УДК:
323.28:004.738.5
Примљено:
13. фебруара 2009.
Прихваћено:
18. фебруара 2009.
Оригинални
научни рад

ПОЛИТИЧКА РЕВИЈА
POLITICAL REVIEW
Година (XXI) VIII, vol=19
Бр. 1 / 2009.
стр. 237-254.

Ивана Дамњановић
Факултет политичких наука, Београд

ПОСТОЈИ ЛИ САЈБЕРТЕРОРИЗАМ?

Сажетак

Експанзија Интернета и на њему заснованих технологија, као и њихов све већи утицај на друштвене појаве и процесе, довели су до повећаног занимања истраживача за све феномене који су произашли из таквог развоја. Један од таквих феномена је и сајбертероризам, који захваљујући својим потенцијално разорним последицама, али и медијској атрактивности заокупља пажњу великог броја аутора. Упркос томе, још увек не постоји дефиниција сајбертероризма која би била општеприхваћена, како у академским, тако и у политичким круговима. Стручњаци се такође споре око тога у којој мери је опасност од сајбертерористичког напада реална и блиска. При томе се не доводи у питање техничка изводљивост сајбертерористичких аката, колико оспособљеност данас присутних терористичких организација да их изведу. Циљ овог рада је да покаже да до данас није било напада који би се недвосмислено могао назвати сајбертерористичким, као и да опасност од таквог напада није непосредна, односно да је сајбертероризам, као политички феномен, још увек више у домену потенцијалног, него актуелног.

Кључне речи: Тероризам, Интернет, сајбертероризам, информатички тероризам, сајбер-напади, кључни инфраструктурни системи.

Присуство терориста и терористичких организација на Интернету није новост. Штавише, чини се да је у последње време Интернет постао омиљено средство терориста како за међусобну комуникацију тако и за комуникацију са јавношћу. Све чешће поруке о отмицама и ликвидацијама до телевизије и штампе стижу

преко веб сајтова које воде терористичке организације. Владе развијених земаља признају реалност претње од сајбертерористичког напада, и убрзано траже одговарајућа решења. Речима Мојре Конвеј (*Maura Conway*), "у новинама и часописима, на филму и телевизији, 'сајбертероризам' је у духу времена".[1)]

Кључно је, међутим, питање колико је (у начелу реална) опасност од сајбертерористичких напада заиста блиска и непосредна. Већ годинама различити аналитичари упозоравају да велики сајбертерористички напад само што се није догодио,[2)] користећи при том изразе као што су "електронски Перл Харбор" или "електронски Ватерло".[3)] Ипак, до сада није било ни једног документованог инцидента који би се с пуним правом могао назвати сајбертерористичким актом.[4)]

Није спорно да су терористи присутни на Интернету, и то на много начина. Према Вајману (*Gabriel Weiman*), Интернет је због саме своје природе на много начина идеална арена за активност терористичких организација. Као основне предности Интернета он наводи:

- једноставан приступ:
- мало или нимало регулације, цензуре или других облика контроле од стране власти
- потенцијално огромну публику раштркану широм света
- анонимност комуникације
- брз проток информација
- јефтин развој и одржавање присуства на мрежи

1) **Conway**, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet.* First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009.

2) Тако су, на пример, неки аутори предвиђали да ће до значајног сајбертерористичког напада доћи у време председничких избора у САД 2004. (Види на пример **Coleman**, K. (2003). *Cyber Terrorism*, Directions Magazine, http://directionsmag.com/article.php?article_id=432, 10.03.2009.)

3) **Rogers**, M. (2003). *The Psychology of Cyber-Terrorism.* U, A. Silke (pr.), Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences, Chichester: Wiley, стр. 79

4) Упор. **Conway**, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet.* First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009., као и **Rogers**, M. (2003). *The Psychology of Cyber-Terrorism.* U, A. Silke (pr.), Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences, Chichester: Wiley, стр. 81

– мултимедијално окружење (могућност да се комбинује текст, слика аудио и видео и да се дозволи корисницима да "скидају" филмове, песме, књиге, постере и тако даље)

– могућност да се убличава извештавање у традиционалним масовним медијима, који све више користе Интернет као извор својих информација.[5)]

И други аутори наводе сличне предности које Интернет може имати за терористе, при чему се нарочито истичу могућности анонимне комуникације и непосредне контроле информација, као и ниски трошкови. Све јефтинији приступ Интернету и његове све веће техничке могућности омогућавају било коме да постане учесник у светским догађањима. Само у последњих осам година, број корисника у свету порастао је за око 336%, при чему је највећи пораст у земљама Блиског Истока (1296,2 %).[6)]

Дискутабилно је, међутим, које се активности на Интернету могу сматрати терористичким у правом смислу те речи, па су неки аутори покушали да их на одређени начин класификују. Према Вајману све активности терориста на Интернету могу се сврстати у једну од осам група:

1. психолошки рат
2. публицитет и пропаганда
3. тражење информација
4. прикупљање фондова
5. регрутовање и мобилизација
6. умрежавање
7. дељење информација
8. планирање и координација[7)]

Са друге стране, Мојра Конвеј предлаже скалу која активност терориста на Интернету карактерише као *употребу*, *злоупотребу*, *офанзивну употребу* и *сајбертероризам*.[8)] Важно је нагласити да ове две класификације не искључују једна другу – тако се готово

5) **Weimann**, G. (2004). *How Modern Terrorism Uses the Internet.* Washington, United States Institute for Peace, http://www.usip.org/pubs/specialreports/sr116.html

6) http://www.internetworldstats.com/stats.htm, 10.03.2009.

7) **Weimann**, G. (2004). *How Modern Terrorism Uses the Internet.* Washington, United States Institute for Peace, http://www.usip.org/pubs/specialreports/sr116.html

8) **Conway**, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet.* First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009.

све активности са Вајманове листе могу заправо сврстати у употребу Интернета, осим неких аспеката психолошког рата, регрутовања и мобилизације, и одређених начина прикупљања фондова.

Највећи део активности терориста на Интернету отпада на, како је већ речено, уобичајене начине употребе Мреже. У ову категорију спадају пропагандна делатност, највећи део комуникације која се одвија путем имејла и у чет-румовима, прикупљање фондова (нпр. путем добровољних прилога или онлајн продајом), прикупљање информација, па чак до неке мере и психолошки рат. Неки аутори сматрају да овај пре свега комуникациони аспект Интернет активности заправо не представља неку радикалну новину, већ да терористи користе Интернет на исти начин на који су користили и остале облике масовних комуникација.[9)]

У злоупотребе Интернета пре свега спадају напади на вебсајтове (разне врсте ДоС напада, дифејсинг)[10)] или мреже, као и спамовање[11)], док би се као офанзивна употреба Интернета могле окарактерисати активности које наносе материјалну и другу штету – као што је ширење вируса, тројанаца и логичких бомби[12)], или електронска крађа.

ДЕФИНИСАЊЕ САЈБЕРТЕРОРИЗМА

Сајбертероризам, према Конвејевој, представља следећи ниво терористичке активности на Интернету, који би по последицама био разорнији од офанзивне употребе Интернета. Упркос великом интересовању истраживача за овај феномен, он је још увек теоријски и правно у великој мери неодређен - још увек не постоји његова јасна и општеприхваћена дефиниција. Размере ових неслагања илуструје и релативно конфузна одредница у иначе веома информативном Такраховом (*John Richard Thacrakh*) «Речнику терори-

9) **Valeri** L., **Knights** M., (2000). *Affecting Trust: Terrorism, Internet and Ofensive Information Warfare*, Terrorism and Political Violence, 12, 1, стр. 16

10) **DoS** (Denial of Service) напади – тип напада који покушава да учини бескорисним извор на мрежи, најчешће слањем огромних количина података. Углавном се користи за нападе на e-mail или IRC сервере и веб сајтове; **defacing** – неовлашћена измена садржаха веб странице

11) **спам** – свака нежељена порука

12) **вирус** – програмски фрагмент који се убацује у већи програм и активира се само када се укључи програм-домаћин, после чега се умножава, инфицирајући друге програме; **тројанац (тројански коњ)** – кодирани фрагмент који се крије у програму и обавља маскирану функцију. То је популарни механизам да се прикрије вирус; **логичка бомба** – једна врста тројанског коња која се користи да би се «лансирао» вирус или за неки други начин напада на систем.

зма», у којој се питање дефиниције потпуно прескаче и само се у неколико пасуса указује на опасност од потенцијалног овладавања терориста новим информационим технологијама.[13)]

Сам термин сајбертероризам сковао је Бери Колин[14)] (*Barry Colin*). Овај термин се састоји од две компоненте: сајберспејса (сајберпростора) и тероризма. Данас постоје различите дефиниције сајберспејса[15)], мање или више прецизне, а Колинова дефиниција – да је сајберспејс "простор у коме функционишу компјутерски програми и крећу се подаци"[16)] у великој мери погађа мету.

Други део дефиниције је много компликованији због познатих тешкоћа и котроверзи при дефинисању тероризма. Укратко, дефиниција сајбертероризма у многоме зависи од дефиниције тероризма коју аутор прихвата. Још један од проблема при јасном одређењу овог појма је његово недовољно разликовање од сајбер криминала. Приручник Уједињених нација о криминалу повезаном са информационим технологијама признаје да ни после неколико година расправе међу стручњацима не постоје међународно признате дефиниције ових термина.

Ваздухопловне снаге Сједињених Америчких Држава су још 1970-их година формулисале своју дефиницију сајбертероризма, као "употребе информација и информационих система као оружја у сукобу у коме су информације и информациони системи мете".[17)] Ова очигледно преширока дефиниција не садржи специфичне карактеристике које би разликовале сајбертероризам од других облика употребе и злоупотребе информација и информационих система, као што су информатички рат, сајбер криминал и слично.

Једна од првих релативно широко прихваћених дефиниција сајбертероризма датира из 1998. године. У извештају Центра за Стратешке и међународне студије (*Center for Strategic and International Studies*) под насловом *Cybercrime, Cyberterrorism, Cyberwar-*

13) **Thackrah**, J. R. (2004). *Dictionary of Terrorism.* London: Routledge, стр. 61

14) **Janczewski**, L. J., **Colarik**, A. M. (ур.) (2008). *Cyber Warfare and Cyber Terrorism,* Hershey, Information science reference., стр. xiii

15) Термин **сајберспејс** (*cyberspace* – сајберспејс, сајбер-простор, кибер-простор) је први употребио писац научне фантастике Вилијем Гибсон (*William Gibson*) у свом роману Неуромансер (Neuromancer) 1984. године.

16) **Collin**, B. C., (2000). *The Future of Cyberterrorism*, izlaganje na skupu **11th Annual International Symposium On Criminal Justice Issues,** http://afgen.com/terrorism1.html, 10.03.2009.

17) **Holtz**, S., *Cyber Terrorism*, Florida Atlantic University, Davie (Feb. 19, 2003). Цитирано према: **Ronczkowski**, M. R. (2004) *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*, Boca Raton: CRC Press., стр. 132

fare, Averting an Electronic Waterloo наводи се да "Сајбертероризам означава унапред смишљене, политички мотивисане нападе поднационалних група, кландестинских актера или појединаца против информационих и компјутерских система, компјутерских програма и података који резултирају насиљем против цивилних (*noncombatant*) мета."[18] Веома је слична и дефиниција Мојре Конвеј, која одређује сајбертероризам као "унапред смишљени, политички мотивисан напад од стране поднационалних група или кландестинских актера против информација, компјутерских система, компјутерских програма и података који имају за последицу насиље над цивилним метама".[19] Обе ове дефиниције се ослањају на законску дефиницију тероризма која важи у САД. На њих се надовезује и даље их прецизира Коларикова (*Andrew Michael Colarik*) дефиниција, по којој је сајбертероризам "унапред смишљен, политички мотивисан криминални акт почињен од стране поднационалних група или кландестинских актера против информационих или компјутерских система, компјутерских програма и података, који има за последицу физичко насиље, када је намера да се изазове страх код цивилних мета.»[20]

Колман (*Kevin Coleman)* сматра да је "сајбертероризам смишљена употреба реметећих активности, или претња њима, против компјутера и/или мрежа, са намером да се проузрокује штета или остваре даљи друштвени, идеолошки, религијски, политички или слични циљеви, или да се застраши нека особа зарад испуњења тих циљева".[21] Према Дороти Денинг (*Dorothy Denning*) "сајбертероризам је конвергенција између сајберспејса и тероризма. Он се односи на противзаконите нападе и претње нападима против компјутера, мрежа и информација ускладиштених у њима када су почињени да би се застрашила или принудила влада или њен народ у промоцији политичких или друштвених циљева. Даље, да би се оквалификовао као сајбертероризам, напад мора да резултира

18) Цитирано према: **Colarik**, A. M., (2006). *Cyber Terrorism: Political and Economic Implications* , Hershey: Idea Group Publishing., стр. 46

19) **Conway**, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet.* First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009.

20) **Colarik**, A. M., (2006). *Cyber Terrorism: Political and Economic Implications* , Hershey: Idea Group Publishing., стр. 47

21) **Coleman**, K. (2003). *Cyber Terrorism*, Directions Magazine, http://directionsmag.com/article.php?article_id=432, 10.03.2009.

насиљем против лица или имовине, или у најмању руку да нанесе довољно штете да би изазвао страх".[22)]

Неки аутори користе уместо овог термина термин *информатички тероризам.* Творац овог термина је Тимоти Томас (*Timothy Thomas*). По његовој дефиницији информатички тероризам обухвата 1) спону између криминалне преваре или злоупотребе информационог система и физичког насиља тероризма и 2) намерну злоупотребу дигиталног информационог система, мреже и компоненте са циљем да се подржи или омогући терористичка кампања или акција.[23)] У овом другом случају, злоупотреба система не би морала да доведе до директног насиља над људима, иако би ипак могла да подстиче страх. Употреба термина *информатички тероризам* заснива се на идеји да у савременом друштву постоје два главна метода које терористи могу да искористе за информатички терористички напад:

1. када је информациона технологија мета

2. када је информациона технологија оруђе за веће операције.

Први метод подразумева да ће терориста напасти информациони систем ради саботаже (електронске или физичке), па и уништења или прекидања самог информационог система и било које информационе инфраструктуре (на пример струје, комуникације итд.) зависне од нападнуте технологије. Други метод подразумева да ће терориста манипулисати информационим системом и користити га, мењајући или неовлашћено преузимајући податке, или приморавајући систем да обави функцију за коју није предвиђен (као на пример ометање контроле ваздушног саобраћаја).

		мета	
		физичка	дигитална
оруђе	физичко	а) конвенционални тероризам (подметање бомбе у Оклахома Ситију)	б) напад ИРА на Square Mile у Лондону, 4. октобра 1992.
	дигитално	в) хакер вара систем контроле лета да би спустио авион	г) тројански коњ у јавној мрежи

(табела преузета из Devost, M. G., Houghton, B. K. i Pollard, N. A. (1998). *Information Terrorism: Can You Trust Your Toaster?*, http://www.ndu.edu/inss/siws/ch3.html, 10.03.2009.)

22) **Denning**, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009.

23) Timothy L. **Thomas**, *Deterring Asymmetric Terrorist Threats to Society in the Information Age* (Carlisle, PA: US Army War College Strategic Studies Inst. Oct. 2001). Цитирано према **O'Brien**, K. A. (2003). *Information Age, Terrorism and Warfare*, u T. R.Mockaitis i P. B.Rich (pr.). Grand Strategy in the War against Terrorism, London: Frank Cass, стр. 191

Према овој табели, поље а) означава конвенционални тероризам (отмице, бомбашки напади, атентати итд.). Поља б), в) и г) представљају информатички тероризам. Поље б) означава конвенционално решење за напад на високотехнолошку (*high-tech*) мету. Терористички напад приказан у пољу в) користи информационе системе да би се створила физичка штета. Поље г) представља напад у коме се користи рањивост војних, комерцијалних и јавних система који се ослањају на информационе технологије. Ово поље означава "чисту форму" информатичког тероризма, који је најтеже открити, и коме се најтеже супротставити. Постоје и суптилније форме информатичког тероризма (на пример, електронска крађа средстава за подршку терористичким операцијама, преусмеравање пошиљки оружја итд.), које такође спадају у политичке злочине, можда још опасније јер су мање драматичне од сајбер-Чернобиља и зато теже за откривање, а могу изгледати и као "обични" злочини.[24)]

Из табеле и објашњења јасно је да би се заправо само поље под в) могло означити као сајбертероризам у правом смислу те речи, а када је реч о пољу г) морали би да буду испуњени још неки услови (наношење материјалне штете, људске жртве, или у најмању руку ширење страха већих размера).

Сумирајући наведене ставове, могли би се као неопходни издвојити следећи дефиниционi елементи сајбертероризма:

1. употреба информационих/компјутерских технологија као оружја (а не само као логистичке подршке, средства комуникације или мете)
2. политичка мотивација
3. оријентација ка симболици/спектакуларности/публицитету
4. значајна материјална штета и/или људске жртве, или претња таквим последицама, што доводи до
5. ширења страха већих размера.

Укратко, чини се да дефиниција сајбертероризма наслеђује све проблеме са којима се сусреће сваки покушај дефинисања тероризма, додајући неке нове (нпр. да ли се под сајбертероризмом може подразумевати физичко уништење компјутера или компјутерског система?). Закључак може бити сличан – без обзира на (не)посто-

24) **Devost**, M. G., **Houghton**, B. K. i **Pollard**, N. A. (1998). *Information Terrorism: Can You Trust Your Toaster?*, http://www.ndu.edu/inss/siws/ch3.html, 10.03.2009.

јање теоријски одређеног појма, препознаћемо сајбертероризам када/ако се деси.

САЈБЕРТЕРОРИСТИЧКИ НАПАДИ – МОГУЋИ АКТЕРИ, СРЕДСТВА И НАЧИНИ НАПАДА

О могућим начинима извођења и метама сајбертероризма углавном постоји слагање међу стручњацима па и владама. Владе су нарочито забринуте због терористичких сајбер напада (или напада иза којих стоје друге државе) на кључне инфраструктурне системе које чине национални "систем за одржавање живота". Због велике зависности ових система од информационе технологије и већ бројних напада и покушаја напада на њих, САД су отишле најдаље у процени ових претњи и проналажењу адекватних одговора, па је још Клинтонова администрација дефинисала осам кључних инфраструктурних система који могу бити мета сајбертероризма или друге врсте информатичког напада: телекомуникације, банкарство и финансије, електрична енергија, дистрибуција и складиштење нафте и гаса, водоводни систем, саобраћај, хитне службе и владине службе.[25] Према Колину, тачке где се састају физички и виртуелни свет (и које могу бити мете напада сајбертерориста) су:

- фабрике за прераду хране
- фармацеутска постројења
- постројења електричне енергије и природног гаса
- раскрснице пруга и системи за контролу саобраћаја
- следећа генерација контроле ваздушног саобраћаја
- практично сва модерна војна опрема
- комуникације војске и јавне безбедности
- цивилне комуникације.

Он сматра да постоје три потенцијална акта сајбертероризма на тачкама спајања:

1. деструкција;
2. мењање и
3. прибављање и ретрансмисија[26]

25) **Denning**, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009.

26) **Collin**, B. C., (2000). *The Future of Cyberterrorism*, izlaganje na skupu **11th Annual International Symposium On Criminal Justice Issues,** http://afgen.com/terrorism1.html, 10.03.2009.

Оваква класификација није у нескладу са другом, углавном прихваћеном поделом, која каже да да постоје четири могућа начина напада: одбијање, обмана, уништавање и експлоатација. То јест, неко би могао да упадне у информациони систем да би зауставио његов рад, да убаци лажне податке или "злоћудан" код да би створио погрешне резултате, да физички или електронски уништи систем, или да се "прикачи" на систем да би крао податке.[27)]

Дефиниционе недоумице и медијска прашина која се подиже око сајбертероризма тешко дозвољавају једноставан и изричит одговор на питање колико је реална и блиска претња сајбертероризма. Стручњаци се, као што је већ речено, углавном слажу да се до сада није догодио ни један напад који би се без сумње и оклевања могао окарактерисати као сајбертеристички. Они сматрају да терористи тренутно углавном једноставно употребљавају Интернет, попут свих осталих корисника, док су злоупотреба и офанзивна употреба Интернета ређе, а да до сада није забележен ни један акт сајбертероризма.[28)] То наравно не значи да сајбер напада на компјутерске системе и мреже, па чак и "кључни национални инфраструктурне системе", није било.

Само током фискалне 2007. године у Сједињеним Америчким државама пријављено је око 37000 случајева нарушавања безбедности информационих система (како у влади тако и у приватном сектору),[29)] при чему треба имати у виду да компаније често не пријављују успешно изведене нападе (по неким проценама свега у 10% случајева).[30)] Осим тога, разне федералне агенције нападнуте су 13000 пута, а компјутерски системи Министарства одбране чак 80000 пута. Важно је приметити да анализе показују да је око 40% свих инцидената на мрежи међународног карактера.[31)]

Многи стручњаци и владини званичници сматрају да има озбиљних разлога за забринутост. Још 1996. године је Џон Дојч (*John Deutch*), бивши директор ЦИА-е рекао: "Међународне те-

27) **Berkowitz**, B., **Hahn,** R. W. (2003) Cybersecurity: Who's watching the store?**,** Issues in Science and Technology; 19, 3, 55-62, стр. 55

28) **Conway**, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet.* First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009.

29) **Posner**, M. (2007). *America already is in a cyber war, analyst says*, http://www.govexec.com/story_page.cfm?articleid=38667

30) **Coleman**, K. (2003). *Cyber Terrorism*, Directions Magazine, http://directionsmag.com/article.php?article_id=432, 10.03.2009.

31) **Grove**, G. D., **Goodman**, S. E. i **Lukasik**, S. J. (2000), *Cyber-attacks and international law*, Survival, 42, 3,стр. 90

рористичке групе очигледно имају могућност да нападну информациону инфраструктуру Сједињених Држава, чак и ако употребљавају релативно једноставна средства. [...] Забринут сам због могућности за будуће такве нападе. Могу се употребити методи у распону од тако традиционалних терористичких метода као што је бомба у возилу, управљена у овом случају против, на пример, телефонске централе или неког другог комуникационог чвора, до електронских средстава напада. Ови други методи могли би се ослањати на плаћене хакере. Способност да се започне напад, међутим, вероватно има велики број терористичких група, које се све више навикавају на Интернет и остала модерна средства за своје сопствене комуникације. Ово укључује како добро познате и одавно створене организације као што је либански Хезболах, као и безимене и мање познате ћелије међународних терориста попут оних који су напали Светски трговински центар".[32)] Пола деценије касније, саветник ове агенције за питања технологије Лоренс Гершвин (*Lawrence Gershwin*) изјавио је да, мада терористи још увек дају предност бомбама, «предвиђамо битније сајбер-претње у будућности, са уласком нове, технички компетентније генерације у редове терориста».[33)]

Има индикација да неке терористичке групе теже сајбертероризму, самом по себи или заједно са актима физичког насиља. Још у новембру 1998. године саопштено је да је Калид Ибрахим, који се сматра чланом организације Харкат-ул-Ансар, покушао да купи војни софтвер од хакера који су га украли из компјутера Министарства одбране. ПИРА (*The Provisional Irish Republican Army*) је користила услуге унајмљених хакера да би дошла до кућних адреса полицајаца и обавештајаца, а ти подаци су коришћени да би се испланирала убиства тих особа у "ноћи дугих ножева", уколико британска влада не пристане на услове примирја.[34)]

Безбедносни пропусти, као и изразито технолошка оријентација неких терористичких организација попут секте Аум Шинрикјо (која велики део својих средстава добија развојем и продајом

32) Цитирано према: **Conway**, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet*. First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009.

33) Tim **McDonald**, 'CIA to Congress: We're Vulnerable to Cyber-Warfare', *NewsFactor Network* (22 June 2001)Цитирано према: **O'Brien**, K. A. (2003). *Information Age, Terrorism and Warfare*, u T. R.Mockaitis i P. B.Rich (pr.). Grand Strategy in the War against Terrorism, London: Frank Cass, стр. 198

34) **Denning**, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009.

комерцијалног софтвера) додатно су подгрејали атмосферу страха од сајбертерористичког напада у блиској будућности. Наиме, Аум Шинрикјо је као подуговарач развила софтвер за праћење 150 полицијских возила. Када је ово откривено, секта је већ имала поверљиве податке о 115 возила. Осим тога, секта је радила на софтверу који је користило најмање 80 јапанских фирми и 10 владиних агенција. Између осталог и због овог инцидента, америчка администрација је послала хитан допис неколицини својих амбасада да престану да употребљавају софтвер за који се накнадно открило да су га писали држављани бившег Совјетског Савеза.[35)]

Бери Колин, творац појма сајбертероризам, сматра да постоји неколико узнемирујућих могућих сценарија сајбертерористичког напада који су сви већ данас технички остварив. Неки од ових сценарија обухватају, на пример, измене у формулама дечије хране и лекова, или преузимање контроле ваздушног саобраћаја од стране терориста, који би онда могли да изазову судар цивилних путничких авиона. Колин закључује: "сајбертерориста ће осигурати да становништво не може јести, пити, кретати се или живети. Осим тога, људи неће бити упозорени, и неће моћи да затворе терористу, који ће вероватно бити на другој страни света."[36)]

Валери и Најтс (*Lorenzo Valeri, Michael Knights*) сматрају да поред логистичке употребе офанзивног информатичког рата за финансирање терористичке групе путем компјутерског криминала, постоје још два начина употребе офанзивног информатичког рата. Прва је да се саботира рад информационих система у покушају да се омете функционисање или они елементи кључних националних инфраструктура који зависе од информација, са или без намере да се у том процесу изазову масовне жртве. Други је да се манипулише подацима у оквиру информационог система или да се они употребе са специфичним циљем да се подрије перцепција поверења, на којима се темеље Интернет и електронска трговина међу корисницима уопште.[37)]

35) **Denning**, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009. Видети, такође **O'Brien**, K. A. (2003). *Information Age, Terrorism and Warfare*, u T. R.Mockaitis i P. B.Rich (pr.). Grand Strategy in the War against Terrorism, London: Frank Cass, стр. 198 и даље

36) **Collin**, B. C., (2000). *The Future of Cyberterrorism*, izlaganje na skupu **11th Annual International Symposium On Criminal Justice Issues,** http://afgen.com/terrorism1.html, 10.03.2009.

37) **Valeri** L., **Knights** M., (2000). *Affecting Trust: Terrorism, Internet and Ofensive Information Warfare*, Terrorism and Political Violence, 12, 1, стр. 28-29

Износећи као аргументе чињенице да су информациони системи повезани са кључним националним инфраструктурама добро, и све боље заштићени, они сматрају да је много вероватније да ће терористи покушати да подрију поверење корисника у Интернет уопште. Подривајући перцепцију корисника о поузданости Интернета, терористичке организације могу да постигну два директно повезана циља. Као прво, они ограничавају ефикасност политика западних влада према електронској трговини. Корисници се неће лако упуштати у е-комерц трансакције због перципираних претњи по своја финансијска средства и приватност. Друга последица је кварење оних елемената који објашњавају друштвени и комерцијални успех Интернета. Да би се супротставили овим ометајућим активностима, комерцијалне институције, владе и војне ораганизације морају да разраде чвршће мере осигурања информација да би очували позитивну перцепцију јавности о овим новим информационим технологијама. Међутим, ако се погрешно схвате, ове мере могу да угрозе оне карактеристике отворености и флексибилног приступа које су језгро успеха Интернета, тако да би се могло испоставити да је за терористе ово игра у којој свакако добијају.[38] Остаје међутим, отворено питање да ли би се овакав начин вођења офанзивног информатичког рата могао окарактерисати као сајбертероризам.

Постоје, наравно, и аргументи у прилог тезе да се сајбертеористички напади неће догодити у непосредној будућности. Тако Дороти Денинг сматра да "иако је 'хактивизам'[39] стваран и раширен, сајбертероризам постоји само у теорији. Терористичке групе користе Интернет, али и даље више воле бомбе него бајтове као средства подстицања страха."[40] Она своје закључке темељи, између осталог и на истраживању Центра за проучавање тероризма и нерегуларног ратовања у постипломској морнаричкој школи у Монтерају из августа 1999. године. Резултати овог истраживања показују да постоје три нивоа сајбертеористичког потенцијала. Први је једноставан: способност за основно хаковање у поједи-

38) **Valeri** L., **Knights** M., (2000). *Affecting Trust: Terrorism, Internet and Ofensive Information Warfare*, Terrorism and Political Violence, 12, 1, стр. 29-32

39) **хактивизам** – ненасилна употреба илегалних или у законском погледу двосмислених средстава ради постизања политичких циљева. Ова средства између осталог могу бити дифејсовање, редирекције, DoS напади, крађа података, пародирање веб сајтова, виртуелне саботаже и развој софтвера

40) **Denning**, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009.

начне системе уз употребу алата које је неко други израдио. На другом нивоу организација може да спроводи компликованије нападе против више система или мрежа, мења или ствара основне хакерске алате. Трећи ниво подразумева могућност за координиране нападе који могу да проузрокују велике поремећаје и пробију веома софистицирану одбрану. Стручњаци из овог тима процењују да би групи која почиње од нуле биле потребне 2 до 4 године да достигне други ниво, а 6 до 10 година да стигне до трећег, мада би неке групе могле то да постигну и брже уз помоћ са стране. По њиховом мишљењу, само би религијски мотивисане групе тежиле да достигну овај последњи ниво, што би било конзистентно са њиховом недискриминативном употребом насиља.[41] И Валери и Најтс се слажу да би извођење сајбертерористичког напада који би као могућу последицу имао масовне жртве захтевао дуготрајне припреме, детаљну анализу мете и могућих последица напада (јер међуповезаност информационих система и савременог друштва уопште тешко дозвољава да се предвиде све последице поремећаја), као и чекање на одговарајућу прилику, што подразумева велико стрпљење. Они изражавају сумњу да је већина терористичких организација фукционално и психолошки спремна на спровођење тако дугорочног пројекта.[42]

САЈБЕРТЕРОРИЗАМ ДАНАС

За терористе сајбертероризам би свакако имао неке предности над физичким методама. Овакве акције могу да се изведу из далека и анонимно, и не захтевају руковање експлозивом или самоубилачке мисије. Вероватно ће привући велику пажњу медија, јер су новинари и јавност фасцинирани свим врстама компјутерских напада. С друге стране, терористи могу оклевати да примене нове методе док старе не постану неадекватне, нарочито ако примена нових метода захтева прилично велика знања. Чини се да за сада недостаци односе превагу над предностима, па се може закључити да претња од сајбертерористичких напада ипак није непосредна. Закључак Дороти Денинг да: "за сада камион бомба представља

41) **Denning**, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009.

42) **Valeri** L., **Knights** M., (2000). *Affecting Trust: Terrorism, Internet and Ofensive Information Warfare*, Terrorism and Political Violence, 12, 1,стр. 20-22

много већу претњу од логичке бомбе"[43] ни после готово једне деценије није оспорен.

Постоји, међутим, један други моменат који терористи могу да искористе: стварање страха од сајбертероризма у сврхе психолошког рата. Према Вајману, "сајберстрах" се ствара када се забринутост због тога шта би компјутерски напад могао да учини појачава, док јавност не поверује да ће се напад догодити.[44]

Једно истраживање је утврдило да 75% корисника Интернета верује да би сајбертерористи ускоро могли да, нападом владине или корпоративне компјутерске мреже, изазову губитак живота и масовне жртве. Према истраживању спроведеном у 19 великих градова широм света, 45% испитаника се у потпуности слаже са тезом да ће "компјутерски тероризам бити све већи проблем", а још 35% се донекле слаже са таквим ставом.[45] С обзиром на овакво стање ствари, могуће је да ће терористи успети да остваре свој најдословнији циљ: ширење ужаса и страха, и без посезања за стварним сајбертерористичким нападима.

ЛИТЕРАТУРА

- Berkowitz, B., Hahn, R. W. (2003) Cybersecurity: Who's watching the store?**,** Issues in Science and Technology; 19, 3, 55-62
- Colarik, A. M., (2006). *Cyber Terrorism: Political and Economic Implications* , Hershey: Idea Group Publishing.
- Coleman, K. (2003). *Cyber Terrorism*, Directions Magazine, http://directionsmag.com/article.php?article_id=432, 10.03.2009.
- Collin, B. C., (2000). *The Future of Cyberterrorism*, izlaganje na skupu 11th Annual International Symposium On Criminal Justice Issues, http://afgen.com/terrorism1.html, 10.03.2009.
- Conway, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet.* First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009.
- Denning, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009.

43) **Denning**, D. (2001). *Is Cyber Terror Next?*, New York: U.S: Social Science Research Council, http://www.ssrc.org/sept11/essays/denning.htm 10.03.2009.

44) **Weimann**, G. (2004). *How Modern Terrorism Uses the Internet.* Washington, United States Institute for Peace, http://www.usip.org/pubs/specialreports/sr116.html

45) **Conway**, M. (2002). *Reality Bytes: Terrorist 'Use' of Internet.* First Monday, 7,11. http://outreach.lib.uic.edu/www/issues/issue7_11/conway/index.html, 10.03.2009.

- Devost, M. G., Houghton, B. K. i Pollard, N. A. (1998). *Information Terrorism: Can You Trust Your Toaster?*, http://www.ndu.edu/inss/siws/ch3.html, 10.03.2009.
- Grove, G. D., Goodman, S. E. i Lukasik, S. J. (2000), *Cyber-attacks and international law*, Survival, 42, 3, 89-103
- Janczewski, L. J., Colarik, A. M. (2008). *Cyber Warfare and Cyber Terrorism,* Hershey, InformatIon science reference.
- O'Brien, K. A. (2003). *Information Age, Terrorism and Warfare*, u T. R.Mockaitis i P. B.Rich (pr.). Grand Strategy in the War against Terrorism, London: Frank Cass.
- Posner, M. (2007). *America already is in a cyber war, analyst says*, http://www.govexec.com/story_page.cfm?articleid=38667
- Rogers, M. (2003). *The Psychology of Cyber-Terrorism.* U, A. Silke (pr.), Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences, Chichester: Wiley.
- Ronczkowski, M. R. (2004) *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*, Boca Raton: CRC Press.
- Thackrah, J. R. (2004). *Dictionary of Terrorism.* London: Routledge.
- Valeri L., Knights M., (2000). *Affecting Trust: Terrorism, Internet and Ofensive Information Warfare*, Terrorism and Political Violence, 12, 1, 15-36
- Weimann, G. (2004). *How Modern Terrorism Uses the Internet.* Washington, United States Institute for Peace, http://www.usip.org/pubs/specialreports/sr116.html

Ivana Damnjanovic

IS THERE CYBERTERRORISM PRESENT TODAY?

Summary

Expansion of Internet and Internet-based technologies, as well as their growing impact on social phenomena and processes, led to increased interest of social researchers for "all things cyber". Among these cyber phenomena is cyberterrorism, It occupies attention of numerous scholars and experts due to tis possibly devastating consequences, but also its attractiveness for the media. Despite this interest, there is still no definition of cyberterrorism which is commonly accepted among scholars and government officials. One of the points of dissent among experts is also the proximity of cyberterrorism threat. It is nto the technical feasibility of cyberterrorist attack that is contested, but rather capabitlity of present day terrorist organizations to engage in cyberterrorism. This paper aims to show that no attack carried out by now fits the definition of cyberterror-

ism. Threat of cyberterrorism is not immediate, so cyberterrorism is still in the domain of potential, rather than an actual political phenomenon.

Key Words: terrorism, Internet, cyberterrorism, informationl terrorism, cyber attacks, key national infrastructures