Абу Мусаб ал-Заркави се сматра одговорним за ширење секташког насиља у Ираку, односно коришћење бомбаша-самоубица против шиитских цивила у Ираку у настојању да се изазове одмазда према сунитима, односно грађански рат, и тако потпуно дестабилизује проамеричка влада у Ираку. Ал-Заркави је последњих година стекао репутацију најтраженијег терористе на свету, засенивши чак и Осаму Бин Ладена. Америчка влада је његову главу уценила на 25 милиона долара. Пре тога је у Јордану био у одсуству осуђен на смрт. Према наводима команданта америчких снага у Ираку, Ал-Заркави је погинуо у ваздушном нападу у близини Багдада 2006. године. Према: BBCSerbian.com, http://www.bbc.co.uk/serbian/news/2006/06/060608_zarqawi_gallery.shtml.

[35] Затвор у близини Багдада у којем су припадници америчке војске подвргавали мучењу и малтретирању ирачке ратне заробљенике.

[36] Weimann, G., *Terror Groups Exploit Internet for Communications, Recruiting, Training*, JINSA Policy Forum, http://www.jinsa.org

ју. У једној од порука које су се појавиле на интернету, Бин Ладен је изјавио: „Америка се повлачи […] мучење њене економије се наставља, али су неопходни даљи ударци. Млади морају да пронађу нове чворове америчке економије и да их погоде“.[37]

Психолошки рат који воде исламске терористичке организације често је усмерен и на одређене групе унутар самог исламског света. На пример, одмах после напада 11. септембра неколицина арапских и египатских радикалних исламиста који су критиковали „Ал каиду“ описани су, на сајту alneda. com, као хипокрити. Реакција терористичке организације била је још жешћа када је једна група од 150 академаца и стручњака из Саудијске Арабије објавила манифест под насловом: „Како можемо коегзистирати“ (*How we can coexist*), у којем је тврдила да ислам и Запад деле одређене универзалне вредности. Путем својих *web*-сајтова (alneda. com и drasat. com) „Ал каида“ је одговорила да ислам и Запад не деле ниједну вредност, да не постоји сличност између два света, да је ислам супериоран и да ништа није супериорно у односу на њега: „Чак је и муслиман који је роб бољи од милион неверничких џентлмена...“ „Муслимани имају дужност да ислам шире сабљом.“ Тврдња Манифеста постала је предмет једне фатве,[38] којој је била посвећена посебна секција сајта alneda. com. Притисак који су вршили чланци и фатва био је толико јак да су одређени учесници у писању чланка били приморани да повуку претходне изјаве. Циљ идеолошке кампање тиме је у потпуности постигнут.[39]

Мобилисање и обука потенцијалних терориста преко интернета

Пропагандна активност се, добрим делом, спроводи ради привлачења пажње оних који имају заједничке интересе са терористичком организацијом или, пак, сличан систем вредности. Пошто је пропагандом привучена пажња симпатизера, у следећем кораку им се додељују једноставнији задаци (активности) унутар организације, као и неопходни инструменти за почетну обуку, нарочито у околностима када није могуће користити праве кампове за обуку.

Web-сајтови и форуми[40] користе се за размену информација и контаката приликом пријављивања у јединицу, као и за дистрибуцију видео-снимака који приказују разне фазе обуке и борилачке сцене из актуелних или минулих сукоба. Такође, на *web*-сајтовима је усвојена и пракса објављивања биографија или интервјуа са познатим муџахединима. Материјал презентован на терористичким сајтовима, осим што делује мотивишуће на нове чланове, има циљ да докаже континуитет борбе (као у случају чеченских

[37] Bergen, P. L., *Holy War, Inc. Inside the secret world of Osama bin Laden*, The Free Press, New York, 2002, p. 253.

[38] *Фатва* (арапски: فتـــوى) значи *саветовање*, које се врши са експертом за исламско право – шаријy. То су, углавном, муфтије. Код шиитâ фатву врше високи чланови верске хијерархије, нпр. ајатоласи. Саветовање може да потврди или оповргне правила која важе у животу појединца (законски стан, наследство) или у вери (канонско право). Фатва спада у подручје теологије и мора се позивати на одређену тачку шеријата. Код суснитâ фатва има знатно мању тежину него код шиитâ – схвата се као мишљење и није пресудна.

[39] Eedle, P., 2002, *op. cit*.

[40] Интернет-форум (енгл. *Message board*) јесте апликација која регистрованим корисницима неког *web*-сајта омогућава онлајн дискусију путем порука (*post*) објављених на сајту. Одређени чланови форума могу бити модератори сајта, са правом да бришу поруке или прекину писање о темама које нису у складу са правилником сајта.

сепаратистичких напада против руских војних снага) – борба се наставља упркос контролисаним информацијама које пласирају медији противничких држава.

Жене и деца су, често, циљна група у информационим кампањама. Мајкама се сугеришу различити начини на које могу васпитавати своју децу да би их припремиле за борачку будућност и на тај начин допринеле џихаду.[41] Међу потенцијалним члановима нарочито се траже они који припадају одређеном културном кругу и који имају специфична техничка и научна знања. Није реткост да се, нарочито на високим оперативним нивоима армије џихада, налазе солидни стручњаци, са потврђеним информатичким способностима. Међу протагонистима значајнијих терористичких атентата из деведесетих година налазе се биолози, хемичари, инжењери, физичари и информатички експерти. Доказано је да је Осама Бин Ладен лично регрутовао еминентне специјалисте у подручју медицине, инжењерства, хемије, физике, информатике и телекомуникација.[42]

Основна средства обуке путем интернета јесу практични приручници са упутствима за израду бомби и експлозива, хемијских реагенаса и отрова или пак инструкцијама за извршење киднаповања или егзекуције на разне начине. Они сегменти приручника који се односе на кибер простор елаборирају технике шифровања информација и електронских порука како их противничке обавештајне службе не би пресретале. На великом броју сајтова могу се пронаћи публикације попут *Терористичког приручника* (*The terrorist's handbook*) и *Кувара за анархисте* (*The anarchist cookbook*), које садрже детаљне инструкције о томе како извести нападе различитим експлозивним средствима. На мрежи је, такође, могуће набавити такозвану *Енциклопедију џихада*[43] која представља, у исто време, комплетан приручник за терористе и политичко-религиозни манифест „Ал каиде".

Још једна онлајн публикација „Ал каиде" јесте *Сабља* (*Al Battar*). Десето издање, које је изашло у мају 2004. године, било је посвећено отмицама са фокусом на методе, потенцијалне жртве и тактике преговарања, а садржало је чак и упутства за снимање одсецања главе киднапованих и објављивање снимка на интернету. Ова публикација објављена је нешто пре случајева отмица и убистава талаца у Ираку.[44] Сматра се да су онлајн приручници нарочито добили на значају након уништења талибанских кампова за обуку „Ал каиде" у Авганистану.

---

[41] Scalese, A., *La sicurezza del cyberspazio: analisi e considerazioni*, Facoltà di Scienze Politiche, Università degli Studi di Trieste, 2005, p. 64.

[42] Hudson, R., *The sociology and psychology of terrorism: who becomes a terrorist and why?*, http://www.fas.org

[43] *Енциклопедија џихада* откривена је 1988. године у претресу који је извршила манчестерска полиција. Има хиљаду страница, подељених у једанаест књига. Енциклопедија, поред осталог, садржи детаљна упутства за израду и постављање експлозивних направа, пружање прве помоћи, коришћење свих врста ватреног оружја, начине комуникације унутар разних муџахединских група, принципе и смернице за извођење класичних герилских, али и биотерористичких операција. Међу бројним стратегијама налази се и она за регрутовање младих муџахедина, будућих „спавача", унутар држава које су потенцијалне мете. Спавачи су у стању да изврше напад и након десет година од регрутовања, на циљеве који су изабрани и по симболичком и психолошком значају, као и на основу практичног ефекта који би изазвало њихово уништење. Међу циљевима предложеним у *Енциклопедији* налазе се: Кип слободе у Њујорку, Ајфелов торањ, нуклеарне централе, аеродроми, луке, небодери-симболи (тринаест година након откривања *Енциклопедије* обистинио се напад на Куле близнакиње), зоне са високом концентрацијом људи, итд.

[44] Northeast Intelligence Network – Terrorism News, Information and Analysis: *Kidnapping & Hostage Taking* (from *Al Battar*, Issue 10), http://www.homelandsecurityus.com

Финансирање терористичких организација и међусобна комуникација

Као и многе друге политичке организације, терористичке групе користе интернет за сакупљање новчаних фондова. Најчешће коришћени метод финансирања састоји се од каналисања фондова који произлазе из легалних (донације и привредне активности, на пример) или нелегалних активности (преваре помоћу кредитних картица, трговине дрогом и дијамантима), најчешће уз посредовање легитимних хуманитарних организација.[45]

Донације, осим оних спонтаних, траже се и од потенцијалних подржавалаца препознатих на основу личних информација унетих у онлајн упитнике и електронске поруџбенице, које терористи са пажњом сакупљају и анализирају. Захтеве за донацију најчешће шаљу електронском поштом признате хуманитарне организације, које немају директне везе са терористима. Еклатантан пример злоупотребе интернета за сакупљање фондова јесте случај америчке хуманитарне организације „Benevolence International Foundation Inc. – BIF", са седиштем у Чикагу. Сајт чеченских терориста qoqaz. net (није више активан) током 2000. године позивао је симпатизере да изврше онлајн донације двема хуманитарним организацијама, од којих је једна била BIF. Између јануара и априла 2000. године BIF је прикупила и преместила око 700.000 долара на банковне рачуне повезане са чеченским сепаратистима у Грузији, Азербејџану, Русији и Литванији.[46] Деветнаестог марта 2002. године откривена је и улога ове организације у опремању и обуци терориста у Босни и Херцеговини.[47]

Информационе технологије и интернет, дакле, омогућавају терористичким групама лако и брзо прикупљање и преусмеравање финансија. Тешкоће које постоје у контроли новчаних токова и непостојање одговарајуће стратегије супротстављања доводи експерте за област тероризма до закључка да ће се овај феномен у будућности ширити.

Интернет и, уопште, информационо-комуникационе технологије постале су терористима неопходне и за остваривање и одржавање међусобне комуникације. Изузетно брз проток информација омогућава „раштканим" члановима терористичких организација готово тренутну комуникацију и координацију. Услуга коришћења глобалне комуникационе мреже јесте, притом, бесплатна, а различитост и количина информација које се њоме могу размени бесконачне су. Интернет повезује не само чланове једне организације, већ и елементе различитих организација.

Бројни терористички сајтови који промовишу идеју џихада представљају мрежу у мрежи којом се служе терористи из различитих земаља за размену не само идеја и савета, већ и практичних инструкција за стварање терористичких ћелија и извођење напада. Неке од терористичких организација заступљених у кибер простору имале су изражену улогу у координацији и промоцији „Ал каиде". Према извештају америчког Института за мир (*United States Institute of Peace*), assam. com био је задужен за подручје Авганистана и Палестине, qassam. net је био линкован на „Ал каиду" и на „Хамас", 7hj.7hj. com је подучавао посетиоце како да хакују владине *web-*

[45] *How is Al Qaeda funded?*, Council on Foreign Relations, http://www.terrorismanswers.org

[46] *Islamic Charity Indicted*, http://www.cbsnews.com, http://news.findlaw.com

[47] http://www.rs-icty.org/PUBLIKACIJE/Paneli%20pdf%20srp/PANEL4srp.pdf

ресурсе, aloswa. org је објављивао цитате Бин Ладена, док је drasat. com нудио линкове на десетине сајтова који су објављивали саопштења „Ал каиде“.[48]

Још један разлог додатно утиче на опредељеност терориста за комуникацију путем интернета. У односу на традиционалне системе за јавну комуникацију (фиксни, мобилни или сателитски телефон), које је могуће прислушкивати, али и лоцирати комуниканте, интернет нуди серију инструмената који, ако се користе на прави начин, гарантују готово апсолутну конспиративност комуникације. У ову сврху користе се различити методи, али, за разлику од представа које у јавности стварају мас-медији жељни сензационализма, ретко се користе технолошки софистицирани начини, јер привлаче пажњу безбедносних служби.[49] Управо због тога, најчешће се преферира једноставност традиционалних, али ефикасних начина шифроване комуникације која се обавља разменом електронских порука између чланова исте ћелије.[50]

Порука размењена електронском поштом међу терористима који су 11. септембра отели авионе, како сматрају у америчком Институту за мир, означавала је мете напада. Последња инструкција Мохамеда Ате (Mohammed Atta) пред извршење терористичког акта гласила је: „Семестар почиње за три недеље. Добили смо деветнаест потврда за студирање на факултету права, факултету урбаног планирања, академији ликовних уметности и факултету машинства.“ Касно се увидело да се „деветнаест потврда“ односило на отмичаре, а поменута четири факултета на број циљаних авиона за извршење напада, тј. на четири мете.[51] Ова порука је пример како размена једноставно кодиране информације са јавног места и помоћу електронске поште (отмичари авиона имали су адресе *Hotmail*-а) може послужити сврси.

Један од напреднијих метода који искоришћава мултимедијалну природу интернета подразумева пласирање скривених порука у на први поглед неважне фајлове који садрже слике, музику или слично, техникама стеганографије.[52] Приступ интернету се, по правилу, обавља са јавних места (из интернет-кафеа, универзитетских мрежа, библиотека и других простора), чиме се постиже додатна гаранција анонимности. Комуникација између врха терористичке организације и ћелија изабраних за акцију може да поприми и облик манифеста објављеног на сајту.

Тако је, на пример, у децембру 2003. године на домену норвешког интернет-провајдера објављен документ на арапском језику. Проглас приписан „Ал каиди“, под насловом *Џихад у Ираку: наде и опасности*, износио је став да би терористички напади, изведени на територији земаља савезника Америке, њих изложили при-

[48] United States Institute of Peace, http://www.usip.org/pubs/specialreports/sr116.html

[49] Шифроване поруке које путују према серверу интернет провајдера сигурно су сумњивије од наизглед баналног текста обичне поруке који крије другачије значење, познато само примаоцу.

[50] На пример, чланови исте ћелије могу да користе само једно корисничко име и лозинку (тј. један кориснички налог) за приступ серверу електронске поште на *web*-у (као што су *Hotmail*, *Yahoo* или *Gmail*). На овај начин сваки од чланова може да пренесе поруку осталим члановима и без слања поруке електронске поште – једноставним меморисањем текста у одељак *drafts*. Будући да ниједна порука није путовала интернетом, у електронској архиви интернет провајдера не постоји траг о обављеној комуникацији.

[51] Thomas, T., “Al Qaeda and the Internet: The Danger of ’Cyberplanning’”, *Parameters*, 2003, Vol. 33.

[52] Термин *стеганографија* (грч. *stéganos* + *grafeîn* = скривено писање), у информатичком контексту, означава технике које се користе за сакривање тајних података у фајлове. Један од најчешће коришћених метода јесте прикривање тајних података у мање важним *bit*-овима неког фајла (фотографије, аудио или видео записа). Према: Џигурски, О., *Могућности заштите од стеганографије*, Зборник Факултета безбедности, Београд, 2008.

тиску, те би оне могле да повуку своје трупе из Ирака. Документ је нарочито упућивао на Шпанију, тј. њену унутрашњу предизборну политичку сцену, као најбољу мету. Три месеца касније, 11. марта 2004. године, напади „Ал каиде“ на четири воза у Мадриду проузроковали су смрт 191 особе. На неки начин, ови напади су условили резултат предстојећих избора. Победила је левица, која је у предизборној кампањи, као један од приоритета, заговарала повлачење војних снага из Ирака.[53]

Поједине терористичке организације користе се специфичним тактикама комуникације у кибер простору, заснованим на мигрирању својих сајтова. Сајт alneda.com, за који се верује да припада „Ал каиди“, забрањен је 2002. године пошто су интернет-провајдери у Малезији и САД открили да служи као огласник „Ал каиде“. Ипак, исти садржај се под различитим именима до данас појављује на интернету, користећи туђе сајтове. Рита Кац (Rita Katz), директор Института за потрагу за међународним терористичким ентитетима (SITE Institute), износи податак да су овакви феномени веома чести: „Није реч само о једном или два *web*-сајта, него о стотинама сајтова који су врло битни за 'Ал каидину' комуникацију“.[54]

Популарни описни назив за сајт који је кришом „угнежден“ на туђи сајт јесте „интернетски паразит“. Паразитски сајтови врло динамично мигрирају, мењајући форму. Сајт „Ал каиде“, на пример, „васкрсавао“ је чак на дневној бази у форми сајта, дискусионих форума (chat forum[s]), огласа (message board), итд. Метод инфилтрације у друге сајтове подразумева „разбијање“ шифре администратора и корисника, те коришћење слабости сервера да се заобиђу безбедносне мере.[55]

Обавештајна активност терориста

Интернет представља неисцрпан извор осетљивих информација, које су често битне за безбедност државе и становништва. У приручнику за обуку „Ал каиде“, откривеном у Авганистану, написано је да је коришћењем јавно доступних ресурса, без употребе нелегалних средстава, могуће прикупити бар 80% корисних информација о непријатељу.[56] То доказује да су терористи временом схватили важност такозваних отворених обавештајних извора. Ова врста обавештајне активности заснива се на прикупљању јавно доступних података из новина, часописа, књига, радијских и телевизијских емисија, телефонских именика, интернета, итд. Само путем интернета терористи имају слободан приступ пројектима, фотографијама, мапама и осталим кључ-

[53] *Qa'idat al-Jihad, Iraq, and Madrid – The First Tile in the Domino Effect?*, The International Policy Institute for Counter-Terrorism, http://www.ict.org.il/Articles/tabid/66/Articlsid/557/currentpage/15/Default.aspx

[54] SITE Institute, http://www.siteinstitute.org/

[55] Америчко-израелска организација *Internet Haganah* задужена је да прати кретање сајтова за које се мисли да припадају „Ал каиди“ и сличним организацијама. Према њиховим сазнањима, Alneda се током 2003. године појављивала „укопана“ унутар сајта једног четрнаестогодишњака, затим сајта компаније за безбедност софтвера, те страницама посвећеним режисеру хорор филмова Клајву Баркеру (Clive Barker) и холандске фирме за консалтинг *Educa.* Једна од скоријих локација на којој се налазио сајт била је регистрована у америчкој савезној држави Њу Џерси (www.conrado.net/_vit_inf/). Линк више није активан, а тренутна локација сајта „Ал каиде“ није позната. Према: Internet Haganah, http://internet-haganah.com/haganah/.

[56] Интервју Доналда Рамсфелда (Donald Rumsfeld), америчког секретара одбране, од 15. јануара 2003. Извор: Inside Defense, http://www.insidedefense.com.

ним подацима о потенцијалним циљевима. Често се са фотографија публикованих на интернету могу добити информације о примењеним мерама заштите на одређеном објекту. На пример, у заплењеном рачунару „Ал каиде“ пронађени су подаци „скинути“ са интернета о структурним и инжењерским карактеристикама једне хидроцентрале. Ови подаци су, помоћу програма за тродимензионалну симулацију, веома лако могли да буду употребљени за планирање акције са катастрофалним последицама.[57]

Терористима су у кибер простору на располагању многи инструменти који олакшавају прикупљање релевантних података: интернет-претраживачи, листе дистрибуираних порука електронске поште, форуми или сајтови намењени вођењу дискусија (chat rooms). Интернет-претраживачи нарочито су погодни за брз и анониман приступ јавним информацијама издатим у дневној и периодичној штампи. Прикупљање исте количине једнако вредних података традиционалним путем, у хемеротекама, било би практично немогуће. Уз одређена информатичка знања и вештине, појединцима и организацијама омогућен је приступ и оним информацијама које спадају у категорију интерних, поверљивих и тајних, дакле поузданих информација.

На размишљање наводи податак да су се планери, приликом припремања напада 11. септембра, користили искључиво информацијама које су биле јавно доступне у кибер простору. На основу реда вожње, модела авиона (капацитета горива), броја резервисаних путничких места и полне структуре путника терористи су били у стању не само да одаберу летове које ће преусмерити, већ и да осигурају стизање авиона до циља, постигну максимизацију штете, али и да процене интензитет евентуалног отпора путника у авионима.

Према доступним подацима из досадашњих истраживања терористи су, користећи се кибер простором, извршили прикупљање података о следећим потенцијалним циљевима у САД:[58]

• Центру за контролу и превенцију болести у Атланти, који се, поред осталог, бави развојем националних одбрамбених стратегија против биолошких напада;

• мрежи националних финансија, која подржава ток банкарских података;

• информационим системима који контролишу рад уређаја у саставу електричних централа, хидротехничких брана и система за прераду воде;

• телекомуникационој мрежи и телефонском сервису хитне помоћи 911;

• председничким и војним командним положајима и њиховим локацијама.

Информације о свим наведеним објектима и системима биле су, са импресивном количином детаља, доступне на интернету.

Закључак

Заштита информације, као најважнијег ресурса XXI века, али и инфраструктуре која је преноси, постала је основна мисија истраживања, студија, норми, мера и напора, под заједничким називом кибер безбедност. Концепт кибер безбедности развио се као последица ширења рачунарских мрежа и стварања глобалне мреже. Тада се увидело,

[57] Putignano, D. S., *op. cit.*, p. 67.

[58] Squitieri, T., *Cyberspace full of targets*, http://www.usatoday.com

захваљујући првим безбедносним инцидентима, у којој мери рачунарски системи и мреже представљају извор ризика за информацију и, посредно, за целокупно информационо друштво. Услед процеса континуиране информатизације становништва и прогресивне аутоматизације инфраструктура и сервиса неопходних за функционисање друштва, повећавао се и значај кибер безбедности. Овај концепт данас је постао централни елемент политика националне безбедности свих технолошки високоразвијених земаља, али и регионалних и глобалних безбедносних политика.

Концепт кибер безбедности је, на теоријском и примењеном нивоу, увео прављење разлике између две категорије претњи: физичке и кибер претње. При том су ове друге перципиране као посебно опасне, будући да их одликује атрибут намерности и да је тешко супротставити им се ефикасно. Инструменти и начини помоћу којих се може конкретизовати безбедносна претња у кибер простору бројни су, а неки од њих су се последњих година наметнули по својој распрострањености и деструктивности. На првом месту то су: напади извршени помоћу малициозних кодова, напади усмерени на опструкцију услуга и разноврсни напади који су инспирисани техникама социјалног инжењеринга, са тежњом да преотму осетљиве информације од свих категорија корисника информационих система.

Међутим, концепт кибер безбедности није евидентирао, или бар не експлицитно, оне безбедносне претње које се заснивају на злоупотреби кибер простора као средства масовне комуникације. Ми смо, у својој класификацији, то учинили сврставши их међу кибер претње. Оправдање за такав поступак нашли смо у чињеници да субверзивне активности у кибер простору, попут информационог ратовања, или пак активности усмерених на подршку тероризму, такође испуњавају нужан критеријум за класификацију одређених претњи у категорију кибер претњи. Наиме, и актери ових претњи, било да је реч о терористима, националним армијама, транснационалним корпорацијама или обавештајним службама, користе информациону технологију као инструмент или, пак, као објект својих активности. Сматрамо да је поменути пропуст последица прилично уског, фрагментарног приступа различитих безбедносних парадигми новим безбедносним изазовима. Чини нам се логичним да информационе науке треба да имају примат на пољу безбедности и заштите информационих система, али и да, исто тако, безбедносне науке не треба да пренебрегавају други аспект феномена – последице за безбедност државе и становништва које могу произаћи из угрожавања или злоупотребе информационих система.

Приступ сложеном проблему безбедносних претњи у кибер простору са позиција наука безбедности захтевао би идентификацију, класификацију и исцрпну анализу не само претњи усмерених ка кибер простору, већ и субјеката претњи, тј. њихових актера, са становишта различитих безбедносних парадигми, као што су: национална, људска, глобална и регионална безбедност. Будући да садашњи степен тематизације овог проблема одликује непостојање јасног теоријског оквира и прецизно дефинисаних основних појмова, у овом раду смо се усредсредили на исцрпну дескрипцију и класификацију појединих појавних облика овог феномена са аспекта безбедносних наука ради формирања полазне грађе за будућа теоријска и емпиријска истраживања. Холистички приступ у истраживању безбедносних претњи информационом друштву захтева даљу разраду концепта кибер безбедности и подразумева интегративно проучавање, са намером да у будућности обухвати све димензије ове сложене појаве, уз уважавање различитих приступа разнородних научних дисциплина.

Литература

1. Arquilla J., Ronfeldt D.: Мрежни рат и кибер рат, РАНД корпорација, извод из студије објављене у "*Comparative Strategy", Volume 12, 1995.*

2. BBCSerbian. com, http://www.bbc.co. uk/serbian/news/2006/06/060608_zarqawi_gallery.shtml.

3. Bergen, P. L.: *Holy War, Inc. Inside the secret world of Osama bin Laden*, The Free Press, New York, 2002.

4. Cartwright J.: Vice Chairman of the Joint Chiefs of Staff, Cyberspace Operations Lexicon, 2010. Retrieved at http://www.nsci-va.org/CyberReferenceLib/201011 Joint%20Terminology%20for%20Cyberspace%20Operations.pdf

5. Dai Qingmin: „On Integrating Network Warfare and Electronic Warfare," *China Military Science*, Feb 2002, pp 112–117.

6. Eedle, P.: "Al Qaeda takes fight for 'Hearts And Minds' to the web", *Jane's Intelligence Review*, 2002, http://www.freerepublic.com

7. Fischer, E.: CRS Report for Congress, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, http://csrc.nist.gov

8. Greenberg, L., Goodman, S., Soo Hoo, K.: *Information Warfare and International Law*, National Defense University, Washington DC, 1998.

9. How is Al Qaeda funded?, Council on Foreign Relations, http://www.terrorismanswers.org

10. Hudson, R.: *The sociology and psychology of terrorism: who becomes a terrorist and why?*, http://www.fas.org

11. Inside Defense, http://www.insidedefense.com.

12. International Association of Defense Counsel, http://www.iadclaw.org/books.cfm

13. Internet Haganah, http://internet-haganah.com/haganah/.

14. Islamic Charity Indicted, http://www.cbsnews.com, http://news.findlaw.com

15. L'Armement, No. 60, Paris, XII.1997–I.1998.

16. Limno, A. N., Krysanov, M. F.: (2003) 'Information Warfare and Camouflage, Concealment and Deception', Military Thought, vol. 12, no. 2

17. Northeast Intelligence Network – Terrorism News, Information and Analysis: *Kidnapping & Hostage Taking* (from *Al Battar*, Issue 10), http://www.homelandsecurityus.com

18. Piccitto, D.: *Terrorismo: dal fondamentalismo religioso ad Internet*, Facoltà di lettere e filosofia, Facoltà di Scienze Politiche, Università degli Studi di Perugia, 2005.

19. Pirumov, V.: (1996) 'Nekotorye aspekty informatsionnoi voiny' (Certain aspects of information warfare). Conference speech in Brussels in May 1996, наведено у R Heickerö, "Emerging Cyber Threats and Russian Views on Information warfare and Information operations'', 2010.

20. Putignano, D. S.: *La criminalità informatica: cyberterrorismo*, Facoltà di Giurisprudenza, Università degli Studi di Bari, 2002.

21. *Qa'idat al-Jihad, Iraq, and Madrid – The First Tile in the Domino Effect?*, The International Policy Institute for Counter-Terrorism, http://www.ict.org.il/Articles/tabid/66/Articlsid/557/currentpage/15/Default.aspx

22. Scalese, A.: *La sicurezza del cyberspazio: analisi e considerazioni*, Facoltà di Scienze Politiche, Università degli Studi di Trieste, 2005.

23. Schleher C.: *Electronic Warfare in the information age*, Artech House, 1999.

24. SITE Institute, http://www.siteinstitute.org/

25. Squitieri, T.: *Cyberspace full of targets*, http://www.usatoday.com

26. Szafranski R.: „A Theory of Information Warfare", Published Airpower Journal Spring 1995; извор – www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm.; приступљено 16. јануара 2011. године.

27. Thomas, T.: "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, Vol. 33, 2003.

28. United States Institute of Peace, http://www.usip. org/pubs/specialreports/sr116.html

29. Weimann, G.: *How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report, New York, http://www.usip.org/pubs/specialreports/sr116.pdf

30. Weimann, G.: *Terror Groups Exploit Internet for Communications, Recruiting, Training*, JINSA Policy Forum, http://www.jinsa.org

31. Форца, Б.: Нове форме сукоба, „Војни информатор", број 4/2001, стр. 14.

32. Волков, В.: *Дезинформација – од тројанског коња до Интернета*, Наш дом, Београд, 2005.

33. Вулетић, Д.: „Шта је информационо ратовање?", *Безбедност*, бр. 3/05, Београд, 2005.

34. Група аутора, Информациони и математички модели у процесима командовања, Лабораторија за примењену математику, Београд, 1969.

35. Милашиновић, Р., Милашиновић, С.: *Увод у теорије конфликата*, Факултет цивилне одбране, Београд, 2004, стр. 289–314.

36. Петровић, С.: *Компјутерски криминал*, МУП Србије, Београд, 2001, стр. 337.

37. Путник, Н.: *Сајбер простор и безбедносни изазови*, Факултет безбедности, Београд, 2009.

38. Републички центар за истраживање ратних злочина Републике Српске, http://www.rs-icty.org/PUBLIKACIJE/Paneli%20pdf%20srp/PANEL4srp.pdf

39. Тофлер, А., Тофлер, Х.: *Рат и антират*, Paideia, Београд, 1998.

40. Цигурски, О.: *Могућности заштите од стеганографије*, Зборник Факултета безбедности, Београд, 2008.