УДК 343.533::004
004.738.5.056.53
DOI: https://doi.org/10.5937/bastina32-38105

Прегледни рад

*Ивана Ж. БАЛТЕЗАРЕВИЋ**
Мегатренд универзитет, Правни факултет Београд, Република Србија

*Драган Љ. ТАНЧИЋ***
Институт за српскзу културу Приштина – Лепосавић

УТИЦАЈ ДИГИТАЛНОГ ОКРУЖЕЊА НА ШИРЕЊЕ САЈБЕР ТЕРОРИЗМА***

Апстракт: Развојем информационо-комуникационих технологија дошло је до убрзаног развоја друштва, међутим уз олакшање комуникације, пословања и забаве дошло је до појаве читавог низа проблема у погледу безбедности корисника у сајбер простору, али и самих држава. Сајбер криминал је постао учестала појава која наноси материјалну и нематеријалну штету корисницима друштвених медија који су често недовољно информисани о методама оваквих сајбер криминалаца. С друге стране, виртуелно окружење, омогућило је сајбер терористима да пренесу своје мотиве и активности из физичког простора у дигитални. На жалост, последице оваквог сајбер терористичког деловања нису ни мало мање девастирајуће него код традиционалних терористичких активности. Сакривени у дигиталном простору, терористи пропагирају своју политичку или религиозну идеологију, регрутују нове чланове и организују нападе, користећи, често са великим успехом, идентичне терористичке стратегије које су коришћене и пре појаве сајбер простора. Недостатак међународне сарадње, усаглашености законодавства, али и занемаривање сигурносних система нових уређаја, од стране стручњака из ове области, који функционишу уз помоћ информационо-комуникационих технологија створиће у будућности још плодније тле за наставак и развој оваквих криминалних активности. На жалост нису све државе мотивисане нити виде своје интересе у погледу сарадње у овој области, али разорни потенцијали сајбер криминала и сајбер тероризма на глобалном нивоу морају бити довољно јак фактор који ће потпуну међународну сарадњу у овој области поставити као императив.

Кључне речи: Информационо-комуникациона технологија, Сајбер простор, Сајбер криминал, Сајбер тероризам

УВОДНЕ НАПОМЕНЕ

Према Валтеру Лакуеуру тероризам подразумева нелегитимну употребу силе за постизање политичких циљева атаком на невине људе (Laqueur 1977). Торе Бјорго додаје да је тероризам скуп метода борбе који укључује употребу насиља

* Доцент, ivana.baltezarevic@gmail.com
** Редовни професор, научни сарадник, dragan_tancic@yahoo.com
*** Рад је написан у оквиру научноистраживачког рада НИО по Уговору склопљеним са Министарством просвете, науке и технолошког развоја број: 451-03-68/2022-14 од 17.01.2022. године и резултат пројекта Правног факултета, Мегатренд универзитета: Безбедносни изазови савременог друштва (ФПБИСД).

са предумишљајем, првенствено против небораца, како би се постигао психолошки ефекат страха на непосредне мете (Bjorgo 2005). Тероризам је био и вероватно ће остати један од највећих извора људских патњи и разарања у последњих неколико векова. Употреба оваквих екстремних облика насиља над обичним, невиним људима и одређеним групама, у циљу изазивања политичке потчињености, или премештања становништва и стварања радне снаге у освојеним територијама колонијалних сила, уништило је у прошлости читаве цивилизације и народе широм света. У двадесетом веку многе модерне државе биле су одговорне за смрт више од 200 милиона људи ван рата (Rummel 1994). Велики број невиних жртава убијен је за време злогласних кампања државног тероризма, попут Маовог и Стаљиновог великог терора, али за време владавине различитих диктаторских режима у Аргентини, Чилеу, Јужној Африци, Уганди, Сомалији, Индонезији, Ираку, Ирану и многим другим земаља. У двадесетом веку, за време великих ратова више милиона цивила било је убијено у кампањама „бомбардовања терором" осмишљеним са једноставним циљем - да поткопају морал, застраше становништво и изазову покорност. Насумична убијања невиних људи у циљу застрашивања остатка становништва била су и остала суштина терористичке стратегије (Grosscup 2006). Евген Виктор Валтер у циљу идентификовања основних карактеристика тероризма тврди да тероризам мора да укључи три кључна фактора: насиље којим се прети или које је усмерено на неку жртву; насилног актера који намерава да насиљем изазове терор код неког сведока који се генерално разликује од жртве; и треће, да насилни актер терорисањем сведока насиљем промени његово понашање. Пол Вилкинсон проширује ове видике и додаје да тероризам има за циљ стварање климе екстремног страха или терора који је усмерен на ширу публику од непосредних жртава насиља; да укључује нападе на насумичне и симболичне циљеве, и да у дословном смислу крши друштвене норме, изазивајући осећај беса код становништва и на крају, да се тероризам користи као средство којим се може утицати на политичко понашање (Wilkinson 1992).

Иако су информационо-комуникационе технологије омогућиле много лакшу комуникацију, забаву и пословање људима, такође су омогућиле и сајбер криминалцима да врше своје илегалне активности у дигиталном окружењу (Baltezarević–Baltezarević 2021). Модерно доба и развој технологије утицало је на многе аспекте друштва између осталог и на методе тероризма, које се све више дешавају у виртуелном окружењу, како за ефикасније регрутовање терористичких истомишљеника тако и за изазивање материјалне и нематеријалне штете и страха код невиних жртава. Појава нових медија омогућила је бржу глобалну комуникацију и намеће се као средство које ће готово у тренутку задовољити потребу за одређеном информацијом (Baltezarević-Baltezarević 2021). Управо такво окружење омогућава плодно тле за многе нелегалне, али и терористичке активности где сајбер терористи могу да нанесу велику материјалну и емоционалну штету дигиталним корисницима. О овом питању се нашироко расправља на међународном нивоу, али изгледа да сајбер криминалци увек проналазе нова креативна решења како би заобишли све безбедносне заштите како би извршили своје криминалне активности (Baltezarević-Baltezarević 2021).

САЈБЕР ТЕРОРИЗАМ У ДИГИТАЛНОМ ОКРУЖЕЊУ

Последњих двадесет година сајбер простор је постао центар истраживачких активности криминолога. Развојем интернета и његових софистицираних облика комуникације дошло је и до појаве сајбер криминала и сајбер тероризма (Yar 2005). Криминолози су схватили да у домену научног истраживања у овој области постоји велики јаз (Nhan-Bachmann 2010). Истраживања у овој области су спора, међутим постоји неколико уређених збирки и ауторских књига о сајбер криминалу које су криминолози написали чисто из криминолошке перспективе (Jewkes 2007). Нова дешавања на пољу сајбер криминала у дигиталном окружењу покренула су нову дисциплину под називом сајбер криминологија. Сајбер криминологија представља мултидисциплинарно поље које обухвата истраживаче из различитих области као што су криминологија, социологија, виктимологија, али и наука о интернету и генерално о рачунарству. Сајбер криминологију је могуће дефинисати као проучавање узрока злочина који се дешавају у сајбер простору, али и његовог разорног утицаја у физичком простору (Jaishankar 2007). Термин „сајбер тероризам" је настао 1980-их када га је Бери Колинс, виши научни сарадник на Институту за сигурност и обавештајне послове у Калифорнији, описао као једноставну конвергенцију сајбер простора и тероризма. Вашингтонски истраживачки центар за стратешке и међународне студије је 1998. године усвојио комбинацију термина (и дефиниција) сајбер простора и тероризма како би описао појаву употребе интернета у остваривању терористичких циљева (Tafoya 2011).

Према Дороти Денинг, сајбер тероризам се односи на незаконите нападе и претње нападима на рачунаре, мреже и информације које се у њима чувају, а које се спроводе да би се застрашила или принудила влада или грађани неке земље у остваривању политичких или друштвених циљева. Да би се квалификовао као сајбер тероризам, напад би требало да резултира насиљем над особама или имовином, или барем нанесе довољно штете да изазове страх. Напади који доводе до смрти или телесних повреда, експлозије, или изазивају тешке економске губитке били би добри примери. Озбиљни напади на кључне инфраструктуре могу се сматрати актима сајбер тероризма, у зависности од њиховог утицаја. Напади који ометају небитне услуге или који су углавном скупа сметња не би били окарактерисани као сајбер тероризам (Denning 2000).

Неколико научника који се баве науком о тероризму почело је да разматра модерни тероризам са више података и из мрежне перспективе. Две књиге Марка Сагемана: „Разумевање терористичких мрежа" из 2004. године, и „Џихад без лидера"из 2008. године, сматрају се најозбиљнијим достигнућима из ове области. Марк Сагеман оспорава конвенционална знања о тероризму, примећујући да је кључ за ефикасну одбрану од будућих напада темељно разумевање мрежа које омогућавају ширење новог облика тероризма (Sageman 2008). Сагеман је спровео велику студију у области сајбер тероризма и након интензивног прикупљања и анализе података које је прикупио из међународне штампе и судских расправа о скоро 200 важних џихадиста, Сагеман је успео да сагледа и понуди боље разумевање оваквих друштвених веза и њиховеидеолошке посвећености. Према њему, такве терористичке групе засноване на мрежи, карактеришу робусне мреже, широка географска дистрибуција и нејасне границе. У својој књизи из 2008. године, „Џихад без лидера",

Сагеман је наставио са систематском анализом своје детаљне базе података о терористима. Након анализе више од 500 терористичких чланова, описао је да процес радикализације који ствара мале, локалне, самоорганизоване групе у непријатељском станишту, које су повезане преко интернета, води до неповезане глобалне терористичке мреже, односно „џихада без лидера". Међу својим налазима, он је открио да су пре двадесет година интеракције лицем у лице биле чешће међу млађим припадницима џихада, док је након 2004. године, већина интеракција била заснована на интернету, а просечан члан имао је око 20 година. У складу са савременом еволуцијом информационих комуникација и технологије, интернет, али пре свега друштвене мреже, помажу радикалним исламистима у стварању глобалног, виртуелног терористичког друштвеног покрета (Sageman 2008).

Након Сагеманових студија, још неколико научника је испитало утицај интернета на ширење и радикализацију глобалног џихадистичког покрета. Међу њима се највише истиче Габријел Веман са одсека за комуникације Универзитета у Хаифи у Израелу, који је открио након осмогодишњег проучавања коришћења интернета од стране терористичких организација и њихових присталица да софистициране веб локације помажу овим организацијама у прикупљању средстава, регрутовању чланова, планирању и покретању напада и објављивању њихових застрашујућих резултата. Веман описује нове медије као средство за промоцију новог тероризма новој генерацији (Weimann 2006).

НОВЕ МЕТОДЕ САЈБЕР КРИМИНАЛА И ТЕРОРИЗМА

Усвајање технолошких иновација у великој мери односи се на лакоћу коришћења и њихову корисност за крајње кориснике и њихове организације. Након многих циклуса ових иновација, могло се очекивати да би захтеви сајбер безбедности дошли више у први план, али то очигледно није случај. Главни разлог је тај што се из ранијих циклуса технолошких иновација нису научиле лекције о сајбер безбедности па су се исте грешке понављале изнова (Averill-Luiijf 2010).

Јасно је да ће и сваки следећи циклус иновација у информационо-комуникационим технологијама резултирати новим претњама за крајње кориснике и наше друштво у целини. Стручњацима из ове области очигледно недостаје историјско разумевање претходних грешака у сигурном дизајну и ранијих лекција идентификованих у доброј пракси кодирања. Често су старе претње прерушене у нови изглед, што омогућава сајбер криминалцима, активистима, сајбер шпијунима и терористима да на неовлашћен начин уђу у системе засноване на информационо-комуникационим технологијама користећи слабости у валидацији улазних вредности и елемената протокола које узрокују неочекиване улазе. Такође, међу карактеристичним слабостима оваквих технологија треба напоменути и могућност сајбер напада додавањем хардверских модула који се сами конфигуришу у постојећем систему или мрежи који обезбеђују споредна врата. Треба нагласити да и недостатак технолошке писмености код великог броја корисника и њихово несвесно и несигурно управљање информационо-комуникационим технологијама такође омогућава сајбер криминалцима неометано деловање у дигиталном окружењу

(Babak и др. 2014). Кларк описује сајбер простор као нови „домен" сукоба, оперативно окружење у којем државни и недржавни актери могу да спроведу стратешке сајбер нападе против својих противника (Clarke 2009).

Могуће је дефинисати неколико области које ће у перспективи од стране сајбер криминалаца и терориста бити окарактерисане као „рањиве" и самим тим као погодне за извршавање оваквих сајбер криминалних дела. Међу њима су дигитални телевизори који су већ данас повезани са јавним мрежама и интернетом и као такви су атрактиван извор процесорске моћи за сајбер криминалце (како би на пример постали део ботнета). Такође, све већи број корисника тренутно надгледа и мења поставке температуре у свом дому или канцеларији даљински са свог паметног телефона. Што је свакако потенцијално занимљива опција за деловање сајбер криминала. Велики број система заснованих на информационо-комуникационој технологији користи се и у здравству за праћење здравља пацијената. Већ је било примера да су пејсмејкери и инсулинске пумпе хаковане преко њиховог бежичног интерфејса. На жалост, дизајнери ових уређаја нису узели у обзир да би хакери могли бити заинтересовани за манипулацију таквим системима, а погрешне поставке оваквих система могу имати опасне последице. Наравно, посебно је угрожен и финансијски сектор. Чипови за блиску комуникацију пружају нови облик идентификације и аутентификације власницима паметних телефона, што чини основу за бесконтактно микро плаћање корисника. Транспортни сектор и савремени аутомобили садрже огромну количину кодова у све већем броју електронских управљачких јединица. Ови „рачунари на точковима" надзиру све већи број сензора и контролишу и активирају многе покретаче од кочница до брисача ветробрана, од светала до система за избегавање судара. Сајбер криминал ће уследити и у овој области у догледно време (Babak и др. 2014). Сектори енергетике и воде за пиће ће формирати први паметни интерфејс између комуналних мрежа (као што су струја, гас, вода за пиће) и локалног комуналног система у оквиру имања (KrebsOnSecurity 2012). Како је сајбер терористима циљ да нападају критичну инфрастуктуру једне државе, заштита оваквих система се намеће као императив у будућности. Скоро сваки уређај у домаћинству ће имати интернет адресу, а паметни фрижидер, машина за прање судова, машина за прање веша и тако даље ће започети комуникацију са паметном мрежом и пронаћи најзеленије или најјефтиније време за коришћење енергије и воде. Дизајн таквих уређаја са очекиваним веком трајања од најмање 15 година не узима у обзир ажурирања сајбер безбедности. Уз слабу сигурност, паметни уређаји могу постати нова дистрибуирана платформа којом се напада преко информационо-комуникационог технолошког система, или путем паметне (енергетске) мреже (Bijlsma и др. 2013). Не треба изоставити и чињеницу да је тренутно на тржишту мобилни робот прве генерације. Очекује се да ће ови роботи постати део радне снаге у болницама и старачким домовима. Може се наслутити да ће се грешке у сајбер безбедности догодити у заштити комуникационих канала између робота и главне контролне станице при потврђивању команди роботу (Babak и др. 2014).

Сајбер терористи користе методе сајбер ратовања да би конвенционалном силом у суштини постигли исте циљеве (Bijlsma и др. 2013). Може се рећи да сајбер криминал и сајбер тероризам представљају пети домен, поред осталих домена рата:

копна, мора, ваздуха и свемира. То је медиј у коме се напади спроводе ради остваривања нечијих политичких, идеолошких или верских циљева, односно као злочини које је омогућила технологија (Holt 2012).

ЗАКЉУЧАК

Информационо-комуникациона технологија омогућава да се многа позната кривична дела, као што су преваре, изврше у невиђеним размерама и преко државних граница. Рачунари и подаци које они садрже предмет су криминалних активности и могу бити средство упада или „хакова" како би се угрозила њихова употреба и извукли или изменили вредни подаци. Транснационална природа сајбер криминала и сајбер тероризма, омогућава таквим актима да избегну конвенционалне интервенције органа за спровођење закона, чинећи тако уобичајене кривичноправне мере немоћним, осим ако је ефикасна сарадња између држава или нпр. приватних служби сајбер безбедности. Иако је разлика између сајбер криминала и сајбер тероризма заснована на мотиву корисна, често се не може увек уочити из самог чина. Сајбер криминалци су мотивисани низом циљева као што су пожуда, освета, авантура, похлепа или на неки други начин и дизајнирани су за личну корист, али сајбер терористи су обично мотивисани екстремистичким, идеолошким, или политичким циљевима, а њихови напади су осмишљени да изазову масовни страх у популацији. Непотребно је рећи да сами мотиви могу бити сложени, а политички циљеви се лако могу мешати са мање алтруистичким или идеолошким циљевима.

Неоспорно је да интернет и друштвене мреже постају ново „бојно поље" у коме се активности сајбер криминала и сајбер тероризма могу чак и делотворније обављати. Вероватноћа да починиоци оваквих криминалних радњи остану анонимни је велика, а самим тим је велика и могућност да остану неоткривени и несанкционисани. Могућности које су на располагању починиоцима оваквих криминалних радњи су превелике и стиче се утисак да ће у будућности бити још више простора за њихово деловање. На жалост, утисак је да је боља међународна сарадња у овој области (сарадња влада и полиције), као и усаглашавање законодавства представљају неопходност у циљу сузбијања ове појаве. Међутим, за сада, очигледно је да немају све земље исте интересе да до такве ефикасне међународне сарадње и дође у догледно време.

ЛИТЕРАТУРА

Akhgar- Staniforth- Bosco 2014: Akhgar Babak, Staniforth Andrew, Bosco Francesca. „Cyber Crime and Cyber Terrorism Investigator's Handbook". Syngress

Averill-Luiijf 2010: Bruce Averill, Eric A.M Luiijf. "Canvassing the cyber security landscape: why energy companies need to pay attention." J. Energy Security, May.

Baltezarević- Baltezarević 2021: Ivana Baltezarević & Radoslav Baltezarević. „Sajber bezbednost: izgradnja digitalnog poverenja." *Megatrend Revija*, Vol. 18 (4). pp. 269-280 UDK 343.533::004 DOI: 10.5937/MegRev2104269B

Baltezarević- Baltezarević 2019: Ivana Baltezarević & Radoslav Baltezarević. „Prikriveno oglašavanje u novim medijima." Baština, sv. 48, pp. 171-179. UDK 659.1 doi: 10.5937/bastina1948171B

Baltezarević- Baltezarević 2021: Radoslav Baltezarevic & Ivana Baltezarevic. "The Dangers and Threats that Digital Users Face in Cyberspace". *IPSI Transactions on Internet Research*, Vol. 17, No. 1, January 2021, pp. 46-52.

Bijlsma-de Kievit- van de Sluis- van Nunen- Passchier- Luiijf 2013: Tjerk Bijlsma, Sander de Kievit, Jacco van de Sluis, Ellen van Nunen, Igor Passchier, Eric Luiijf. „Security challenges for cooperative and interconnected mobility systems". In: Luiijf, E., Hartel, P. (Eds.), Critical Information Infrastructures Security, 8th International Workshop, CRITIS 2013, Amsterdam, Lecture Notes in Computer Science, vol. 8328. Springer, Heidelberg, pp. 1–15.

Bjorgo 2005: Tore Bjorgo. „Root causes of terrorism". Routledge

Clarke 2009: Richard Clarke. "War from cyberspace." *The National Interest* 104: 31-36

Denning 2000: Dorothy Denning. "Cyber terrorism: The Logic Bomb versus the Truck Bomb." Global Dialogue, 2(4), 29-37.

Grosscup 2006: Beau Grosscup. „Strategic Terror: The Politics and Ethics of Aerial Bombardment." London: Zed Books.

Holt 2012: Thomas Holt. "Exploring the Intersections of Technology, Crime, and Terror." Terrorism and Political Violence, 24(2), 337-354. doi:10.1080/09546553.2011.648350

Jaishankar 2007: Jaishankar, K. "Cyber criminology: Evolving a novel discipline with a new journal." International Journal of Cyber Criminology, *1*(1), 1–6.

Jewkes 2007: Yvonne Jewkes. "*Crime online."* Cullompton, United Kingdom: Willan.

KrebsOnSecurity 2012: KrebsOnSecurity. "FBI: Smart Meter Hacks Likely to Spread." https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ (Pristupljeno: 01.01.2022).

Laqueur 1977: Walter Laqueur.„Terrorism" London: Weidenfeld and Nicholson

Nhan-Bachmann 2010: Johnny Nhan&Michael Bachmann. "Developments in cyber criminology." In M. Maguire & D. Okada (Eds.), *Critical issues in crime and justice: Thought, policy, and* practice (pp. 164–183). Thousand Oaks, CA: Sage Publications.

Rummel 1994: Rudolph Joseph Rummel."*Death by Government*." New Brunswick, NJ: Transaction Books.

Sageman 2008: Marc Sageman. "Leaderless Jihad," University of Pennsylvania Press, Philadelphia, Pennsylvania

Tafoya 2011: William L. Tafoya. "Cyber Terror." FBI Law Enforcement Bulletin (FBI.gov), November 2011 attributes the coining of the term to Barry C. Collin.

Weimann 2006: Gabriel Weimann. "Terror on the Internet: The New Arena, the New Challenges," US Institute of Peace Press, Washington, DC

Wilkinson 1992: Paul Wilkinson. "International Terrorism: New Risks to World Order". In John Baylis and Nick Rengger (eds) *Dilemmas of World Politics: International Issues in a Changing World*, London: Clarenden Press: 228–57.

Yar 2005: Majid Yar. "The novelty of 'cyber crime': An assessment in light of routine activity theory." *European Journal of Criminology*, 2(4), 407–427.

Ivana Ž. BALTEZAREVIĆ
Dragan Lj. TANČIĆ

THE INFLUENCE OF THE DIGITAL ENVIRONMENT ON THE SPREAD OF CYBER TERRORISM

Summary

The development of information and communication technologies has led to the accelerated development of society, but with the facilitation of communication, business and entertainment, there have been a number of problems regarding the security of users in cyberspace, but also the states themselves. Cybercrime has become a frequent occurrence that causes material and non-material damage to social media users who are often insufficiently informed about the methods of such

cybercriminals. On the other hand, the virtual environment has enabled cyber terrorists to transfer their motives and activities from physical to digital space. Unfortunately, the consequences of such cyber-terrorist activities are no less devastating than in traditional terrorist activities. Hidden in the digital space, terrorists propagate their political or religious ideology, recruit new members and organize attacks, using, often with great success, identical terrorist strategies that were used before cyberspace. The lack of international cooperation, harmonization of legislation, but also the neglect of security systems of new devices by experts in this field, which function with the help of information and communication technologies, will create even more fertile ground for the continuation and development of such criminal activities. Unfortunately, not all countries are motivated or see their interests in terms of cooperation in this area, but the destructive potential of cybercrime and cyber terrorism at the global level must be a strong enough factor to make full international cooperation in this area imperative.

Key words: Information and communication technology, Cyberspace, Cyber crime, Cyber terrorism

Рад је предат 6. фебруара 2022. године, а након мишљења рецензената, одлуком одговорног уредника *Баштине*, одобрен за штампу.