САЈБЕР ТЕРОРИЗАМ КАО РЕАЛНА ПРЕТЊА ПО ДРЖАВЕ И МЕЂУНАРОДНУ ЗАЈЕДНИЦУ

МА Катарина Јонев*

Сајбер тероризам постао је, као и сваки други облик тероризма, глобална претња. Терористи све више користе информационе технологије и интернет као инструмент у борби али и као мету напада. Постоје многе спекулације колико је заправо реална опасност од сајбер тероризма. Пре свега, на било ком нивоу приступа мора да постоји разлика између сајбер тероризам као нелегалног акта у односу на просте активности које спроводе терористи употребом интернета, као што је пропаганда. Разлика је у томе да ли је сајбер напад изазвао ефекат, односно да ли је имао последице која су проузроковала реална физичка оштећења националне инфраструктуре повезане на рачунарске системе, да ли је изазвао смрт или повреду људи, физичко уништење инфраструктуре, оштећење животне средине и финансијске губитке. Стручњаци из области безбедности инсистирају на чињеници да је сајбер простор постао уједно и домен рата и терора, али са друге стране признају да се сајбер терористички напад никада званично није десио. Упркос несугласицама, сајбер тероризам представља озбиљну претњу по државу јер су многи битни аспекти данашњег друштва потпуно зависни од компјутерских система.

*Ауторка је докторски кандидат на Факултету безбедности

Сајбер напади су реалност. Дешавају се свакодневно, са већим или мањим интензитетом и различитим последицама. Расту по обиму, учесталости, софистицираности и деструктивности. Сајбер напади су постали изузетно моћно средство за постизање одређених циљева – нелегална економска добит (сајбер криминал), долажење у посед индустријских и војних тајни (сајбер шпијунажа), укључивање

сајбер напада у војне доктрине (потенцијални сајбер рат). Чињеница је да се све више непријатељстава из физичког, пребацује у сајбер простор. И терористи све чешће користе информационе технологије и интернет, било као инструмент у борби или као мету напада. Информациона безбедност подразумева пре свега безбедност информација у ИТС, а затим саму безбедност рачунара, система и мрежа[1].

Преузето са сајта nato review

Након рушења кула Светског трговинског центра у Њујорку и напада на Пентагон удружена међународна заједница прогласила је рат тероризму. Борба против било каквог облика тероризма постављена је као највиши приоритет у безбедносним агендама скоро свих држава чланица Уједињених нација. Један од облика тероризма који је протеклих година нагло еволуирао и изазвао додатну бојазан држава по њихову сигурност јесте сајбер тероризам.

Попут сваког другог облика тероризма, и сајбер тероризам је глобална претња[2]. Рачунари, рачунарске мреже и интернет стварају глобални сајбер простор који такође прелази границе држава. Интернет је омогућио развој нових облика деловања које дају прилику теро-

[1] Потпуковник Марио Станковић, мајор Небојша Петровић, потпуковник др Ненад Димитријевић, *Информациона безбедност и заштита тајних података у информационо-телекомуникационим системима*, „Нови гласник", 1/2016, стр. 23

[2] Gábor IKLÓDY The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities Defence Against Terrorism Review Vol.3, No. 2, Fall 2010, page 5

ристима да задрже анонимност, а да се истовремено укључе у комуникацију са светом. Све је олакшано, од пласирања својих идеала кроз пропагандне активности, ширење страха на глобалном нивоу широј, глобалној публици, подстицање на тероризам, регрутовање из свих делова света, па чак и извођење софистицираних сајбер напада. Глобални сајбер простор представља јединствени амбијент али и простор у ком је могуће извести акте тероризма.

Постоје многе спекулације да ли сајбер тероризам заправо постоји и колика је реална опасност. Пре свега, од почетка анализе као темељ мора да се постави разлика између сајбер тероризам као нелегалног акта, међународно забрањеног, у односу на једноставну употребу интернета у терористичке сврхе.

ПРОБЛЕМ ДЕФИНИСАЊА ПОЈМА

Први проблем на који се наилази у самој анализи сајбер тероризма као нелегалног акта јесте недовољна прецизна формулација термина. Сајбер тероризам није јасно дефинисан[3]. Последњих година међу академцима, стручњацима из области безбедности, али и политичарима и медијима тај термин се све више користи, чиме је добио на популаризацији и популарности. Сам термин односи се на „политички мотивисане нападе, унапред планиране, на информације, компјутерске системе и програме, како би се изазвао, пре свега, осећај страха и несигурности[4]" државе и грађана. Узимајући у обзир да се одвија у сајбер простору, може се схватити да је терористички акт планиран, извршен или координисан коришћењем рачунарских мрежа и рачунара.

Један од најцитиранијих дефиниција сајбер тероризма је и следећа: „то је смишљени, политички мотивисани напад на информације, рачунарске системе, рачунарске програме и податке који доводи до насиља над невојним циљевима[5]". Сајбер тероризам је и облик тероризма који укључује коришћење компјутера „да би се изазвао колапс у систему јавних сервира и критичне националне инфраструк-

[3] Taliharm Anna Maria ''Cyberterrorism in Theory or in Practice?'' Defence Against Terorrism Review, Vol 3mNo 2, 2010

[4] Pollitt, Mark M. „CYBERTERRORISM– Fact or Fancy." Georgetown University. Department of Computer Science. Dostupno na:w ww. cs.georgetown.edu/~denning/infosec/ pollitt.html>

[5] Center for Stretegic and International Studies „Cybercrime,cyberterrorism,cyberwarfare,Averting and Electroinic Waterloo", CSISM 1998.

туре и изазвало неповерење јавности у институције[6]". Дефиниција сајбер тероризма може бити тумачена и као „политички мотивисана употреба компјутера, било као мета било као оружје субнационалних група или тајних агената који желе да на насилан начин утичу на јавност и владе држава[7]"

Други проблем у дефинисању овог појма је недостатак таксативно и егзактно наведених дела у сајбер простору који би могли бити подведени као дело сајбер тероризма. Ипак, није сваки напад у сајбер простору аутоматски и акт сајбер тероризма[8]. Професор Дороти Денинг са Универзитета Џорџтаун, пионир у дефинисању сајбер тероризма, тврди да је сајбер тероризам „напад који резултира у насиљу против људи или имовине, или да проузрокује штету која ће изазвати страх[9]". Она истиче да се акт сајбер тероризам односи на угрожавање националне инфраструктуре. Већина академика и данас се слажу са њеном дефиницијом[10].

Сајбер простор постао је веома важан домен и централни систем путем ког инфраструктура нормално функционише. Стотине хиљада рачунара, сервера, рутера, оптичких каблова међусобно повезаних чине сајбер простор и омогућавају критичкој инфраструктури успешно функционисање. Циљ сајбер тероризма је да се нанесе „штета или искључи критична национална инфраструктура помоћу рачунарских алата[11]". Критична инфраструктура састоји се из физичког али и сајбер дела и кључна је за функционисање државе, институција, организација, нормалног живота грађана. Угрожавање њеног функционисања имало би велике и озбиљне последице по друштво. Стога су државе и више него забринуте за своју безбедност у сајбер простору. Страх од напада који би могли угрозити функционисање виталних инфраструктура, која се све више ослања на информационо-комуникацио-

---

[6] Soo Hoo, K., Goodman, S. and Greenberg, L., 'Information technology and the terrorist threat', Survival, vol. 39, no. 3 (autumn 1997), pp. 135–55.

[7] Clay Wilson Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, October 2003, str 7

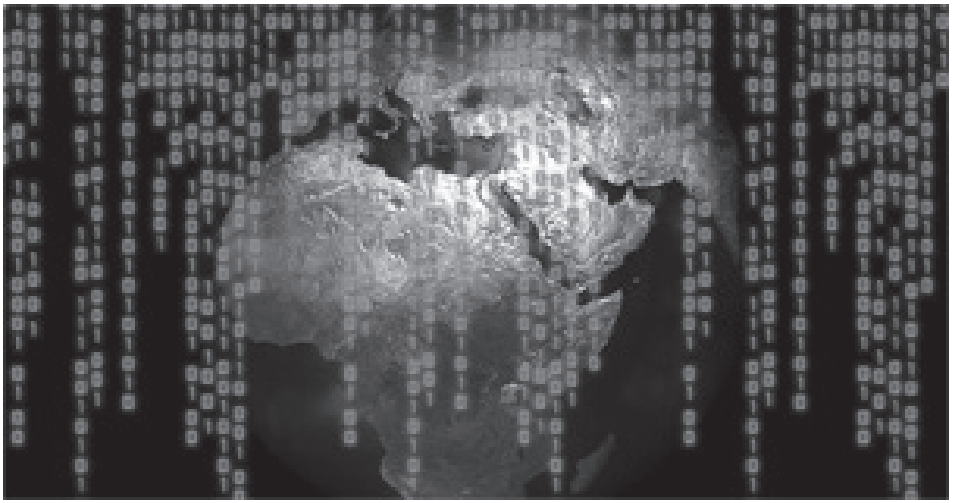
[8] Weimann, 'WWW.Terror.Net: How Terrorism Uses the Internet', United States Institute for Peace, special report number 116, 2004.

[9] Denning Dorothy „Activism, Hactivism,Cyberterrorism", Networks and Netwars, John Arquilla, David Ronfelt, eds, RAND, 2001, str 281

[10] B. Collin, 'The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge', Paper presented at the 11th Annual International Symposium on Criminal Justice Issues, Chicago, September 23–26, 1997.

[11] Gabriel Weimann, „Cyberterrorism:The sum of All Fiers",Studies in Conflict and Terrorism,28, Taylor&Francis Inc, 2005. page 130

не технологије, расте. Страх да ће терористи употребом модерних технологија моћи из било ког дела света да изведу напад довољно великих размера такође расте. Управо то је разлог зашто су сајбер напади у врху приоритета у стратегијама националних безбедности држава као озбиљна претња.



Преузето са сајта start -up. ro. jpg

Трећи проблем када се дискутује о сајбер тероризму је што се овакав напад никада није званично десио. Стога је логично поставити питање да ли је сајбер тероризам данас заиста реална опасност по друштво. Све је већи број заговорника, нарочито у Сједињеним Америчким Државама, који заузимају опрезан став и тврде да је претња стварна и да ће се у будућности све више стрепети од дејства терориста у сајбер простору.[12]

Иако су пракса и теорија изузетно подељене када је реч о тумачењу сајбер терористичког акта, стручњаци се слажу да је употреба ИТ технологија у терористичке сврхе реална опасност. Оно што забрињава безбедносне стручњаке јесте питање да ли су терористи можда развили методе и стратегије за вођење великих сајбер напада са смртоносним намерама и за уништавање националне виталне инфраструктуре.

Не треба из вида искључити јако битну чињеницу да је садашња генерација младих терориста одрастала у дигиталном свету и да су

[12] B. Foltz, Cyberterrorism, computer crime, and reality, Information Management & Computer Security, 15.03.2004, Vol. 12, No. 2, pp. 154-166.

неки од њих свакако развили потребне специјализоване ИТ вештине[13]. Сама природа сајбер простора и интернета и више је него интересантна терористима управо јер гарантује висок ниво анонимности. Нападачима је мало вероватно, понекад и немогуће, ући у траг. Напад може да се деси са било које тачке на планети.

КРИТИЧНА НАЦИОНАЛНА ИНФРАСТРУКТУРА КАО ПОТЕНЦИЈАЛНА МЕТА

У развијеним земљама критичне националне инфраструктуре умногоме се ослањају у свом раду на рачунаре и ИКТ технологије. Док је са једне стране то допринело лакшем функционисању, донело је и проблем јер су постале потенцијално лака мета за нападаче различитих профила, па и терористе. Управо та чињеница да има потенцијално много мета, лако рањивих, представља разлог за појачану забринутост од сајбер тероризма[14].

Ако се узме у обзир да национална инфраструктура обухвата, између осталог, енергетске системе, нуклеарне електране, здравствене и владине институције, бране, електричну енергију и водоснабдевање, саобраћај, телекомуникационе мреже, може се јасно закључити да би потенцијални напад на њихове системе имао огромне последице по државу и њене грађане. Могућност да терористи могу да нападну систем, да оштете, измене режим функционисања или га ставе под своју контролу је застрашујућа. Такав напад такође би узроковао потенцијално огромну катастрофу физичког оштећења, нанео еколошке последице, финансијски губитак и најбитније – изазвао повреду или смрт људи.

Нико не може да предвиди тачан временски оквир за терористички напад, а поготово за напад у сајбер простору. Чињеница је да ће ово постати све више национални, регионални и глобални безбедносни изазов. Управо због једноставности, ефикасности, релативно ниске цене у покретању оваке врсте напада као и потенцијалне делотворности, сајбер напади које су починили сајбер терористи представљају претњу међународној заједници колико и било који други облици тероризма. Моћ терориста да поремете економски систем убацивањем погрешне информације потенцијално је велика. Њихове мете могу да буду здравствене, владине и војне институције. Сајбер

[13] C. Wilson, Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress (RL32114), updated April 1, 2005, p. 23

[14] G. Weimann, Sum of All Fears?, Studies in Conflict & Terrorism, 28 (2005), pp. 129–149 (137).

простор пружио им је прилику да нападну систем и угрозе његово функционисање, да манипулишу подацима, мењају их или бришу. Ово је ефикасан, ефикасан и економичан начин застрашивања и демонстрације моћи сајбер терориста. Сајбер терористи, као и „класични ", имају за циљ да нападају и застрашују цивиле, али овог пута помоћу рачунара, рачунарских мрежа и интернета са мотивом ширења сопствених идеала и политичке борбе. Професор Денинг сматра да постоје три аспекта дефиниције сајбер тероризма, а то су: политичка и друштвена мотивација, настала озбиљна штета и страх. Напади које могу довести до смрти или повреде људи, као што су експлозије у индустријском сектору, авионским несрећама, загађење воде, ометање енергетских система, искључивање рада војних сателита, били би примери. У будућности сајбер напади могу потенцијално да се комбинују са физичким нападима[15].

За сада не постоје званични извештаји која терористичка организација је развила могућности за сајбер нападе који би могли угрозити националне инфраструктуре. Срећом, већина активности које терориста вратило коришћењем информационе технологије до сада је посвећена на ширење идеје и пропаганду.

ПРОПАГАНДА ТЕРОРИСТА НИЈЕ ИСТО ШТО И САЈБЕР ТЕРОРИЗАМ

Терористи на разне начине користи сајбер простор за испуњење својих циљева али, ипак, свет још није доживео јасан сајбер терористички напад. Зато и даље не постоје унифициране дефиниције и сваки покушај остаје само у домену теорије.

Пре само једну деценију терористичке групе биле су ограничене могућношћу ПР маневрисања, у смислу да су само поједине могле да финансирају штампање новина, магазина, снимање и емитовање телевизијских и радио емисија. Данас, захваљујући интернету као глобалном медију свако може да покрене он-лајн магазин, да поставља видео и фото записе на сајтове или друштвене мреже. Не треба изгубити ни на тренутак из вида колико је интернет моћан медиј.

Било би апсурд порећи да терористи активно користе предности које им сајбер простор нуди. Терористичке групе користе сајбер простор да регрутују нове чланове, шире пропаганду, комуницирају, организују своје

[15] Roland Heickerö, „Cyber Terrorism: Electronic Jihad'', Strategic Analysis, 2014 Vol. 38, No. 4, page 564

активности. Познато је да је Осама бин Ладен комуницирао са члановима Ал Каиде преко лаптоп рачунара и шифрованих порука, а чак су организатори напада на Светски трговински центар 11. септембра комуницирали преко имејла[16]. С друге стране, тзв. Исламска држава направила је револуцију у коришћењу друштвених мрежа као што су Twitter, Facebook, Instagram, Youtube канали, како би ширила своју пропаганду већем кругу људи[17]. Међутим, пропаганда терориста не може да буде оквалификована као акт сајбер тероризам. Употреба популарних друштвених мрежа, постављање фотографија, видеа, вандализам на сајтовима (као што су промене у изгледу почетне странице), само су неки од активности које терористичке групе широм света користе као тактику. Интернет је изнедрио лакшу комуникацију терориста међусобно, са члановима, али и са јавношћу. На овај начин терористи могу да пренесу своју поруку и људима који у другој ситуацији никад не би ни обратили пажњу на њих и њихове циљеве. Исто тако, људи који су заинтересовани да доприносу раду терористичке групе (било финансијским донацијама, речима подршке или пак да се придруже борби) сада лакше могу да успоставе директан контакт.

Наведене активности само су неки од аспеката како терористи користе предности интернета као глобалног медија, али њихов циљ није уперен ка компјутерским системима[18]. Ове активности могу да изазову страх, терор, панику, могу надоградити сигурност на вишем нивоу, могу да имају политичку, верску и идеолошку позадину, али не могу директно изазвати физичко уништење, смрт људи, еколошку или финансијску катастрофу. Зато је неопходно да се направи разлика између директних терористичких акција са једноставном пропагандом.

Дакле, можемо закључити да терористи користе компјутер као помагач у њиховим активностима, без обзира на то да ли се то односи на пропаганду, регрутовање, дата мајнинг, комуникацију или у друге сврхе. Ипак, ове активности једноставно нису сајбер тероризам.

---

[16] M. Conway, Cyberterrorism and Terrorist 'Use' of the Internet, First Monday, 4. 11. 2002, Vol. 7, No. 11, http://firstmonday.org/issues/issue7_11/conway/ /pregledano 10. 9. 2016/

[17] Katarina Jonev, „Šta je sajber terorizam", http://www.politika.rs/sr/clanak/348284/Pogledi/Sta-je-sajber-terorizam

[18] Gabriel Weimann ''Cyberterrorism:The sum of All Fiers'',Studies in Conflict and Terrorism,28, Taylor&Francis Inc, 2005. Page 130.

Закључак

Постоји много различитих мотива за терористе да присегну ИТ алатима како би остварили своје циљеве. Сајбер тероризам као средство у тој борби је и више него користан јер напади могу потицати из било ког дела света, нису ограничени физичким границама, нападач може остати анониман, а при том да нанесе оштећење или уништење. Бојазан да терористи могу да се домогну злонамерног софтвера који може да се „ушуња" у рачунарске системе критичне националне инфраструктуре постоји и оправдан је. Сајбер напад великих размера може да има огромне последице.

Дебате о сајбер тероризму наставиће се и у будућности, али чињеница је да овај феномен представља глобални проблем и као такав захтева глобалну пажњу.

Државе су више него забринуте за своју безбедност у сајбер простору. Страх од напада који би могли угрозити функционисање виталне инфраструктуре, која се све више ослања на информационо-комуникационих технологија, расте. Зато су сајбер напади у врху приоритета у стратегијама националне безбедности као озбиљна претња која би могла угрозити државу. Апсолутни одбрана против тероризма и сајбер тероризма изузетно је тешка, па је неопходна међудржавна сарадња.

Литература

1. Anna-Maria TALİHÄRM Cyberterrorism: in Theory or in Practice? Defence Against Terrorism Review Vol.3, No. 2, Fall 2010
2. B. Foltz, Cyberterrorism, computer crime, and reality, Information Management & Computer Security, 15.03.2004, Vol. 12, No. 2
3. B. Collin, 'The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge', Paper presented at the 11th Annual International Symposium on Criminal Justice Issues, Chicago, September 23–26, 1997.
4. C. Wilson, Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress (RL32114), 2005
5. Center for Stretegic and International Studies ''Cybercrime,

cyberterrorism, cyberwarfare, Avertingand Electroinic Waterloo'', CSISM 1998.
6. Dorothy E. Denning ''Cyberterrorism'', Global Dialogue, 24.09. 2000
7. Denning Dorothy ''Activism, Hactivism,Cyberterrorism'', Networks and Netwars, John Arquilla, David Ronfelt, eds, RAND, 2001
8. Gabriel Weimann ''Cyberterrorism:The sum of All Fiers'',Studies in Conflict and Terrorism,28, Taylor&Francis Inc, 2005
9. Gábor IKLÓDY The New Strategic Concept and the Fight Against Terrorism: Challenges & Opportunities Defence Against Terrorism Review Vol.3, No. 2, Fall 2010
10. Jonathan A.Ophandt ''Cyber Warfere and the crime of sggression: the need for individual accountability on tomorrow's battlefield'' Duke Law & Technology Review, 2010.
11. Roland Heickerö ''Cyber Terrorism: Electronic Jihad'' Strategic Analysis, 2014 Vol. 38,No. 4
12. Потпуковник Марио Станковић, мајор Небојша Петровић, потпуковник др Ненад Димитријевић „Информациона безбедност и заштита тајних података у информационо- телекомуникационим системима", Нови гласник 1/2016,
13. M. Conway, Cyberterrorism and Terrorist 'Use' of the Internet, First Monday, 04.11.2002, Vol. 7, No. 11.