УДК 343.326:004.738.5
323.285
343.95:343.341
DOI: https://doi.org/10.5937/bastina33-44435

Прегледни рад

*Радослав В. БАЛТЕЗАРЕВИЋ**

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

ТЕРОРИЗАМ У ДИГИТАЛНОМ ОКРУЖЕЊУ

Апстракт: Распрострањеност дигиталних технологија и њихова моћ да повезују милијарде људи широм света, омогућила је савременом друштву ефикаснију комуникацију, доступност информација, обављање посла, али и забаву. Међутим, све је више примера у којима се оваква могућност злоупотребљава за сајбер криминалне активности, међу којима је свакако и сајбер тероризам. Активностима традиционалног тероризма, терористи покушавају да изазову анксиозност код становништва, бирајући мете насумично или селективно, над којима се врши насиље, са намером да служе као пример осталим члановима друштва. Овакво изазивање страха је управо средство терористичких појединаца и група, којима се жели извршити притисак на владу и ширу јавност да се испуне њихови захтеви. У последње време све је више примера у којима се овакве активности селе (са више или мање успеха) у дигитално окружење. Сајбер тероризам је средство којим се шири радикална идеологија, пропаганда, регрутовање истомишљеника, али и организовање сајбер терористичких напада. Предност коју терористички активисти виде у коришћењу оваквих метода, свакако јесте могућност да остану анонимни и лако се сакрију у пространству сајбер света. Сајбер криминалци се лако прилагођавају и налазе нове методе вршења сајбер насиља, што мора бити позив владама да се синхронизованим напорима регулише законодавство, али и оформе стручни тимови који ће на време идентификовати, спречити и адекватно санкционисати овакве криминалне активности и заштитити своје становништво и критичну инфраструктуру.

Овај рад жели да приближи и предочи информације академској заједници, али и стручњацима из области сајбер тероризма који им могу помоћи да унапреде стратегије препознавања и одбране од оваквих сајбер активности. Основни циљ овог рада је да анализира прикупљене информације из доступне научне литературе и да понуди нове смернице како би се у блиској будућности овакве активности свеле на минимум.

Кључне речи: дигитално окружење, тероризам, сајбер тероризам, терористичке организације.

УВОДНЕ НАПОМЕНЕ

Дигиталне технологије, као саставни део савременог друштва, олакшавају комуникацију, пословање и утичу на квалитет живота људи. Међутим, са друге стране, дигитално окружење се све више користи за разне врсте криминалних активности

* Редовни професор, r.baltezarevic@gmail.com
** Доцент, ivana.baltezarevic@gmail.com

са којим се суочавају корисници интернета, пословни системи, али и саме државе (Baltezarević, Baltezarević 2021). Традиционални тероризам претходних пет векова изазива панику и може имати девастирајуће ефекте по становништво и државу, а намера терориста је да скрену пажњу и изврше притисак на владу и широку јавност у циљу испуњења сопствених захтева. Дигитално окружење у модерном друштву постаје ново бојно поље оваквих појединаца и организација у вршењу различитих видова криминалних активности.

Сајбер тероризам треба посматрати одвојено од терористичке употребе интернета, која укључује аспекте као што су комуникација (James 2005), регрутовање, финансирање, организовање физичких напада, пропаганда (такође у облику „хактивизма"), подстицање на тероризам, иизвињење тероризма (Ronen 2010). У исто време, одређене сајбер операције (нпр. упади у базе података критичне инфраструктуре ради прикупљања информација о рањивим циљевима) могу да допринесу сајберекстремистима, али сами по себи нису акти сајбер тероризма. Научници, предлажу поделу сајбер-напада на употребу интернета у циљу изражавања идеја и комуникације, на злоупотребу (ометање или компромитовање веб-сајтова или инфраструктуре), на увредљиву употребу (коришћење интернета за проузроковање штете или се за крађу) и коначно на сајбер тероризам (Conway 2003).

У пракси је много примера активности сајбер криминала које наносе велике штете компанијама, појединцима, али и државама. Данас су многе државе свесне неопходности доношења јаснијих закона у овој области и адекватнијег идентификовања и санкционисањасвих активиста оваквих незаконитих сајбер криминалних радњи (Baltezarević - Baltezarević 2021). Успостављањем мреже свих мрежа (www), интернет је створио могућност за свакога да шири информације без трошкова и углавном без икакве контроле садржаја. Терористи стога користе интернет не само за покретање напада, већ и за борбу против „рата идеја" (Giacomello 2004). Сајбер тероризам се сматра кривичним делом, извршеним употребом компјутера и телекомуникационих средстава, које доводи до уништавања и/или прекида услуга како би се створио страх у датој популацији, а у циљу утицања на владу или становништво да се повинује одређеној политичкој, друштвеној или идеолошкој агенди (Pujari 2016).

Број сајбер напада је повећан последњих година и учинио је да се сајбер безбедност више брине за људе, нације и планету. Друштвени медији омогућавају комуникацију са људима који имају налоге на друштвеним мрежама. Ширење информација путем друштвених медија је брзо, лако и супериорније у односу на било који други медиј. У свету је око 2,67 милијарди људи користило друштвене медије и очекује се да ће их ускоро бити 3 милијарде (Kirichenko и др. 2018). Лака доступност широком аудиторијуму је мотив кога су терористичке организације свесне и недостатак дигиталне писмености, код једног дела становништва, још више олакшава спровођење сајбер терористичких активности. Иако је ова појава све присутнија у свету, ипак се њене последице не могу мерити са оним које изазива традиционални тероризам. У годинама које следе, онлајн терористички активисти, који се константно адаптирају новонасталим условима, спроводиће све софистицираније сајбер терористичке методе, што мора натерати владе свих земаља да се усагласе и сарађују у погледу откривања, елиминисања и санкционисања оваквих аката.

ТЕРОРИЗАМ: ДЕФИНИЦИЈА И КОНЦЕПТУАЛИЗАЦИЈА

Задатак дефинисања тероризма је компликован, али је апсолутно неопходан да би се развило довољно разумевање овог феномена. Сложеност дефинисања тероризма има много аспеката и произилази из разних страна које су користиле насиље да би изазвале терор. У литератури се може пронаћи више од 100 различитих дефиниција „тероризма" (Record 2003), што је индикатор потребе да се овај појам прецизније дефинише и елиминише конфузија. Израз „тероризам" означава предумишљајно, политички мотивисано насиље које против неборбених циљева врше поднационалне групе или тајни агенти, обично са намером да утичу на публику. Са друге стране, термин „међународни тероризам" означава тероризам који укључује грађане или територију више од једне земље. „Терористичка група" је термин који означава сваку групу која практикује међународни тероризам или има значајне подгрупе (US Code, Title 22 у 2656f(d)).

Тероризам се генерално сматра методом поновљене насилне акције која изазива анксиозност код становништва, коју користе тајни појединачни, групни или државни актери из идиосинкратичних, криминалних или политичких разлога, при чему, за разлику од атентата, директне мете насиља нису главнемете. Непосредне људске жртве насиља се генерално бирају насумично или селективно (симболичне или репрезентативне мете) из циљне популације које служе као генератори порука. Комуникациони процеси засновани на претњи и насиљу између терористичких организација, жртава и главних циљева се користе да би се манипулисало главном метом (публиком), претварајући је у мету терора, мету захтева илиметупажње, у зависности од тога да ли се првенствено жели постићи застрашивање, принуда или пропаганда (United Nations Office on Drugs and Crime 2022). Многе концептуализације тероризма приближавају се идеји да он укључује унапред смишљено, политички или идеолошки мотивисано (Hoffman 1998) екстремно насиље (Tilly 2004) против симболичних мета (Crenshaw 2001) или цивила (Rodin 2004) од стране организације која настоји да утиче на државу или државе путем застрашивања публике (Primoratz 2004).

Тероризам је одувек био један од највећих извора људских разарања и патњи. Употреба различитих облика насиља над обичним становништвом била је мотивисана изазивањем политичке потчињености у новонасталим националним државама, али у неким случајевима и стварањем радне снаге у освојеним колонијалним територијама. Током двадесетог века, модерне државе биле су одговорне за смрт скоро 200 милиона људи ван рата. Велики број невиних жртава убијен је током злочиначких кампања државног тероризма (попут Стаљиновог великог терора, Маовог великог скока Напред, као и за време владавине различитих диктаторских режима у Уганди, Сомалији, Чилеу, Аргентини, Јужној Африци, Индонезији, Ирану, Ираку итд. (Rummel 1994). У двадесетом веку, током великих ратова, више милиона цивила убијеноје у атомским нападима и у терористичким кампањама осмишљеним да поткопају морал и изазову покорност. У већини случајева насумичним убијањем одређених група становништва (за пример) изазивањем страха, утицало се на друге, што се може сматрати суштином терористичке стратегије (Grosscup 2006).

Тероризам је нешто у шта се могу укључити и државе и недржавни актери (Chomsky 2001). Међутим, многе концептуализације уопште не праве разлику између недржавног и државног насиља (Schmid, Jongman 1988). Да би се једно дело означило као државни тероризам, његови елементи морају бити у складу са елементима недржавног тероризма, међутим, као што је горе наведено, данас још увек не постоји консензус о томе како би тероризам требало дефинисати (Cooper 2001).

Историја је показала да су жртве државног антитероризма увек биле знатно веће од жртава насталих недржавним тероризмом. Државни тероризам као далеко распрострањенији и деструктивнији од недржавног, још увек није добио пажњу коју заслужује у оквиру безбедносних студија или студија о тероризму и међународних односа, што је изненађујуће, с обзиромна то дасу академска јавност, али и активисти за људска права дужи низ година шире проучавали репресију државе (Jackson 2008).

Развојем дигиталних технологија терористи су добили нове могућности организовања терористичких активности. Највећа предност коришћења оваквих метода је то што им омогућава да остану анонимни (уколико желе) у сајбер простору, али још увек сајбер тероризам није преузео примат од традиционалног тероризма из простог разлога што му недостаје „ефекат театралности", којим се преноси порука путем оваквих напада и врши притисак на јавност и владе на испуњење захтева ових терористичких група.

САЈБЕР ТЕРОРИЗАМ – НОВИ ИЗАЗОВИ САВРЕМЕНОГ ДРУШТВА

Дигиталне технологије су значајно допринеле савременом друштву и постало је евидентно да су предности интернета велике, али само када се интернет схвати као алат, а не као тренутна замена стварног живота (Baltezarević, Baltezarević 2016). Међутим, предности интернета познате су и појединцима и организацијама, које све чешће користе способност технологија да допру до широке публике и тиме им је олакшана намера да прошире своје идеологије коришћењем пропагандног садржаја, али и да регрутују истомишљенике или организују терористичке сајбер активности.

Постоје многе карактеристике тероризма које се могу спроводити путем интернета, иако је ово првенствено информативни и комуникациони медиј који омогућава знатно проширени домет и далеко бржу комуникацију. Тероризам се посматра као политички мотивисан чин и стога захтева публицитет и форум комуникације. Кључне области експлоатације у савременој терористичкој употреби су пропаганда, регрутовање, радикализација, комуникација и истраживање. Интернет омогућава малим групама или појединачним терористима прилику да дођу, врло лако, буквално до милиона људи. Једна од карактеристика интернета, која највише обећава, је та што даје глас многима који нису били у могућности да купе или привуку пажњу медија (Weimann 2006).

У последње време, неколико аутора који се баве науком о тероризму почело је да разматра модерни тероризам са више података и из мрежне перспективе. Деценијама је нова врста тероризма (сајбер тероризам) тихо прикупљала редове у свету. Америчка способност да остану несвесни нових покрета престала је 11. септембра 2001. године. Исламски фанатици у глобалном селефијском џихаду (насилни, препородитељски друштвени покрет чији је део и Ал Каида) циљају на Запад, али њихове

операције немилосрдно убијају и хиљаде људи свих раса и религија широм света. Марк Сегман оспорава конвенционалну мудрост о тероризму, примећујући да је кључ за ефикасну одбрану од будућих напада темељно разумевање мреже која омогућава ширење новог тероризма (Sageman 2008). Званичне веб странице владиних организација поред пропаганде малог обима, за хакере поседују потенцијал да изазову праву панику. Чест сценарио је такав да терориста квари веб локацију за националну безбедност и саветује људима да напусте град због цурења хемикалија. Ако ову информацију прими штампа или довољно људи, оваква лажна порука може да добије легитимитет и изазове панику, са небројеним жртвама које у журби покушавају да оду из града. Ова врста напада има релативно малу вероватноћу да ће успети, јер други облици упозорења то не би подржали. Повећање популарности нових медија заиста омогућава већи потенцијал за ову врсту сценарија јер је ова област још увек недовољно регулисана и може недостајати одговорност да се потврди извор који би традиционални медији имали. Друштвени контактни медији као што је Твитер могу ненамерно ширити лажне информације и бити схваћени као оригинални (COE DAT Strategic Communications Workshop 2009). Срећом, многи напади до данас нису резултирали насиљем и распрострањеним страхом који су неопходни за сајбер тероризам. Дистрибуирани напади ускраћивања услуге узроковали су, у најбољем случају, привремене сметње на јавним веб страницама, које су често трајале само неколико минута. Хаковање веб страница обично се огледа у постављању антизападних текстова и фотографија, што се може сматрати онлајн панданом фарбању зграде спрејом. Корисници који посећују ове веб сајтове током напада су можда искусили извесну фрустрацију јер су сајтови били привремено недоступни или су приказивали увредљиве поруке. Без обзира на преувеличане тврдње о сајбер тероризму од стране неких стручњака за компјутерску безбедност, људи који су покушавали да приступе хакованим веб локацијама вероватно нису осећали страх од насиља и физичког застрашивања повезаног са тероризмом (Denning 2012). Сајбер напади су веома скупи, а често терористичким групама недостају и вештине за успешне сајбер нападе. Деструктивни потенцијал физичких напада може се лакше материјализовати, док сајбер тероризму недостаје театралност конвенционалних напада и стога је мање привлачан терористичким групама (Conway 2014).

У својој књизи „Терор на интернету", Габријел Веман (Weimann 2006) са одсека за комуникације Универзитета у Хаифи у Израелу, известио је о свом осмогодишњем проучавању коришћења интернета од стране терористичких организација и њихових присталица. Његовом студијом откривено је да софистициране веб локације помажу терористичким организацијама у прикупљању средстава, регрутовању чланова, планирању и покретању напада, али и објављивању њихових застрашујућих резултата. Веман описује интернет као нове медије за промоцију сајбер тероризма новим генерацијама публике. Због свеприсутности и размера интернета, предложио је удруживање техничких и језичких ресурса за праћење екстремизма на интернету за земље чланице ЕУ. Такође је предложио ширење умерених мишљења веродостојних муслиманских научника и лидера веб мишљења и охрабрио садржај на друштвеним медијима усмерен на кориснике као средству супротстављања радикализацији и насиљу (Weimann 2006).

За терористичку организацију изузетно је важно да саопшти своје ставове, циљеве и амбиције. Иако је у ранијим временима то било изузетно тешко, интернет сада нуди могућности за лаку комуникацију и могућ утицај на медије и јавност у целини (Brunst 2008). Стога није ни чудо што данас скоро свака организација „подземља" има своју веб страницу и број оваквих страница је у сталном порасту. Терористичке веб странице могу се користити у различите сврхе. Могуће је циљати на посебну публику, нпр. дизајном у стилу цртаног филма и дечијим причама чиме се таргетирају деца (Weimann 2006). Терористичке веб странице нису ограничене на представљање само сопствених гледишта. Уместо тога, могу се користити и за претњу непријатељу или за ширење пропаганде. Нарочито ако се претње износе уз помоћ мултимедијалне технологије, што привлачи пажњу штампе и јавности. Из тог разлога су развијене компјутерске игрице, нпр. једна под називом „Потрага за Бушом" која омогућава интернет корисницима да „убију" америчког председника Буша. Оглашавање на мрежи и слични начини стицања новчаног прихода уз интернет услуге постали су профитабилан пословни модел за многе. За терористе и терористичке групе то није тако лако, посебно ако се на веб страници налази експлицитни терористички садржај. Ипак, неке организације су почеле да користе свој сајт не само за ширење информација, већ и као извор прихода за финансирање и прикупљање средстава. Неки веб сајтови се користе, осим за своје првобитне намене, и за продају компакт дискова, мајица, значки, застава или књига. Други начин финансирања терористичких активности је давање инструкција корисницима интернета како да донирају новац (Weimann 2004).

Проблематично питање у вези са намером тероризма иза акције на интернету је, међутим, то што се често не може открити. Ако, на пример, хакерски напад са циљем затварања важних система на аеродрому буде успешан, терористи ће вероватно имати интерес да то јавно објаве и да изазову страх код становништва. У овом случају, лако је одредити терористе јер су извор дела сајбер криминала, као и основни план, јасни. Међутим, ако се хакерски напад изврши у нади да ће се добити информација о аутомобилској рути важне особе, то би се могло држати у тајности како се не би угрозили будући планови за бомбашки атентат на ту особу (Brunst 2008).

Општи тренд држава усмерен је на то да се повећа безбедност путем онлајн надзора. Ово се остварује деловањем служби задуженим за међународну безбедност, као и деловањем страних обавештајних служби (Buchanan 2020), али и настојањем да се доследно примењују закони како унутар појединачних држава тако и на међународном нивоу (Eijkman – Weggemans 2013). Док владе и медији непрестано дистрибуирају информације о сајбер претњама, прави сајбер напади који резултирају смрћу и повредама остају углавном ствар холивудских филмова или теорије завере. У ствари, претећи сценарији од великих поремећаја у сајбер домену, изазвани злонамерним актерима, остали су, за сада, само то – сценарији (Cristiano 2018). Сајбер тероризам у друштвеним медијима се користи за прање новца, крађу идентитета, онлајн преваре, сајбер нападе и друго (Broadhurst и др. 2017). Срећом, сајбер тероризам, у насилном смислу, никада се није догодио и до данас нема доказа да су терористи прибегли компјутерима да убију или деструктивно поремете друштва. Већина научника мисли да је мало вероватно да ће то и десити у скорије време (Lee, Stuart 2015).

ЗАКЉУЧАК

Може се закључити да ће се опасност од сајбер терористичких напада стално повећавати, јер како људи постају зависни од интернета, самим тим повећавају се и могућности сајбер терористичких напада. Можемо бити сигурни да ће терористи настојати да искористе предности дигиталних технологија и да ће се непрестано повезивати и прилагођавати, посебно имајући у виду да сајбер простор нуди атрактивне могућности за новине и изненађења. Главни разлог зашто терористичке организације остају углавном лоше опремљене или неспособне да изведу ефикасне сајбер нападе је због равнотеже трошкова и користи.

У овом тренутку, трошкови ресурса, прикупљања обавештајних података и организовања тако софистицираних операција премашују тренутне могућности оваквих активиста за спровођење софистицираних или ефикасних сајбер напада. Међутим, могуће је регрутовати способније актере из „подземног тржишта" за компјутерске експлоатације и на тај начин се лако могу повећати ограничени капацитети сајбер терориста. Стога је вероватно да ће се ниво оваквих претњи променити у наредној деценији. Сајбер тероризам је показао, у сваком случају, велики потенцијал и како не би ескалирао неопходно је развити стратегије превенције и реаговања на међународном нивоу. Континуирана међународна сарадња и партнерства влада и заједнице у превенцији сајбер тероризма, заједно са наменским тимовима за реаговање у хитним случајевима биће од суштинског значаја. Мере које могу повећати извесност хапшења или ометање активности преступника и друге ефикасне противмере као што су јачање атрактивних, али рањивих циљева и побољшање сајбер способности особља за безбедност информација такође су генерално корисне у повећању ризика за сајбер терористе и друге криминалне актере.

ЛИТЕРАТУРА:

Baltezarević, Baltezarević 2016: Vesna Baltezarevic, Radoslav Baltezarevic. „The internet and virtual "reality". In Proceedings International Conference, *Technology + Society Future*, 2016, Podgorica, Montenegro. Transition to a new society, Montenegrin Academy of Sciences and Arts, World Academy of Art and Science, ALL European Academies (ALLEA), European Academy of Sciences and Arts, Podgorica, Montenegro: Pro File, pp. 193-200.

Baltezarević, Baltezarević 2021: Ivana Baltezarević, Radoslav Baltezarević. „Sajber bezbednost: izgradnja digitalnog poverenja." *Megatrend Revija*, Vol. 18 (4). pp. 269-280.

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.

Broadhurst, Woodford-Smith, Maxim, Sabol, Orlando, Chapman-Schmidt, Alazab 2017: Roderic Broadhurst, Hannah Woodford-Smith, Donald Maxim, Bianca Sabol, Stephanie Orlando, Ben Chapman-Schmidt, Mamoun Alazab. „Cyber Terrorism: Research Review: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology (June 30, 2017)." SSRN: https://ssrn.com/abstract=2984101 or http://dx.doi.org/10.2139/ssrn.2984101.

Brunst 2009: Phillip Brunst. „Use of the Internet by Terrorists – A Threat Analysis." In Centre of Excellence– Defence Against Terrorism (Ed.), Responses to Cyber Terrorism (pp. 34–60). Amsterdam: IOS Press.

Buchanan 2020: Ben Buchanan. „The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics". Cambridge, MA: Harvard University Press

Chomsky 2001: Noam Chomsky. „US: A leading terrorist state." Monthly Review 53: 10–19.

COE DAT Strategic Communications Workshop May 2009 https://www.tmmm.tsk.tr/wsreports.html (Приступљено: 06.05.2022)

Conway 2003: Maura Conway. „Terrorism and IT: Cyberterrorism and Terrorist Organisations". Online 6 (paper prepared for presentation at the International Studies Association Annual International Convention in Portland, Oregon).

Conway 2014: Maura Conway. *„Reality Check: assessing the (un)likelihood of cyberterrorism."* In: Chen, Tom, Jarvis, Lee and Macdonald, Stuart, (eds.) Cyber Terrorism: Understanding, Assessment and Response. Springer, New York, pp. 103-122.

Cooper 2001: H. H. A. Cooper. „Terrorism: The Problem of Definition Revisited". *American Behavioral Scientist*, 44: 881–93.

Crenshaw 2001: Martha Crenshaw. „Terrorism." In: International Encyclopedia of the Social & Behavioral Sciences. Amsterdam, the Netherlands: Elsevier, pp. 15604–15606.

Cristiano 2018: Fabio Cristiano. „From Simulations to Simulacra of War: From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises." *Journal of War & Culture Studies* 11, no. 1: 22–37.

Denning 2012: Dorothy E. Denning. „Stuxnet: What Has Changed?" *Future Internet* 4, no. 3: 672-687. https://doi.org/10.3390/fi4030672

Eijkman, Weggemans 2013: Quirine Eijkman, Daan Weggemans. „Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability?" *Security and Human Rights* 23, no. 4 (2013): 285–96.

Giacomello 2004: Giampiero Giacomello. „Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism." *Studiesin Conflict & Terrorism*, 27(5), 387–408.

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

Hoffman 1998: Bruce Hoffman. *„Inside Terrorism."* New York: Columbia University Press.

Jackson 2008: Richard Jackson. „The Ghosts of State Terror: Knowledge, Politics and Terrorism Studies." *Critical Studies on Terrorism*, 1 (3): 377–92.

Kirichenko, Radivilova, Carlsson 2018: Lyudmyla Kirichenko, Tamara Radivilova, Anders Carlsson. „Detecting cyber threats through social network analysis: short survey."CoRR abs/1805.06680

Lee, Stuart 2015: Jarvis Lee and Macdonald Stuart. „What Is Cyberterrorism? Findings from a Survey of Researchers." *Terrorism and Political Violence* 27, no. 4 (2015): 657–78

Lewis 2005: James Lewis. „The Internet and Terrorism". *Proceedings of the ASIL Annual Meeting*, 99, 112-115. doi: 10.1017/S0272503700071196

Primoratz 2004: Igor Primoratz. „What is terrorism"? In: I. Primoratz (ed.) Terrorism: *The Philosophical Issues*. New York: Palgrave Macmillan, pp. 15–30.

Pujari 2016: Amaresh Pujari. „Cyber Terrorism. World Wide Weponisation!" TN Police Sesquicentennial Anniversary Souvenir.

Record 2003: Jeffrey Record. *„Bounding the Global War on Terrorism."* Carlisle Barracks: Strategic Studies Institute, US Army War College.

Rodin 2004: David Rodin. „Terrorism without intention." *Ethics* 114: 752–771.

Ronen 2010: Yaël Ronen. „Incitement to Terrorist Acts and International Law". *23LEIDEN J. I NT' L L.,* 645, 654.

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

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

Schmid, Jongman 1988: Alex Peter Schmid, Albert J. Jongman. *„Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature."* (revised from 1983 ed.) New Brunswick, NJ: Transaction.

Tilly 2004: Charles Tilly. „Terror, terrorism, terrorists." *Sociological Theory* 22(1): 5–13.
United Nations Office on Drugs and Crime. 2022: Definitions of Terrorism. https://www.unodc.org/unodc/en/terrorism/index.html (Приступљено: 06.05.2022)
US Code, Title 22, y 2656f(d).
Weimann 2004: Gabriel Weimann. „Cyberterrorism: How Real is the Threat?" [Electronic Version]. Special Report (United States Institute of Peace), 119.
Weimann 2006: Gabriel Weimann. „*Terror on the Internet: The New Arena, the New Challenges*," US Institute of Peace Press, Washington, DC.

Radoslav V. BALTEZAREVIĆ
Ivana Ž. BALTEZAREVIĆ

TERRORISM IN THE DIGITAL ENVIRONMENT

Summary

The spread of digital technologies and their power to connect billions of people around the world, has enabled modern society to communicate more efficiently, access information, do business, but also have fun. However, there are many examples in which this possibility is abused for cybercriminal activities, among which is certainly cyber terrorism. Through the activities of traditional terrorism, terrorists try to provoke anxiety in the population, choosing targets randomly or selectively, against which violence is committed, with the intention of serving as an example to other members of society. Such incitement to fear is precisely the means of terrorist individuals and groups, who want to put pressure on the government and the general public to meet their demands. Recently, there are more and more examples in which such activities are moving (with more or less success) to the digital environment. Cyber terrorism is a means of spreading radical ideology, propaganda, recruiting like-minded people, but also organizing cyber terrorist attacks. The advantage that a terrorist activist sees in using such methods is certainly the possibility to remain anonymous and easily hide in the cyber world. Cybercriminals easily adapt and find new methods of committing cyberbullying, which must be a call to governments to regulate legislation in a synchronized effort, but also to form expert teams that will identify, prevent and adequately sanction such criminal activities and protect their population and critical infrastructure.

This paper seeks to bring closer and present information to the academic community, but also to experts in the field of cyber terrorism that can help them improve strategies for recognizing and defending against such cyber activities. The main goal of this paper is to analyze the collected information from the available scientific literature and to offer new guidelines in order to reduce such activities to a minimum in the near future.

Key words: digital environment, terrorism, cyber terrorism, terrorist organizations.

Рад је предат 2. октобра 2022. године, а након мишљења рецензената, одлуком одговорног уредника *Баштине*, одобрен за штампу.