Ивана Лукнар

САЈБЕР ТЕРОРИЗАМ

Мере за сузбијање и превенција

Проф. др Ивана Лукнар

САЈБЕР ТЕРОРИЗАМ
Мере за сузбијање и превенција

Београд, 2022.

Проф. др Ивана Лукнар

САЈБЕР ТЕРОРИЗАМ

Издавач
Институт за политичке студије, Београд

За издавача
Др Живојин Ђурић

Рецензенти
проф. др Ивана Дамњановић
Академик Драган Симеуновић
др Живојин Ђурић

Пословни секретар
Смиљана Пауновић

Дизајн корица
Марија Стевановић

Лектура
Светлана Вујчић

Прелом и штампа
Ситопринт, Житиште

Тираж
100

Монографија је настала у оквиру научноистраживачке делатности Института за политичке студије из Београда, суфинансирана од стране Министарства просвете, науке и технолошког развоја Републике Србије.

САДРЖАЈ

ПРЕДГОВОР

Последњих година дошло је до значајног пораста насилних инцидената, нарочито оних који су поткрепљени расним, етничким, политичким и идеолошким мотивима. Терористички напади који су засновани на ксенофобији, расизму и другим облицима нетолеранције, у име религије или политичког уверења постају главна брига међународне заједнице, а тероризам један од најактуелнијих безбедносних изазова савременог доба. Бројни ризици, као што су: употреба хемијског, биолошког, радиолошког или нуклеарног оружја или сродних материјала, употреба савремене информационо - комуникационе технологије од стране недржавних актера у терористичке или друге криминалне сврхе, представљају једну од највећих брига данашњице. Да би спречила и супротставила се овој претњи, Међународна заједница настоји да подигне свест о овом проблему; да боље познаје и разуме феномен тероризма, као и факторе који у знатној мери утичу на његово настајање и даље „мутације".

Обзиром на разноврсност појавних облика савременог тероризма и његову мултикаузалну природу сарадња на међународном нивоу намеће се као примарна, витална компонента за спречавање и борбу против тероризма. Поменута сарадња се остварује кроз: размену информација, доказа и изјава сведока или захтева за међународну правну помоћ у виду изручења окривљеног или осуђеног, преузимања и уступања кривичног гоњења, извршења кривичне пресуде или неки други облик међународне правне помоћи.

Глобализација је омогућила повезивање света у једну целину, односно повезивање екомоније, технологије, информација и различитих култура преко националних граница. Док је развој савремених информационих и комуникационих технологија (у даљем тексту скраћено: ИКТ) изменио свакодневни живот људи, начин комуницирања и пословања у готово свим аспектима савременог живота. Брз и интензиван развој технологија, све бржи и приступачнији интернет омогућавају готово свакоме да постане учесник у светским догађањима и да прати дешавања на светској сцени. Поменути развој савремене технологије мења форму друштвено - политичког активизма те он поприма онлај (*online*) одредницу.

У новоформираној реалности под утицајем здравствене кризе интернет је као никада пре постао примарно оруђе за одржавање комуникације и сарадње међу људима широм света на сва три

нивоа друштвеног постојања: 1. макро (глобални, међународни); 2. мезо (национални, локални) и 3. микро ниво (лични). Савремене информационе технологије поред тога што пружају бројне погодности истовремено остављају простор за различите врсте злоупотреба. На индивидуалном (личном) нивоу научно - технолошка револуција изнедрила је нову форму идентитета, тзв. онлајн идентитете, који доводе у питање негдашње друштвене улоге и идентитете. „Контакти лицем у лице“ постају све ређи, а познанства виртуелна. Формира се нови облик друштвених заједница (виртуелне заједнице) и сајбер култура. Сајбер простор пружа могућност да се идентитети мултиплицирају, што може негативно да се одрази на појединца и изазове кризу и расцеп идентитета. Ово је нарочито интензивирано крајем 2019. године када је због пандемије коронавирусом уследила нова реалност услед препоручених мера вакцинације и социјалног дистанцирања.

Глобално гледано, друштво никада није било зависније од интернета, онлајн платформи и дешавања на „мрежи“ које су биле не само препоручена, већ у појединим земљама и једина дозвољена средства комуникације, пословања и социјалног живота. Терористичке организације се служе погодностима интернета и сајбер простора у различите сврхе: да би пласирале своје информације, ширили идеје и утицај у медијима, организовале нападе, за регрутовање нових чланова итд. Управо таква ситуација оставља простора код појединца за идентификовање са онлајн терористичким групама и малициозна деловања у сајбер простору. Тако с једне стране наведени услови погодују ширењу терористичких аспирација путем интернета, док истовремено с друге стране јавни сектор све више ослања своје пословање на информационе и комуникационе технологије због чега постаје рањивији од сајбер тероризма и других сајбер претњи. Узевши у обзир чињеницу да процеси који обликују свакодневницу потпомажу брзи развој и примену технологија, како у развијеним тако и у неразвијеним регионима света, може се рећи да је сајбер тероризам изазов садашњости, али и облик тероризма који ће бити актуелан у будућности.

Терористичке претње и напади у сајбер простору нису само проблем безбедности појединих држава, обзиром да представљају претњу по глобалну безбедност у најширем смислу. Различите државе примењују различите мере и методе како би се одбраниле и заштитиле од ове врсте тероризма. Које су то адекватне мере и методе које државе могу да усвоје како би се заштитиле од сајбер тероризма? Које су основне карактеристике сајбер тероризма, односно његове

основне специфичности у односу на друге врсте сајбер напада? Који фактори значајно утичу на стварање и појавни облик сајбер тероризма? Какво је њихово међусобно дејство и динамика? Које савремене политике, превенција и мере се примењују у борби против сајбер тероризма у свету и у Републици Србији? Управо у овој књизи кренули смо у потрагу за одговорима на поменута, као и многа друга питања. Монографија је проистекла из дорађене докторске дисертације уприличене за објављивање на тему, "Борба против кибертероризма у стратешким документима Републике Србије", одбрањене на Факултету политичких наука, Универзитета у Београду.

Поред обраде саме теме, био је изазов бавити се сајбер тероризмом и због правописних недоумица. Многи термини преузети су из енглеског језика, а у свету, па и код нас, не постоји усаглашеност око начина писања основних појмова.[1] Потешкоће нису проистекле само из језичке баријере, већ и због веома малог броја радова који се конкретно баве овом тематиком. Мада се у ни у једној националној стратегији термин сајбер тероризам конкретно не помиње, овај термин ипак износим одвојено, обзиром да су у актуелној „Стратегији развоја информационог друштва и информационе безбедности за период 2021 - 2026. године", термини: сајбер простор, сајбер безбедност, сајбер одбрана, сајбер претње, написани одвојено.

Захваљујем се свим људима добре воље који су подржали објављивање монографије.

Аутор

1 На пример, на сајту Савета Европе термин cybersecurity је написан спојено. Види: https://www.enisa.europa.eu/ На сајту НАТО, термини: cyber defence, cyber threats, cyber attacks су написани одвојено, док је термин cyberspace написан спојено. Види: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en. У Немачкој и УК термин cyber security је написан одвојено. Види: у Немачкој: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=FF6FBEBEAF4CB782B6D2E9A796F33399.1_cid364?__blob=publicationFile&v=3.У УК:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/937702/6.6788_CO_National-Cyber-Security-Strategy-2016-2021_WEB3.pdf. Домаћи аутори такође нису усаглашени по питању писања поменутих термина. Неки аутори пишу спојено сајбертероризам, сајберпростор, сајбертерористички напад. Види: Дамњановић, И. (2009). Постоји ли сајбертероризам, *Политичка ревија*, бр. 1, 237 - 254. Док неки аутори пишу одвојено. Види: Вулетић, Д. (2017). Употреба сајбер простора у контексту хибридног ратовања, *Војно дело,* вол. 69, бр.7, 308 - 325.

1. ПРОЦЕСИ КОЈИ ОБЛИКУЈУ САДАШЊОСТ

Научно - технолошка револуција

Једна од најзначајнијих промена које су се догодиле током XX - тог века је развој информационе технологије. Друштво се трансформисало из индустријског у информационо. За разлику од претходног друштва у којем су примарни ресурси били материја и енергија, у информационом друштву су примарни ресурси знање и информације. Технолошке творевине као што су: рачунари, рачунарске мреже, интернет, *Twitter*, *Facebook, YouTube* паметни телефони и остало, прихваћени су великом брзином у готово свим сегментима друштва. Савремене информационе и комуникационе технологије представљају неизоставни део свакодневнице без чије примене су пословање и приватни живот постали готово незамисливи.

Научно - технолошка револуција подразумева интегрисање научног и технолошког знања у готово све аспекте људске делатности. Она је неуједначеним темпом у већој или мањој мери захватила читав свет. Научно - технолошки развој и иновације у области информационих и комуникационих технологија омогућили су глобално умрежавање, лаку доступност и брзу размену информација без обзира на реалну просторну удаљеност. Умрежавање друштва омогућило је брз пренос информација широм света (Кастелс, 2000), толико да је „посреди продубљивање и убрзавање светске међузависности у свим друштвеним аспектима“ (Хелд, 2003, 48). Међутим, нису сви светски региони подједнако укључени у информациону револуцију због разлика као што су: степен развоја, економска стабилност, технолошке могућности и др.

Отворене системе карактерише флуидност, променљивост, динамичност, као и велика могућност развоја. Технолошки прогрес омогућио је да комуникација буде мултидимензионална и да се одвија у различитим правцима просторно и временски неограничено. Ово подразумева да савремена друштва нису више везана за свој географски положај, државу или нацију у истој мери као и претходна, јер постоје у сајбер простору кроз системе комуникација као „систем мрежа знања и информација“ (Кастелс, 2000). Савремени свет је саткан од информација, слика, знакова и симбола (Miller, Matusitz, O'Hair& Eckstein, 2008). Технолошки развој није донео промене само у начину информисања, него је знатно изменио функционисање целокупног друштва и његових кључних националних и међународних структура, и изменио начин пословања и живљења.

Интернет нуди могућности за мобилизацију и оснаживање друштвено искључених и мање привилегованих појединаца и група. Јер, савремене технологије олакшавају приступ појединцу да претражи и лако пронађе друштвену групу, политички субјект или покрет који је у складу са његовим интересовањима и ставовима, независно од локалних расположивих садржаја. На тај начин су „нове технологије побољшале комуникацију и поверење у друштвене покрете и мобилизацију чланова“ (Della Porta, 2012, 49). Информационе и комуникационе технологије су поједноставиле комуникацију у савременом друштву и пружају бројне могућности појединцима и групним актерима да изразе своје ставове, промовишу идеје, искажу апел или незадовољство постојећим системима моћи, критикују или промовишу политичке идеје и др. На тај начин се друштвено - политичка арена смешта у онлајн (сајбер) простор, који је, као што Сасен примећује, постао „далеко конкретнији простор за друштвене борбе од национално политичког система“, наводећи даље да поменута ситуација олакшава „појаву нових типова политичких субјеката, који постоје изван формалног политичког система“ (Sassen, 2002, 382). Појављује се сајбер активизам, односно нова врста активизма који подразумева употребу нових технологија за подстицање расправа на оне теме које су политички дискутабилне и проблематичне, јер наилазе на отпор у реалном свету. Интернет нуди алтернативне садржаје, стога постаје интересантан различитим друштвено - политичким актерима. На пример, активисти за родну равноправност се интензивно служе интернетом у политичке сврхе, да укажу на неравноправност, експлоатацију и контрадикције између „мушких“ и „женских“ послова како би повећале видљивост проблема у јавности и могућност за ослобађање и еманципацију од родног угњетавања (Khamis, 2015; Everett, 2004; Schuster, 2013). Савремени терористи такође обављају различите активности посредством интернета: да остваре међусобну комуникацију и промовишу своје идеје или пошаљу поруке мржње, или да пошаљу слику учињених дела насиља свету како би изазвали панику код што већег броја људи. Неоспорно постоји вишеструка веза између тероризма и интернета. Употребу интернета од стране терориста можемо поделити у две категорије:

1) „употреба интернета ради комуникације – подразумева ширење пропаганде, кампање психолошког ратовања, интерну комуникацију и радикализовање регрута ширењем порука мржње;

2) инструментална употреба интернета - подразумева онлајн

едукације терористa, „виртуелне кампове“ за обуку будућих нападача“ (Weimann, 2015, 24).

Научно - технолошка револуција изнедрила је нове форме организованог криминала и нове форме терористичких организација. Дакле, ни починиоци међународног криминала (тероризам или организовани криминал), такође нису остали имуни на примену савремених информационих и комуникационих технологија. Савремене ИКТ постале су значајно средство за вршење криминалних дела и њихово међусобно организовање. Некадашње криминалне организације су биле строго хијерархијски уређене, док савремене криминалне организације одликује флексибилност и мрежна структура са неколико центара моћи и велика мобилност чланова. Савремене ИКТ и глобализација омогућиле су да поједине криминалне активности добију глобалне размере (Selley, 2003).

Савремена информациона и комуникациона технологија је један од најзачајнијих елемената који на макро нивоу обликује друштвене токове. Међутим, због сложености и двострукости ефеката развоја и употребе савремених информационих и комуникационих технологија јавност, правно - економске, друштвене и безбедносне науке су пред великим изазовом да реше питање сајбер безбедности. Разнолика примена ИКТ у готово у свим сферама друштвеног постојања и утицај који оне тренутно врше на готово сваки сегмент друштвеног постојања, будуће промене које ће њена употреба неминовно изнедрити свакодневно нас подсећају на хитно разматрање тренутних изазова, али и евентуалних будућих проблема. Велики су изгледи да ће сајбер тероризам да постане популарнија претња у будућности. На то нас упућују: интензивна, готово неухватљива динамика развоја ИКТ, растућа потреба у свету за све већим бројем високо квалификованих стручњака из ове области, релативно ниски трошкови имплементације и примене савремених ИКТ и бројне могућности за извршење сајбер напада. Једино добро познавање и разумевање савремене ситуације може да доведе до адекватног реаговања надлежних органа и правног система, ефикасног откривања и доказивање кривичних дела која спадају у овај облик криминалитета.

Глобализација

Глобализација је свепрожимајући процес који је трансформисао различите земље света. То је феномен који се не дешава негде "напољу", него се одвија управо "овде" и снажно утиче и захвата скоро све аспекте савременог живота. Томе је допринела, поред глобализације и научно - технолошка револуција; превасходно развој интернета који „повезује удаљена места на такав начин да локална збивања уобличавају догађаји који су се одиграли хиљадама километара далеко и „vice versa" (Гиденс, 1998, 69). Дакле, то је сложени процес који карактеришу динамичност и вишеструкост ефеката о којима пишу савремени мислиоци. Нагар и остали аутори примећују да глобализација истовремено доводи до инклузије и ексклузије у економији, култури и политици (Nagar, Lawson, Mc Dowell & Hanson, 2002, 260). У савременој литератури постоји неколико различитих начина дефинисања и изучавања глобализације.

Према теоријском приступу разликујемо: скептике, хиперглобалисте и трансформационисте (Хелд, 2003; Bauman, 1998). Први правац размишљања чине скептици, који сумњају у постојање целокупног процеса и виде „глобализацију као мит" (Волерстин, 2003), или не поричу њено постојање, али сматрају да је мит то да овај процес нема алтернативу и представља „нови вид светске доминације" (Бурдије, 1999, 39). Тако поједини аутори дефинишу глобализацију као да она „није ништа друго до реколонизација у новом руху" (Neeraj, 2001, 6 - 7). Други приступ размишљања чине хиперглобалисти који наглашавају ефекте глобализације у свим друштвеним сферама (било позитивне било негативне). Отуда глобализацију виде као: „интеграцију светске економије" (Gilpin, 2001, 364), „развој глобалних финансијских тржишта, раст транснационалних корпорација и њихова све већа доминација над националним економијама" (Сорос, 2003, 13). Трећи приступ чине аутори који се појмом глобализације служе да објасне трансформацију друштвених промена крајем XX и почетком XXI века – трансформационалисти. За њих је карактеристично то што глобализацију виде као „историјску трансформацију" (Albrow, 1996, 88) која је довела до промена „у до сада невиђеном степену" (Friedman, 1999, 7) и до те мере интензивирала друштвене односе широм света „на начин да се локални догађаји уобличују на основу догађаја који се дешавају миљама далеко и обратно" (Гиденс 1998, 21); у економији је утицала на „начин стицања прихода и егзистенције" и омогућила „ширење слободног тржишта капитализма до сваке

земље на свету“ (Friedman, 1999, 8); „у политици губитак степена локалне контроле, а у култури губитак достигнућа колективитета“ (Mittelman, 2000, 6).

Као што примећује Јејтс (Yeates, 2001) међу савременим мислиоцима постоје дијаметрално супротна мишљења о феномену глобализације. Из тога је проистекла подела на поборнике (глобалофоличаре) и критичаре глобализације (антиглобалисте = глобалофобичаре и алтерглобалисте). Присталице глобализације наводе њене предности и указују на развој и позитивне ефекте поменутог процеса. Неки аутори се позивају превасходно на економске промене које је изнедрила глобализација, као што су: давање превласти слободном тржишту, ограничавање улоге државе на неопходан минимум, либерализација трговинских токова, међународна мобилност капитала, радне снаге, информација, технологије и идеја. Други аутори је сматрају решењем за многе социјалне проблеме. На пример Каул наводи: “глобално изједначавање очекивања, које је настало као резултат унапређења у образовању, глобалној комуникацији и транспорту, који су водили ширењу и све већем прихватању норми и вредности као што су правичност, једнакост и људска права – грађанска и политичка, као и економска и социјална” (Kaul, 1994, 2). Такође, неки поборници глобализације указују на позитивне промене у друштвеној структури, односно стварање слоја врхунских менаџера и научне елите, државних функционера и политичко - војне елите, смањење инфлације и убрзани технолошки напредак који доводе до раста продуктивности и БДП-а (Deardorff & Stern, 2001). Критичари глобализације указују на њене противречности и позивају се на недостатке као што су: „глобално уништавање животне средине, експанзивно освајање мање развијених нација западним социо - културним моделима и све јачи социо - економски притисци да се прилагоди компетицији на светском нивоу“ (Hengsbach, 1997, 182 - 195). Они глобализацију сматрају главним узроком бројних социјалних проблема као што су: сиромаштво (Katz, 2004), растући јаз између оних који имају и оних који немају (Гиденс, 2003, 598 - 599; Жоа & Шулер, 2005, 256 - 259), незапосленост (Carter, Schwartz & Norris, 2008), миграције (Silvey, 2009), пренасељеност градова услед масовног напуштања села, употреба дроге, разарање породице (Милић, 2001), организовани криминал, трговина људима и др.

Дакле, аутори нуде различите дефиниције глобализације у зависности од тога шта им је у фокусу. Односно, у зависности од тога да ли се глобализација поима као процес: „незадржив и неповратан

процес интеграције култура, тржишта и државних заједница, који је достигао незабележен ниво“ (Вулетић, 2006, 11), или пројекат утицајних група које желе да успоставе светску доминацију и даље ширење капитализма кроз економску либерализацију и политичку дерегулацију. Џон Грej и Емануел Тод разликују два модела глобализације: асиметрични - овај модел глобализације је антагонистички и неоимперијални (Gray, 1998) и асоцијативни - овај модел је неантагонистички, социјалдемократски (Todd, 2003). Лесли Склер такође говори о два модела глобализације: капиталистичком и социјалистичком (Sklair, 2013).

Земље у развоју, углавном постсоцијалистичке земље су своју транзицију базирале на добровољном задуживању код међународних фондова (ММФ, Светска банка и др.), што доводи до осиромашења народа и омогућава строгу контролу над државама дужницима. Друштва у транзицији се орјентишу на остварење профита, што даље узрокује процват сиве економије, корупције, организованог криминала и нелегалног капитала. Као што примећује Стиглиц “ММФ не само да је учинио врло мало како би спречио кризу него је и погурао политике дерегулације, укључујући либерализацију тржишта капитала и финансијских тржишта, које су допринеле настанку кризе и њеном брзом ширењу по свету” (Стиглиц, 2013: 247). Онемогућен је хармонични природни поредак, јер се постојано продубљује јаз између развијеног и неразвијеног дела света, односно света богатих и сиромашних, а принцип једнакости постаје управо оно што разједињује људе. Отуда, као што Франсес (Frances, 2004) примећује сиромашне прожима хронична економска рањивост и несигурност због којих они усвајају краткорочне стратегије преживљавања, које их ограничавају тако да они остају у зачараном кругу сиромаштва без готово икакве перспективе и могућности да напредују и остваре своје потенцијале. Дакле, различити аутори дијаметрално различито гледају на глобализацију. Као што наводи Јејтс (Yeates, 2001) једни глобализацију виде као решење бројних социјалних проблема, а други је сматрају основним узроком истих. Постојећа ситуација се прелама са макро на микро ниво и доводи до „кородирања карактера“ (Sennett, 1998) услед опадања поверења, лојалности, радне етике и посвећености.

Пандемија COVID - 19

Поред претходно наведених несигурности пандемија COVID - 19 вирусом појачала је тензије које су проистекле из страха за живот људи, али и опстанак савремене економије. Здравствена криза се прелила на економију, након што се због претње вирусом COVID - 19 свет закључао, што је даље произвело застој у кретању капитала, али истакло употребу информационих и комуникационих технологија у први план. Примену савремених ИКТ најбоље илуструје рад од куће који је препоручена врста рада за време пандемије јер „омогућава појединцу мање времена проведеног на путовања и више времена за породицу, а послодавцу већу продуктивност, мање трошкове због уштеде простора“ (Baruch, 2000, 38).

Пандемија COVID - 19 вирусом је интензивирала онлајн активности и мултиплицирала евентуалне онлајн претње и злоупотребе. Таква ситуација ствара негативан утицај на онлајн безбедност. За свеобухватно тумачење и разумевање новонастале ситуације потребно је: 1) поседовање минималног нивоа знања неопходног за обављање предложеног типа комуникације путем информационих и комуникационих технологија за време пандемије. У неким земљама то је био једини дозвољени облик комуникације за време закључавања (lock down - a); 2) афирмисаност – несумњиво је развој ИКТ донео савременој цивилизацији бројне бенефите. Међутим, не смемо да заборавимо да поменути развој има два лица, односно поред поменутих бенефита и повећан број криминалних онлајн активности и оних који желе да злоупотребе интензивнију употребу интернета, компјутера и осталих паметних уређаја за време пандемије; 3) разумевање реалности у којој је вирус изненада погодио свет и захтевао хитно реаговање од стране светских влада који су се за време првобитног шока насталог услед ванредне ситуације и изолације ослањали на размену информација у сајбер простору и ИКТ инфраструктуру; 4) препознавање рањивости ИКТ инфраструктуре је значајан корак у обезбеђивању њене сигурности и ефикасности; 5) разматрање потенцијалне штете коју би евентуални сајбер напад учињен од стране терориста могао да узрокује; 6) решавање – пружање заштите у сајбер простору од различитих врста сајбер напада; 7) свесност претње и ограничења услед тешкоћа за праћење технолошких предности и недостатака, јер се технологија развија много брже од своје примене; 8) тежња кроз активну међународну сарадњу за откривање и развој најбољих стандарда и пракси у борби против сајбер тероризма и сајбер криминала; 9) усаглашеност

међународне заједнице о растућем броју малициозних активности и претњи у сајбер простору током пандемије; 10) препознатљивост значаја и ургентности за достизање сајбер безбедности како на индвидуалном, тако и на институционалном нивоу (Luknar, 2020b, 32).

Буровс и Енгелке (Burrows & Engelke, 2020, 12 - 14) разматрају утицај пандемије COVID - 19 вирусом и помињу три могућа сценарија. Први сценарио говори о значајном убрзању економске кризе. У земљама у развоју расте ниво сиромаштва, јер пандемија негативно утиче тако што убрзава деглобализацију. Потврђен је спор економски раст готово свуда у свету до средине 2020 - их. Тензије на међународном нивоу се заоштравају и „постоји потенцијал за отворени сукоб између Сједињених Држава и Кинеско - Руског савеза“ (Burrows & Engelke, 2020, 12). Други сценарио је јачање позиције Кине, која је за време пандемије нагнула геополитичку равнотежу у своју корист. Мада држава није у потпуности опорављена од пандемије, политичко руководство Кине у пандемији види прилику да ради на јачању меке моћи кроз пружање помоћи, давање повољних кредита и инфраструктурних пројеката државама у Азији, Африци и Латинској Америци, па и на Балкану. Трећи, сценарио је „нова ренесанса“, који подразумева проналазак заједничких интереса у борби против климатских промена и будућих здравствених криза.

Миграције

Савремено друштво карактеришу локалне и међународне миграције становништва због многобројних разлога (посла, образовања, породичних разлога, туризма, преживљавања) интензивније него икада у прошлости (Табела 1). Присуство миграната и њихово кретање је фундаментална демографска, друштвена, културна и економска динамика која обликује друштвени контекст, како локално, тако и глобално. Међутим, пандемија COVID - 19 је изненадила свет, који је неспремно дочекао епидемију. Нису све државе показале подједнаку спремност за ублажавање негативних последица епидемије, без обзира на степен развијености. Неке државе ће се суочити са тежим дугорочним директним и индиректним последицама. Напори за ефикасно обуздавање и ублажавање COVID - 19 пандемије су кључно утицали на миграцију.

Табела 1. Глобални тренд миграција (Migration Data Portal, 2021)

Година	Број миграната у милионима
1990	153
1995	161,3
2000	173,2
2005	191,4
2010	221
2015	248
2020	280,6

Као и у многим другим кризама, мигранти су посебно рањива друштвена група. Њихова способност да избегну инфекцију, добију адекватну здравствену негу и изборе се са осталим економским, социјалним и психолошким утицајима пандемије COVID – 19 зависи од низа различитих фактора који су често у вези са њиховим миграционим статусом. Аутори (Liem et al.,2020) наводе следеће факторе: животне и радне услове миграната, недостатке или постотак уважавања њихове културне разноликости, језика, ксенофобија, њихово ограничено локално знање и мреже, њихов приступ правима и ниво укључености у заједнице домаћина. Специфична рањивост миграната углавном проистиче из њихове: класе, расе и статуса. Мигранти су углавном заступљени у дискриминисаним мањинама, остварују ниске приходе и сусрећу се са недостатком права на

здравствену и социјалну заштиту, суочени су са константним страхом од стигматизације и / или хапшења и депортације.

Укупан број миграната на глобалном нивоу средином 2020. године износио је 280, 6 милиона, од тога: САД 50, 6 милиона, Немачка 15, 8 милиона, Саудијска Арабија 13, 5 милиона, Руска Федерација 11, 6 милиона и Велика Британија 9, 4 милиона (Migration Data Portal, 2021). Субошић и Васиљевић (Лукнар) указују да актуелне миграције на европском тлу имају негативне последице међу којима нарочито издвајају:

1. поновна успостава граничне контроле унутар „шенгенског" простора,
2. успоравање промета људи, роба и услуга,
3. могућност инфилтрације терориста међу мигрантима,
4. раст јавних трошкова услед прихвата и збрињавања миграната, односно спречавања њиховог доласка у поједине земље (жичане ограде, појачано ангажовање полиције, ангажовање војске и др.),
5. одсуство солидарности и нарушавање поверења међу државама чланицама Европске уније, као и између држава чланица и држава кандидата за чланство у Унији,
6. раст незапослености,
7. смањење плата и прихода,
8. пораст сиве економије,
9. ксенофобија,
10. раст могућности конфликта између домицилног становништва и миграната." (Субошић, Васиљевић (Лукнар), 2017, 87). Мигранти су нарочито погођени кризом. Једино се инклузивном праксом и пружањем помоћи у заштити и промовисању права, здравља и благостања, може омогућити појединим заједницама да у друштву добију ефикасније одговоре на ову кризу и смање ризик од будућих.

Климатске промене и енергетска криза

Иако је пандемија COVID – 19 ставила у други план климатске промене, климатска криза и даље не јењава. Након незапамћеног пада од 5, 4 процента у 2020. години, глобална емисија угљен - диоксида враћа се на нивое пре појаве COVID - 19, и концентрација антропогеног гаса који ствара ефекат стаклене баште (GHG) наставиће да расте у атмосфери. Упркос паду у 2020. години, према подацима ИЕА (International Energy Agency), глобалне емисије CO2 остале су на 31,5 Gt, што је допринело да CO2 достигне највећу икада просечну годишњу концентрацију у атмосфери од 412,5 делова на милион у 2020 – око 50% више него када је индустријска револуција почела (IEA, 2021). Предвиђања су да ће у наредне две деценије глобално загревање прећи 1, 5°C уколико не дође до тренутног брзог и великог смањења емисије штетних гасова у атмосферу. Решавање климатског проблема захтева брзо и континуирано смањење емисија и сарадњу на међународном нивоу (United Nations Environment Programme, 2021).

Немарно опхођење према природи довело је до деградације животне средине. Све чешће смо сведоци бројних поплава, разорних ветрова и земљотреса широм света. Обе кризе, и климатска и здравствена криза која је изазвана пандемијом COVID - 19 деле заједничке карактеристике. Обе су настале као производ немарне људске активности, а њихови ефекти су блиски јер крајње угрожају људске животе. Здравствена криза се прелила у економску, док су климатске промене постојећу кризу само додатно утврдиле. Екстремне климатске промене су повећале потражњу за енергентима и њихову потрошњу, нарочито гаса због хладније зиме и топлијег лета (ради расхлађивања). Поплаве су негативно утицале на производња угља у Индонезији и Колумбији. Климатске промене су се такође негативно одразиле и на рад хидроелектрана, у Бразилу је смањења производња струје, а услед недостатка ветра и промена ваздушних струјања ветрењаче на Северном мору мање производе струје. Ни нагле климатске промене, ни пандемија нису биле неочекиване, а ипак их је свет дочекао неспремно.

Развијене економије и тржишта у развоју се знатно шире и фокусирају на прелазак на зелену економију, производњу чисте енергије и на улагања у природни капитал. Скоро 90 процената улагања у опоравак и нискоугљеничну потрошњу чини седам земаља: Република Кореја, Шпанија, Немачка, Велика Британија, Кина, Француска и Јапан. Према последњим подацима до маја 2021.

године, Француска, Немачка, Канада, Финска, Норвешка и Данска се могу сврстати у „лидере“ зеленог опоравка. Уједињено Краљевство, Шпанија и Шведска се такође високо котирају према извештају УН за очување животне средине (United Nations Environment Programme, 2021, XXVII). Угрожене нације са ниским приходима заостају далеко више него напредне економије.

Економска криза и сиромаштво

Глобализација је несумњиво олакшала начин живљења, али не за све светске земље и њихове становнике подједнако. Појединци или друштвене групе сусрећу се са различитим проблемима који онемогућавају, отежавају или угрожавају њихове могућности да остваре своја права или задовоље фундаменталне људске потребе.

Један од проблема је сиромаштво. Светска банка, Међународни монетарни фонд, Светска трговинска организација и друге глобалне институције намећу своју моћ тако што нуде финансијску помоћ у виду кредита земљама које су у развоју. Међутим, у пракси је потврђено да су на тај начин многе домаће економије упале у „дужничко ропство". Јер, нису сви принципи применљиви на истоветан начин код различитих националних економија. Отуда, Сорос указује да ММФ „не располаже методологијом за разликовање између здравих и нездравих економских политика" (Сорос, 2003, 89). Даље, делом или у целости демократски принципи се не примењују и не поштују у пракси. Богати имају различите могућности да се изборе за политике које им одговарају било лобирањем или корупцијом и на тај начин очувају или повећају постојеће стање неједнакости (Li, Squire & Zou, 1998).

Савремени капиталисти широм света поједине секторе производње измештају у друге зоне светске економије које су исплативије због јефтине радне снаге и других услова пословања. На тај начин мигранти из руралних предела по први пут улазе на тржиште рада и обављају послове који им пружају повољније услове и вишу зараду од претходне коју су примали за пољопривредне послове, дешава се „убрзана деруралиазација" (Волерстин, 2003, 105).

Упркос томе што су нека истраживања (Dollar & Kraay, 2001; Ferreira, 1999) потврдила да глобализација може да допринесе смањењу сиромаштва, друга истраживања су потврдила да је поменуто смањење сиромаштва врло скромно у поређењу са оствареним стопама раста (Vandemoortele, 2002). Јер, нужно је тумачити сваки доходак засебно, односно удео који остварују сиромашни припадници средњег слоја и богати у укупном дохотку (Табела 2). Мада генерално глобализација доноси корист, она штети најугроженијима и најсиромашнијима (Lundberg & Squire, 2000).

Табела 2. Укупна неједнакост дохотка у времену и простору (Piketty, 2015, 264)

	мала неједнакост (у Скандинавији 70-80.)	умерена (Европа 2010)	велика (Европа 1910, САД 2010.)
1% најбогатијих	7	10	20
следећих 9%	18	25	30
следећих 40%	45	40	30
половина друштва која је најсиромашнија	30	25	20

Јаз између богатих и сиромашних може се тумачити са глобалног аспекта и на нивоу једне државе. Земље можемо да поделимо у три категорије: „богате земље, носиоце глобализације и неглобализоване земље“ (Dollar & Kraay, 2001). Објашњење и разумевање савремених економских токова је готово немогуће без разумевања принципа либеларне економије и мултинационалних компанија. Мултинационалне компаније су важан глобални друштвени актер, које свој рад заснивају на принципима неолибералне економије, који су „изнад добробити заједнице, здравља радника, здравља становништва, мира, заштите средине или државне безбедности” (Мандер, 2003, 316). Односно, мултинационалне компаније се воде искључиво сопственим интересима и остварењем добити. Отуда ове глобалне институције поседују моћ да инвестирају по сопственом избору и на тај начин поспешују глобалну неједнакост и сиромаштво, тако што улажу у жељене регионе света, док друге избегавају. На тај начин се одржава сиромаштво већ сиромашних и још више продубљује јаз између оних који имају моћ и диктирају услове и оних који ту моћ немају. То потврђује и позната „теорија пређеног пута“ (Mahoney, 2000).

Сиромаштво се најчешће дефинише као материјална депривација – лишеност, недостатак или ускраћеност новчаних средстава за нормалан живот. Међутим, то је мултидимензионалан феномен који поред тога што значи недостатак ресурса, основних животних услова и потрепштина укључује и социјалну димензију. Јер, подразумева немогућност учествовања у активностима „које су уобичајене или барем широко одобраване или прихваћене у друштву којем припадају” (Townsend, 1979, 31). Оно што је карактеристично за сиромаштво је субјективни осећај незадовољства који настаје због дискрепанције између реалних потреба, очекивања и стварних могућности за њихово реализовање. Неки аутори виде сиромаштво

и искљученост као синониме (Abrahamson, 1995), док други истичу разлике имеђу материјалне и социјалне депривације (Townsend, 1987). У литератури сиромаштво се своди на једну димензију - финансијску (материјалну), док је искљученост мултидимензионална и поред недостатка финансијских средстава подразумева и депривираност у остваривању права и разних животних могућности као што су: становање, образовање, политичко одлучивање, социјалне везе, запослење и др.

Глобализација, пандемија, глобална економска криза, климатска и енергетска криза сузиле су могућности националних економија да се одупру сиромаштву. Глобални поредак је испреплетан систем моћи. Развијене земље света се утркују за позицију технолошког лидера и набавку енергената. Тензије се у кризним ситуацијама заоштравају. Због широког дијапазона могућности које савремене информационо-комуникационе технологије нуде (одашиљу поруке широком аудиторијуму, производе ефекте најширих размера) глобални свет се све више ослања на поузданост ИКТ. Отуда се као приоритетни циљ намеће питање безбедности сајбер простора и информационо - комуникационе технологије. Јер, као што је наведено у „Стратегији националне безбедности Републике Србије“: „насупрот очекивањима да ће бити повећан ниво одговорности свих укључених субјеката у погледу коришћења научних достигнућа у општем интересу и за добробит читавог човечанства, процењује се да ће развој науке и технологије наставити да буде подложан различитим видовима злоупотреба, што ће доводити до негативних безбедносних импликација. Динамика глобалног развоја информационо-комуникационих технологија условиће даље интензивирање активности у сајбер простору чију безбедност ће, превасходно, угрожавати сајбер шпијунажа, напади на критичну инфраструктуру, неовлашћени продори у базе тајних података, као и ширење лажних вести и дезинформација путем друштвених мрежа“ („Службени гласник РС“, број 94/19).

У савременом друштву мултикултуралност и толеранција се промовишу као глобалне вредности, међутим јавно испољавање етничких, верских и расних обележја није пожељно и неретко наилази на политичку осуду, било као расизам или неки други вид дискриминације. „Технолошке иновације створиле су могућности за сајбер конфликте и револуционарне борбе; појава дронова - беспилотних летелица, истовремено развија могућности надзора, док у неким случајевима отежава или угрожава могућности за отворене сукобе у облику протеста и неслагања“ (Wagner – Pacifici

& Hall, 2012, 195). Глобализацијске промене преламају се и на класну структуру, која се такође трансформише (Горц, 1982, Басан и др., 2005, 230). Отуда се „конфликти између друштвених група мењају, све чешће губе класни карактер и фокусирају се на идентитете друге врсте, попут религијских“ (Хантингтон, 2000).

Кризна ситуација ствара незадовољство, несигурност и производи негативне последице као што су: смањење извоза, пад продуктивности, несигурност радног места, незапосленост, смањење доходка и пензија и друге проблеме. Несумњиво је „савремено друштво превасходно ризично“ (Бек, 2001, 29). Појединци попуштају под притисцима. Постојећа друштвена ситуација на макро нивоу због бројних проблема може да изазове одбојност према капиталистичком развоју, национал - шовинизам или верски фанатизам, сепаратистичке тежње, што уз лаку доступност технолошких иновација чини сајбер тероризам најактуелнијим обликом тероризма. На тај начин постојеће стање погодује ширењу алтернативних облика испољавања незадовољства и покушаја да се постојећи поредак промени.

Криза идентитета и алијенација

Идентитет је предмет разматрања онда када га доводимо у питање, тј. када је у кризи. У литератури се појмови идентитет, јаство (*self*), сопство и личност преплићу и помињу на различите начине. Стојнов је дао неутрално одређење појма идентитета као класе елемената која сачињава јаство (Стојнов, 1999). Ериксон указује на потешкоће дефинисања овог појма и његову тесну повезаност са друштвеним контекстом, јер „идентитет говори сам за себе у бројним конотацијама" (Ериксон, 2008, 118). Вишеструки „слојеви" идентитета настају кроз сталну „игру" значења у социјалном контексту. Идентитет је једна релативно постојана структура која представља укорењене особености неког одређеног појединца или групе (колектива). Поменуте особености које су део колектива се чувају у колективном памћењу групе. Индетитет се обликује кроз процес интеракција у које је појединац укључен. Отуда Бамберг види идентификацију као процес који се никада не завршава и који се одиграва из момента у моменат услед бројних непредвиђених ситуација (Bamberg, 2011, 8). Идентитет увек настаје из односа. Формирање "постигнућа идентитета, мораторијума, одбацивања или дифузије идентитета" (Kacerguis & Adams, 1979) зависно је од тога да ли ће се особа прилагодити или не новим захтевима друштва. Постигнути идентитет даје одговоре на питање: ко сам и у шта верујем; какве односе ћу успоставити са другима и даје јасну представу о јаству, док дифузија идентитета представља опасно стање по психичко здравље, јер особа нема јасан центар свог постојања (сопства).

За време пандемије COVID - 19 вирусом информационе и комуникационе технологије су препоручено средство комуникације, јер пружају могућност повезивања људи уз истовремено поштовање ванредних здравствених мера и мера социјалне изолације. У новој реалности интернет пружа могућност бекства из ванредне кризне ситуације. Савремене ИКТ пружају сваком појединцу понаособ да упркос пандемији задовољи своје социјалне потребе, као што су: потреба за комуникацијом, интерперсоналним контактом, припадност друштву, односно одређеној заједници, друштвеној групи и др. Упркос бројним могућностима које се савременом појединцу нуде присутна је криза идентитета, јер поменути процеси који обликују садашњост имају двоструки ефекат. Како савремени процеси и изазови утичу на појединца? Како их индивидуа доживљава, разуме, схвата и психолошки процесуира? Разумевање савремене

јединке (индивидуе) од почетка 21. века готово је неизводљиво без узимања у обзир: ефеката процеса глобализације (Бек, 2001, 17 - 44), карактеристика „глобалитета“ (Yergin & Stanislaw, 2002) и утицаја који пандемија и примена информационих и комуникационих технологија имају на савремени живот појединца.

Процеси који обликују савремено друштво не конструишу само глобално и локално, такође значајно утичу и на индивидуално. Глобалну реалност карактерише конкурента атмосфера која се најпре уочава на економском пољу друштвене реалности, а потом прелива у политичко и културно поље. Мултинационалне компаније су глобални економски актери који базирају своје пословање на основу следећих принципа: 1. императив профита, 2. императив раста; 3. конкуренција и агресивност; 4. аморалност; 5. дехуманизација; 6. хијерархија; 7. бројивост, линеарност и сегментација; 8. експлоатација; 9. ефемерност и покретљивост; 10. несклад са природом; 11. хомогенизација“ (Мандер, 2003, 315). Ове компаније наносе штету локалним, националним економијама. Мултинационалне компаније због својих интереса најчешће бирају економски слабе и неразвијене земље, односно националне економије у којима могу да доминирају и диктирају услове и извлаче корист због неуједначених правила пословања између развијених и неразвијених земаља (неуједначена дневна надница радника, услови рада, права радника и др). На тај начин се на локалном и глобалном нивоу ствара нова прерасподела светског богатства и руши пређашња хијерархија економских снага и утицаја.

Мултинационалне компаније јачајући своју економску моћ, истовремено оснажују свој политички утицај, обзиром да њихово руководство представља део владајућих структура „елите власти” укључујући и политичку елиту, и јачају свој културно - идеолошки утицај услед ширења идеологије конзумеризма и добре сарадње коју имају са медијима и лобистима. Глобално децентрализовано пословно окружење карактерише појава нових правила пословања и управљања, инкорпорирање страних утицаја и модификација локалног. То се даље одражава и на промене у културној сфери које настају услед „слабљења или раскидања везе између културе свакодневног живљења и територијалне локације“ (Tomlinson, 1999, 128). На тај начин се економска глобализација прелива у политичку и културну и ствара културне утицаје који слабе локалне културне идентитете на које се надограђују глобалне вредности.

Створени су изазови за интеграцију индивидуалног и глобалног. Глобализација подразумева искорак из домена властите

културе, док брзина којом се дешава промена отежава адаптацију човека на новонасталу ситуацију. Појединац је на међи да бира између најмање два типа личности: „локалног“ и „космополитског“ (Merton, 1957). То изазива код појединца осећај несигурности, страх, отпор, неповерење, доживљај страног као наметање и својеврсну агресију према свему страном, што доводи до појаве екстремних реакција.

Дакле, глобализација поред бројних олакшица и предности ствара и „дубоку кризу морала и система вредности. Три су основна етичка изазова која су довела до глобалне кризе: 1) огромна похлепа изражена кроз сумануту трку за профитом; 2) одсуство емпатије и елементарног осећаја за другог човека; 3) етос расипништва који је тако моделиран да подстиче на задуживање, стицање и трошење“ (Љајић, Мета & Младеновић, 2016, 45). Да глобализација истовремено наглашава разлике и уједно ствара сличности, односно да истовремено уједињује и одваја примећују Лехер и Боли (Lechner & Boli, 2003). Чиу и сарадници (Chiu, Gries, Torelli & Cheng, 2011) наводе: „страх, завист, бес, изоловање, одбацивање, агресију, јављање побуде да се брани интегритет властите културе“, као одбацујуће реакције на глобалну културу. Ове емоционалне реакције и страх од културалне контаминације се према наводима Ченга (Cheng, 2010) најчешће јављају у незападним културама.

Негативне реакције на последице глобализације су најчешће код људи из незападних и неразвијених земаља, те су они због дотадашњих историјских искустава и културе сећања подозриви према западњачким утицајима и виде развијене земље као извознике капитализма. „Централни проблем глобалних интеракција је тензија која настаје између хомогенизације и хетерогенизације“ (Appadurai, 2000). Арнет (Arnett, 2002) предлаже поделу идентитета на: 1. „бикултурални идентитет“ који настаје комбинацијом локалног и глобалног идентитета, односно стварањем сложене хибридне форме идентитета, 2. „конфузни идентитет“ који карактерише отуђеност, осећај маргинализованости и не припадање ниједној култури, 3. „идентитет самоодабране културе“ који подразумева индивидуални одабир и / или придруживање одабраној култури колега дисидената и 4. „помањајућа одраслост“ који представља идентитет који одликује прихватање ситуације и проналажење себе. Упркос томе што се Арнет (Arnett, 2002) бавио тумачењем ефектата глобализације превасходно на адолесцентима, његова подела идентитета је применљива због општег утицаја који глобализација има на идентитет појединца без обзира на старосно доба.

Истраживања су показала да „прихватање страних или глобалних вредности не значи нужно и жртвовање локалног културног идентитета“ (Tong, Hui, Kwan & Peng, 2011; Morris, Mok & Mor, 2011). Локални културни идентитет настаје као резултат вишегенерацијског колективног деловања и памћења у коме се чувају знања и искуства која дају смисао деловању превасходно на темељу културних претпоставки у односу на друге изворе смисла. Колективни идентитети представљају моћно средство за „одређивање и лоцирање појединачних ’ја’ у свету, кроз призму колективне личности и њене особене културе. Управо нам заједничка, јединствена култура омогућава да сазнамо ко смо ми у савременом свету. Поново откривајући ту културу, откривамо сами себе, аутентично лично ја” (Смит, 1998, 34). Међутим, као што Кастелс примећује „ти су идентитети, у већини случајева, одбрамбене реакције на наметање глобалнога нереда и промена које се брзо одигравају и које се не могу надзирати. Они граде склоништа, али не и небеса” (Кастелс, 2002, 73). Постоји неколико врста идентитета: друштвени, политички, културни, религиозни, национални, територијални итд. Појединци који се налазе у стању конфузије идентитета, или никако не могу да се идентификују ни са једном формом идентитета, углавном су маргинализовани појединци, са ниским нивоима локалне и глобалне идентификације (Norasakkunkit & Uchida, 2011).

Истовремено примена савремених ИКТ такође доводи у питање некадашње поставке идентитета и води његовом редефинисању. Информационе и комуникационе технологије су „нова средства за изградњу замишљених себе и замишљених светова“ (Appadurai, 2000, 3) која пружају одржавање социјалних веза и комуникација у одсуству чулне пуноће под окриљем имагинације. Употреба интернета и ИКТ пружају могућност корисницима да представе жељену слику себе и формирају онлајн идентитете, што повлачи за собом умањење личне одговорности и остале бихејвиоралне и психолошке ефекте.

Савремене ИКТ су омогућиле редефиницију простора (Бауман, 2003), односно „сабијање простора и времена” (Giddens, 2005, Robertson, 1992) пружајући брз проток информација. Отуда с једне стране имамо технолошки прогрес и бројне олакшице које он са собом носи, док с друге стране расте стрес код људи, слабе друштвени односи (породични, партнерски и пријатељски), мења се начин комуникације, присутна је отуђеност и криза идентитета, расте број физичких и менталних обољења изазваних стресом, некретањем и другим факторима који произилазе из савременог

начина живота.

Савремени свет карактерише све већа отуђеност појединца, а одржавање социјалних веза и комуникација постају површније. Алијенација (отуђење) је сложен феномен. Различити елементи (фактори) могу да допринесу отуђености. Први су економски елементи, јер упркос томе што економски развој има позитивне последице на остварење материјалних циљева, он „истовремено слаби осећај заједништва и ствара хладније, мање хумане друштвене средине“ (Fu & Chiu, 2007, 636 – 653; Yang et al., 2011, 677 - 695). Други је социјални елемент, где отуђеност настаје као резултат немогућности појединца да се прилагоди савременим друштвеним токовима. Унутар истог друштва појединци драматично различито доживљавају глобализацију (Norasakkunkit & Uchida, 2011, 774 - 786). Најчешћи разлози социјалне отуђености су непотпуна социјализација и угрожена породица (развод и самохрани родитељ). Карактеришу је делимична или потпуна неукљученост у социјалне везе (нематеријалне аспекте животног стандарда). Депривација подразумева четири димензије: „објективно сиромаштво, оскудне социјалне везе, услови становања и потрошња добара“ (Tsakloglou & Papadopoulos, 2002). Психолошки фактори могу да допринесу отуђености која настаје као последица кризе идентитета појединца или неког психичког поремећаја. Технологија је наредни, четврти елемент који може да допринесе отуђености, јер технолошки развој је знатно проредио контакте лицем у лице услед онлајн комуникације и умрежавања појединца посредством интернета и савремених ИКТ (паметни телефони, таблети, компјутери, видео - игре и др.) у виртуелне онлајн заједнице (Luknar, 2021, 230 - 231). Појединци који не практикују примену савремених информационих и комуникационих технологија било због незнања, финансијских немогућности, или неког другог разлога бивају искључени из савремених друштвених токова и форми (виртуелна познанства, виртуелне заједнице и сајбер култура). Такође, с друге стране прекомерна употреба друштвених мрежа доводи до социјалне искључености толико да она прелази у зависност од информационих и комуникационих технологија. Пети, културни елемент отуђености се заснива на одбијању појединца да прихвати нове културне садржаје. Отуђеност такође може настати и услед непотпуне идентификација са културом заједнице којој појединац припада, што повећава склоност ка одређеним субкултурама, контракултурама. Шести, политички елемент алијенације настаје услед незадовољства постојећим друштвеним поретком и односима

моћи, односно када појединац сматра да постојећи друштвени свет и политичка ситуација нису вредни учествовања.

Политичко отуђење је „добровољан избор појединца, који настаје услед његовог става према друштвеном систему да систем не пружа активности или циљеве које он вреднује“ (Olsen, 1969, 291 - 92). Студије показују да демократске политичке институције уживају најслабију подршку од стране оних који су маргинализовани у друштву којем припадају, јер стање немоћи у којем се налазе представља важан услов који их наводи на пружање отпора према локалним питањима и власти. Зато су маргинализовани у друштву склонији да гласају за радикалне популистичке странке, пре него за оне које су „подупирачи" постојеће политичке и економске ситуације и глобализацијских тежњи (Pauwels, 2014). Савремене демократије карактерише криза легитимитета која је проистекла из незадовољства услед разлике између реалног учинка и очекивања. Норис је упоредном анализом педесет демократских земаља широм света дошао до закључка да је већина успостављених демократија искусила стално растућу плиму политичког незадовољства (Norris, 2011). Постоји позитивна корелација између демократије и тероризма (Li, 2005, 278 - 297; Luknar, 2018, 96). Низак ниво људских права може да буде узрок терористичких аспирација и деловања (Luknar, 2018, 98). Сви претходно наведени елементи не искључују један другог, већ су тесно међусобно повезани узрочно – последичним везама.

Образложена ситуација оставља простора за сајбер тероризам као примамљиву и лако приступачну форму тероризма. У условима отуђености и кризе идентитета терористичке организације могу да представљају алтернативну форму која пружа социјалну сигурност, заједништво и подршку социјално искљученима, противницима друштвеног поретка, отуђенима и обесправљенима. Јер, терористичке организације нарочито базирају своје програме на незадовољству и критици новонастале ситуације, негују осећај емпатије и припадности са жртвама савременог поретка и апелују на ургентност проблема и хитност у реаговању с циљем да уведу промене у савременом друштву. Терористичке организације карактерише висок степен поверења међу члановима, које се гради кроз њихову међусобну комуникацију и заједничку праксу. Извођењем различитих терористичких активности чланови развијају осећај припадништва, што даље учвршћује њихову оданост заједничким циљевима и вредностима.

2. ТЕРОРИЗАМ И ЊЕГОВА КЛАСИФИКАЦИЈА

Савремено друштво суочава се са глобалним изазовима као што су: тзв. „глобални тероризам“ (Cronin, 2009, 63), климатске промене, пандемија COVID – 19 вирусом, економска криза и енергетске промене. Последице глобалног тероризма су светских размера, а карактеришу га мотиви који су углавном етнонационалистичке и религијске природе. Премда је прошло више од две деценије након терористичких напада на САД од стране Ал Каиде 11. септембра 2001. године када је тероризам ступио кроз „велика врата“ на светску сцену, време је показало да је тероризам проблем дугог трајања.

Светска сцена уздрмана је бројним глобалним проблемима. Претње и страхови од тероризма не јењавају, штавише поменуте претње и страхови могу бити подстакнути незадовољством услед новонастале ситуације. Тероризам несумњиво представља значајан изазов по глобалну безбедност, а његово разумевање и дефинисање је од суштинске важности за адекватно суочавање и борбу са овим феноменом. Утврђивање његових кључних карактеристика намеће се као један од основних циљева савремених наука (друштвених, правно - политичких, безбедносних и др). Иако се у литератури појава тероризма везује за савремено доба, чињеница је да тероризам није појава новијег датума. Историја је потврдила постојање различитих облика тероризма. Отуда је због његове сложености и лакшег разумевања важно узети у обзир: 1) друштвено - историјске околности у којима се тероризам јавља, 2) врсту и квалитет друштвено - политичких и економских односа у земљи и окружењу, 3) актуелне политичке ставове, 4) „климу“ међународне заједнице, 5) деловање и понашање других држава и 6) постојање / непостојање евентуалних подстицаја за мешање у унутрашње односе и вршење спољних притисака на поједине суверене земље.

Тероризам може послужити као средство да се индиректно утиче на спољну политику тако што може да угрози интегритет једне државе, отежа, успори или онемогући њену интеграцију у поједине међународне организације или институције. Такође, тероризам може да потпомогне промоцију одређене владе на међународној сцени или пак да прикаже неку владу као неподобну и неспособну да се избори са проблемима, чак може да прикаже одређену државу као подржаваоца тероризама. Бављење тероризмом засигурно захтева вишеслојну интервенцију од стране међународне заједнице, што може да подстакне дезинтеграцију и спровођење одређених облика санкција. Због могућности тероризма да утиче на спољнополитички план, као и због последица тероризма које могу да имају далекосежни ефекат по националну безбедност, веома је значајно што веће

укључивање научне заједнице у разумевање појаве тероризам и у доношење мера за његово сузбијање и превенцију.

Тумачење раније литературе на тему тероризам указало је да се значење речи тероризам мењало током прошлости. Дефиниције тероризма су углавном сложене и контроверзне, јер овај термин означава примену насиља и застрашивање. На пример, током XIX века овај термин се користио да означи анархисте, који су сами себе тако називали. Такође су Лехи, борци за ослобођење Израела током 40 - тих година XX века себе представљали као јеврејску терористичку групу. Иначе, корен речи тероризам проистекао је из латинског језика где израз „*terror*“, „*terroris*“ значи „ужас, велики страх, владавина застрашивањем, начин владања уливањем страха и насиљем“ (Вујаклија, 1975, 947). Односно као што Симеуновић наводи:, „терор је претежно вршење насиља у оквиру процеса спровођења моћи са циљем одржања на власти, односно задржања или увећања моћи владајућих, дакле насиља власти“ (Симеуновић, 1989, 144 - 145).

Упркос чињеници да је тероризам проблем дугог трајања, због његове комплексности и великог броја различитих појавних облика током историје, научна заједница се није сложила око једне опште прихваћене дефиниције тероризма. У енглеском речнику тероризам је одређен као: „метод владавине или супротстављања некој влади који покушава да проузрокује страх“ (Flaxner, 1987). У италијанском речнику овај појам је дефинисан као „средство екстремног и илегалног насиља у политичкој борби“ (Palazzi, 1965). Терористи су временом мењали и прилагођавали методологију свог деловања актуелним историјским процесима. То је један од разлога зашто је тероризам до данашњих дана остао нерешен проблем. Одликују га сложеност и променљивост као његове примарне карактеристике, те је тероризам потребно тумачити у друштвено - политичком контексту у којем је настао. Симеуновић указује на различита значења овог термина током историје. Тако је, према речима професора, тероризам најпре служио да означи насилно преузимање власти од стране револуционара, да би „током 19. века био везан за насилно деловање анархистичких и нихилистичих организација. У двадесетом веку је два пута термин тероризам поново везиван за насиље власти, прво поводом деловања режима страховладе какви су били нацистички и стаљинистички, а затим и поводом неслагања западних великих сила са ослободилачким пројектима колонијалних народа који су се служили и насиљем у својој борби за ослобођење, да би седамдесетих година до данас

поново био везан за насиље против неке и нечије власти, мада повремено и за насиље неких држава које су означаване као спонзори тероризма, осовине зла и сл.“ (Симеуновић, 2009, 19).

Опасност од тероризма је константна, никада не јењава. „Савремени тероризам, као вишедимензионални политички феномен, иако присутан од самог почетка класног друштва у свим друштвено – политичким системима, поприма тако опасне и широке размере да се данас сматра једним од највећих пошасти на планети” (Савић & Стајић, 2006, 211 - 212). Многи аутори су се бавили тумачењем тероризма са аспекта разних научних дисциплина, што је изнедрило велики број различитих дефиниција тероризма. Томашевски то објашњава тиме што се под „појмом тероризма обухватају различити акти насиља и угрожавања људских права и људских живота, као и јавних, односно заједничких и индивидуалних добара. У том мноштву и разноликости аката који се подводе под појам тероризма, остаје део разлога због којих није могла бити утврђена једна свеобухватна и опште прихватљива дефиниција тероризма“ (Томашевски, 1983, 13). Међутим, упркос великом броју различитих дефиниција о тероризму, анализа садржаја је показала да постојеће дефиниције садрже у себи сличности, односно основне карактеристике тероризма. Тако се страх и насиље помињу као његове основне одреднице у готово свакој дефиницији о тероризму. За потребе монографије аутор је приложио следеће примере дефиниција:

1. „Под општим појмом тероризам подразумева се доктрина, метод и средство изазивања страха и несигурности код грађана систематском употребом насиља ради остваривања одређених, првенствено политичких циљева” (Скакавац, 2010, 331).
2. Гаћиновић као главну карактеристику тероризма види насиље и његову употребу и сматра да је то: „организована примена насиља (или претња насиљем) од стране политички мотивисаних извршилаца, који су одлучни да изазивањем страха, зебње, дефетизма и панике намећу своју вољу органима власти и грађанима“ (Гаћиновић, 1998, 31). Односно види га као „продужену руку политике, која се води другим (нелегалним) средствима“ (Гаћиновић, 2011, 18) за постизање својих циљева.
3. Кегли (Kegley, 2003, 13) предлаже одређење тероризма на основу његовог описа. Сматра да је најпре потребно: 1) утврдити његове основне елементе, 2) понудити објашњење овог феномена помоћу узрока који мотивишу актере да реализују своје циљеве практикујући терористичко деловање,

3) размотрити до сада постојеће, предложене и примењиване мере, како превентивне, тако и репресивне за сузбијање тероризма на глобалном нивоу.

4. Шмид и Јонгман одређују тероризам помоћу насиља и у зависности од основног циља тог насиља, односно у зависности од жељене поруке коју терористи желе да пошаљу медијима. Отуда они наводе: „Тероризам је страхом инспирисан метод понављања насилне акције вршене од стране индивидуа, група или државних актера из криминалних или политичких разлога, при чему – за разлику од убиства – конкретна мета насиља није кључна мета. Непосредне људске жртве насиља генерално су биране из циљане популације насумично (мете по прилици) или селективно (представници или симболичне мете) и служе као генератори порука. Базиран на претњи и насиљу, процес комуницирања између терористе (организације), (угроженог) жртве и главне мете служи да се манипулише главном метом (јавношћу - медијима) претварајући је у мету путем терора, захтева или скретање пажње зависно од тога да ли су у првом плану застрашивање, принуда или пропаганда“ (Schmid & Jongman, 2005, 28).

5. Лемкин дефинише тероризам на основу основних мотива терористе, наводећи да је застрашивање људи њихов примарни мотив.

Терористи се служе различитим врстама насилништва како би створили „danger commun“ (Lemkin, 1933, 900 – 901), односно једну свеопшту опасност која представља претњу по сигурност и угрожава интересе грађана, заједнице и у неким случајевима интересе појединих држава.

Тероризам као вишедимензионалан феномен се може јавити у различитим формама: манифестна (чији је циљ да одјекне у медијима и узнемири што ширу јавност) или латентна форма тероризма (камуфлирана, формално правно легална). Без обзира на форму у којој се јави, тероризам подразумева „вид индивидуалног, нелегитимног и неинституционалног насиља“ (Симеуновић, 1993, 736) и као такав представља претњу за неко друштво, државу или њене институције, те „нема легитимне основе у релевантном правном и етичком кодексу међународне заједнице“ (Симеуновић, 1993, 736).

У литератури о тероризму су наведени различити примери класификације тероризма у зависности од примарног китеријума класификације. Мноштво појавних облика и комплексност тематике

усложњава и отежава његову исцрпну класификацију, јер поједине терористичке организације истовремено одликује неколико различитих облика тероризма, које према карактеристикама не можемо сврстати у једну конкретну категорију. Управо због тога различити аутори предлажу различите класификације тероризма.

Симеуновић предлаже класификацију тероризма према:

„Програмско - циљној оријентацији:

1. Идеолошки мотивисан тероризам

1.1. Левичарски тероризам

1.2. Десничарски тероризам

2. Етно – сепаратистички тероризам

3. Верски фундиран тероризам

3.1. Тероризам секти

3.2. Тероризам фундиран на интерпретацијама великих религија

- према средствима и методима

1. Класификација тероризма према средствима

1.1. Класични (конвенционални) тероризам

1.2. Биохемијски тероризам

1.3. Нуклеарни тероризам

2. Класификација тероризма према методима

2.1. Класични (конвенционални) тероризам

2.2. Самоубилачки тероризам

2.3. Сајбер - тероризам (употреба интернета у терористичке сврхе)

2.4. Нарко - тероризам

- према типу актера – субјеката тероризма

1. Индивидуални тероризам

2. Тероризам организација и илегалних група

3.Институционални тероризам (државни и сл.)“ (Симеуновић, 2009, 82 - 85).

Милашиновић и Мијалковић предлажу класификацију тероризма према начину извршења терористичког напада. Отуда помињу: „тзв. промишљени (који изводе терористи који не желе да буду ухваћени нити убијени) и самоубилачки тероризам (који изводе политички, верски, националистички и други фанатици, користећи конвенционалне или импровизоване експлозивне направе, не марећи за свој живот). Средишњу, умерену тактику користи тзв. активни стрелац који, користећи ватрено, ређе хладно оружје или оруђе погодно за напад, убија што више невиних људи око себе, најчешће на јавном месту (на улици, у школи, у цркви, у средствима јавног

превоза, у самоуслузи, на спортском стадиону итд.)“ (Милашиновић & Мијалковић, 2011, 6).

Шикман на основу следећих одредница: „мотив извршења, средство извршења, начин извршења, објекат напада или неки други критеријум“ (Шикман, 2011, 46) даје класификацију тероризма. Током историје су се мењали покретачки мотиви терориста. Некадашњи „традиционални“ терористи углавном су били усмерени против тековина савремене демократске државе, њених структура моћи и настојали су да број жртава буде што је могуће већи. Док је савремени тероризам усмерен углавном против постојећих економско – енергетских система, како у националним тако и у међународним оквирима, као што су, на пример, тзв. „енергетски тероризам“, или тзв „рационални / калкулишући“ тероризам које помињу Милашиновић и Мијалковић (Милашиновић & Мијалковић, 2011, 6). Тежње савремених терориста усмерене су на стварање економске штете што већих размера и прекидање дотадашњих токова новца, како би угрозили постојећи животни стандард и променили тренутну економску ситуацију у своју корист.

Тероризам можемо да класификујемо према средствима извршења, односно у зависности од оружја које се користи у терористичким активностима на: „нуклеарни, кибер тероризам, биолошки, хемијски или комбиновани тероризам“ (Милашиновић & Мијалковић, 2011, 6). Савремени терористи употребљавају различита средства и оружја чија је деструктивност таква да могу да произведу штету већих размера, отуда Милашиновић и Мијалковић предлажу заједнички назив за ову врсту тероризма - „постиндустријски тероризам“, односно „супер (мега) тероризам“ (Милашиновић & Мијалковић, 2011, 7). Разни аутори (Weimann, 2006; Bobbitt, 2008, 55 - 57; Geer, 2006; Лукнар, 2020а) наводе да су развој и примена технологије изнедрили нове постмодерне неконвенционалне форме тероризма и злоупотребу високоразвијене технологије за остварење комуникације и организовање напада због разних погодности које интернет пружа (могућности анонимне комуникације и ниских трошкова). Да нове информационе технологије значајно олакшавају међународни тероризам такође указује и практичан пример Исламске државе, која се служила друштвеним мрежама за пропагирање и остваривање својих идеја.

Хармон говори о посебној врсти тероризма, тзв. „еколошки тероризам“ (Harmon, 2000, 137 – 185). Ову форму тероризма одликује примена насиља ради остварења једног јасно одређеног циља, а то је указивање на конкретне еколошке проблеме (очување природе,

биодиверзитета, воде, спречавање емисије угљен - диоксида, ефекта стаклене баште итд.) због којих се насиљем врши притисак на органе власти како би они иницирали доношење законских прописа којим би се ти проблеми решили. Даље, тероризам можемо да разликујемо у зависности од простора у којем се претежно испољава - тзв. „урбани“ или „рурални“ (Симеуновић, 2009, 82), и у зависности од тога да ли је присутан на тлу једне конкретне државе - „унутрашњи“ или „спољни“ – када његове последице превазилазе националне границе (Симеуновић, 2009, 82).

3. САЈБЕР ТЕРОРИЗАМ

Постојећа сазнања о сајбер тероризму

Постоји обилан фонд литературе која пружа општа разматрања о тероризму. Док је литература која се конкретно бави сајбер тероризмом оскудна. Готово да нема литературе у свету која се нарочито бави сагледавањем сајбер тероризма из угла специфичних националих оквира, односно кроз тумачење различитих стратегија за борбу против сајбер тероризма. Имајући у виду константан технолошки развој, нарочито развој и примену информационо - комуникационих технологија и интернета, поменуто стање указује на озбиљан недостатак у литератури, и потребу за хитним реаговањем најпре од стране научне заједнице кроз дебату, а потом и на националном и глобалном плану кроз предложене мере, политике и стратегије.

Сајбер тероризам је форма тероризма новијег датума, која је недовољно истражена. Све већа примена интернета и савремених информационих и комуникационих технологија указују на актуелност проблема и потребу за тумачењем могућих претњи и опасности у сајбер простору. Сајбер тероризам је специфична форма тероризма, не само по средствима која сајбер терористи користе, већ и због тога што се одиграва у специфичном окружењу – виртуелном, где постоје онлајн средства и принципи, где дешавања и опасности у сајбер простору остају неприметни у стварном физичком свету, а његове последице и причињена штета могу директно да утичу на свакодневни живот људи, на медије, јавно мњење, инфраструктуру и безбедност.

Научно - технолошка револуција изнедрила је поред нових изума и нове друштвене форме (виртуелне заједнице, сајбер култура), нове начине комуницирања, али и проблеме. Док је пандемија COVID – 19 вирусом истакла у први план напредну технологију и могућности њене примене у готово свим областима људског деловања (е - управа, медицина и здравство, производња хране, учење на даљину итд.) (Luknar, 2020б, 621). У савременом друштву је техничко - технолошки фактор добио на значају, толико да технолошка надмоћ на светској сцени данас значи много. Зато се савремене државе света утркују за развијањем нових технологија и њиховом применом. То има за последицу да је инфраструктура савремених држава поред традиционалних физичких средстава сачињена великим делом од средстава у онлајн (сајбер) простору, а знање нарочито у ИТ области је постало један од примарних ресурса у савременом друштву.

Најмоћније државе света издвајају велику количину финансијских средстава за наоружање и технолошки развој, чиме се енормно увећавају капацитети за уништење планете и нарушава глобална безбедност. Актуелна друштвено - политичка ситуација је пољуљана негативним последицама које је изазвала пандемија коронавирусом. Економска криза и нова прерасподела моћи на глобалној сцени уз технолошки развој доприносе увећању тензија. На тај начин се опасност од сајбер тероризма намеће као актуелан безбедносни проблем. Безбедност активности на интернету, заштита и превенција од сајбер напада и сајбер тероризма се намећу као актуелне теме за разматрање од стране стручњака и теоретичара из области безбедносних, правних, војних, информатичких, политичких и других наука.

Колин наводи да је термин сајбер тероризам скован крајем двадесетог века (Collin, 1997, 15). Међутим, у научној заједници још увек није успостављена општа сагласност о општеприхваћеној дефиницији појма сајбер тероризам. Овај термин се употребљава углавном да означи безбедносне претње и различита криминална дела и саботаже која су извршена помоћу савремене информационе и комуникационе технологије и интернета у сврху политичког деловања и стварања одређених политичких ефеката и климе. Тумачење и разумевање поменутог појма отежава велика тамна бројка сајбер тероризма која настаје услед отежавајућих околности за откривање починиоца и доказивање учињеног дела. Док предности које сајбер тероризам има над традиционалним облицима тероризма чине ову форму тероризма актуелном, нарочито у савременом друштву. Поменуте предности произилазе из могућности које корисници ИКТ имају, као што су: 1) анонимност – могућност да креирају виртуелни (сајбер) идентитет, 2) могућност да без улагања великог физичког напора и конкретног оружја у реалном (физичком) свету нанесу штету великих размера независно од реалне удаљености починиоца и мете, 3) релативно лако извршење, које осим знања из ИТ области и технолошке опремљености не захтева неке додатне организације и ризике.

У литератури која се бави тумачењем сајбер тероризма, издвајају се два основна правца размишљања. Први правац, подразумева уско дефинисање појма тако да: „Он обухвата политички мотивисане хакерске операције које су намењене да изазову озбиљну штету, као што су губитак живота или тешке економске штете“ (Denning, 2001, 241). Дакле, овај правац дефинише сајбер тероризам у односу на његово разликовање од обичних хакерских активности и

компјутерског криминала, односно одређује га као хактивизам који је политички мотивисан. Дакле, сајбер терористи су они починиоци, хакери који инсистирају на томе да су првенствено мотивисани политиком, а не некаквом злом намером или жељом да остваре финансијску корист.

Други шири правац размишљања углавном заступају владини званичници и лица војне одбране, према којем сајбер тероризам подразумева било који напад у виртуелном (сајбер) простору којим се угрожава безбедност. Овом, правцу одређења сајбер тероризма припада Шиндер који наводи: „Напади на компјутере и рачунарске мреже могу се дефинисати као сајбер тероризам уколико су њихови ефекти довољно деструктивни толико да изазвају страх који је упоредив са физичким терористичким актом“ (Shinder, 2002, 19). Сајбер тероризам је савремена форма тероризма која се односи на „незаконите нападе и претње напада на рачунаре, мреже и информације које се тамо чувају“ како би „застрашили или приморали владу или њен народ да ради на остварењу политичких или друштвених циљева“ (Manap & Tehrani, 2012, 409) који погодују терористима. Левис указује да сајбер тероризам представља значајну претњу, обзиром да подразумева „употребу компјутерских мрежа и интернет алата за ометање критичних националних инфраструктура (као што су енергија, јавни превоз, владине активности) или за застрашивање или присиљавање влада једне земље или њених грађана“ (Lewis, 2002, 1).

Адекватно суочавање са одређеним проблемом захтева његово претходно прецизно дефинисање. Отуда се намеће питање: Које су то активности на интернету које можемо да сматрамо терористичким у правом смислу те речи? Разни аутори су покушали да понуде одговор и поменуте активности класификују. Вејмен је предложио да „све активности терориста на интернету можемо да класификујемо у осам различитих 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“ (Weimann, 2004, 5 - 10). Мојра Конвеј предлаже скалу која активности терориста на интернету карактерише као употребу, злоупотребу, офанзивну употребу и сајбер тероризам (Конвеј у: Дамњановић, 2009, 238). Елементи који могу послужити као основне одреднице којима се прецизно дефинише сајбер тероризам и јасно разликује од осталих онлајн злоупотреба информационих и комуникационих технологија и интернета (сајбер криминала, хакерских активности, па чак и

сајбер екстремизма) су: „а) правни контекст (намера, завера, само претња или чин?); б) сајбер простор служи као оружје или је циљ; ц) циљ (и) злонамерни поступак који садржи неку врсту насиља са далекосежним психолошким ефектима код циљаног аудиторијума; д) намера комбинована са дугорочним циљем (нпр. друштвене или политичке промене, утицај на политичко одлучивање) којима тежи терориста или терористичка група“ (Akhgar, Staniforth & Bosco, 2014, 13). Дамњановић издваја следеће основне елементе за дефинисање појма сајбер тероризам: „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“ (Дамњановић, 2009, 244).

Комплексност истраживаног феномена и разноликост облика у којима се испољава сајбер тероризам имају за последицу бројне могућности његовог дефинисања на основу различитих критеријума. Једну од најприхваћенијих дефиниција сајбер тероризма је понудила Денинг, која под сајбер тероризмом подразумева „политички мотивисане хакерске операције које имају за циљ да нанесу озбиљне штете, као што су губитак живота или тешка економска штета“ (Denning, 2001, 241).

Петровић акт сајбер тероризма прагматично дефинише као „коришћење информационих ресурса у виду претње или уцене да би се остварио одређени терористички циљ“ (Петровић, 2000, 649). Ради постизања својих циљева сајбер терористи се служе разноразним тактикама (застрашивање, мрежни упади и саботаже, онлајн терористичке обуке итд.), које могу бити све сложеније и савременије услед ширења могућности које ИКТ пружају својим корисницима. Најчешћи покретачи за сајбер тероритичке активности су политичке природе. Сајбер терористи, неретко прибегавају и сајбер криминалу, што најчешће није њихов примарни циљ, него само успутни противзаконити начин за прибављање средстава (финансијских и других) који им омогућава лакше остварење примарног циља. Сајбер тероризам може бити тесно повезан са сајбер криминалом, али га треба разликовати од сајбер криминала, информационог рата, сајбер шпијунаже, јер представља посебну врсту сајбер претње. Дакле, сајбер тероризам подразумева организовани облик криминалног деловања, који подразумева низ криминалних мера и процедура где су савремене технологије средства или циљеви напада. Сајбер

тероризам није исто што и сајбер криминал. Разликује их основни циљ напада, јер је основни мотив сајбер криминалаца остварење економске добити. Његово успешно спречавање је једна од основних функција криминалне политике.

Сајбер напади не само да наносе значајне материјалне штете финансијским институцијама, него „могу такође циљано да угрожавају рад националних одбрамбених система“ (O'Harrow, 2005, 10). „Да би се разумела потенцијална опасност од сајбер тероризма, морају се узети у обир два фактора: прво, да ли постоје циљеви који су рањиви на нападе који могу довести до насиља или озбиљне штете; и друго, да ли постоје актери који поседују способност и мотивацију да их спроведу“ (Denning, 2001, 7). Управо због бројних штетних последица које ови напади могу да узрокују нужно је предузети адекватне мере за спречавање сајбер тероризма. Јер, као што Дороти Денинг (Dorothy Denning) наводи сајбер тероризам 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 сајбер тероризам, напад мора да резултира насиљем против лица или имовине, или у најмању руку да нанесе довољно штете да би изазвао страх“ (Денинг у: Дамњановић, 2009, 242 - 243).

Сајбер тероризам је несумњиво комплексан, вишедимензионалан феномен чије сузбијање изискује организоване мере борбе и превенције. То су препознале поједине државе, те имају специјалне тимове (*Computer Emergency Response Teams - CERT*) за хитно реаговање и борбу са онлајн претњама. Не постоје усаглашене методе за супростављање овом друштвеном проблему. Од државе до државе примењују се различите методе. Неки аутори (Dogrul, Aslan & Celik, 2011, 35) наводе да су САД и Велика Британија добар пример безбедносне политике за супростављање сајбер тероризму, јер примењују две врсте метода сајбер одбране: активне и пасивне. Шиндер (Shinder, 2002, 35- 41, 44) указује да су мере борбе против сајбер тероризма несумњиво значајне, али да је потребно њихово прецизно дефинисање и адекватна едукација оних који те мере примењују уз употребу одговарајуће технологије. У активне методе одбране (*Active Cyber Defense*) убрајамо директну одбрану и превенцију, односно „активности које су усмерене да онемогуће, ублаже или пониште сајбер претње“ (Denning, 2014, 3) које су упућене према цивилима и имовини. Док пасивне методе

одбране подразумевају различите сигурносне компјутерске технике и мере заштите (Stallings & Brown, 2015) као што су: криптографија (Talbot & Welsh, 2006), употреба антивирус софтвера и *Firewall* - а (Walsh, 1997), различити системи за откривање упада и заштиту лозинки, кључеви за шифровање (*DES*, *3DES i RSA*[2]) (Куљански, 2010, 65 -77) и др.

Генерално посматрано појам тероризам је комплексан друштвени проблем. Имајући у виду да је сајбер тероризам један од његових појавних облика који се одиграва у специфичном окружењу – сајбер простору и да ова форма тероризма захтева познавање и примену савремених знања и вештина, комплексност истраживаног феномена се још више усложњава и захтева примену мултидисциплинарног приступа за његову анализу и тумачење. За потребе истраживања и боље разумевање истраживаног појма аутор анализира питања која предлаже Ешли за тумачење сајбер тероризма:

1) Ко су починиоци сајбер тероризма (да ли их подржава држава, да ли их држава одбацује, било да су квази формације, хакерске групе или људи на власти који се баве шпијунажом);
2) Које алате и технике примењују у процесу планирања и извршења самог напада;
3) Како примењују технике, тактике и поступке за извођење сајбер напада (метод социјалног инжењерства, стварање и ослобађање вируса, злонамерни софтвери);
4) Након извршења напада које су категорије мета или потенцијалне мете терористичких сајбер напада (информационе и комуникационе мреже, подаци, објекти у "стварном" свету, енергија, банкарство и финансије, виталне услуге једне земље);
5) Зашто врше напад, односно шта их мотивише за спровођење сајбер терористичких напада;
6) Када се напад изведе, који су резултати, предности и мане таквих акција" (Ashley, 2003).

2 Кључеви за шифровање су криптографски алгоритми који служе за очување безбедности података. Могу да буду класични и модерни. Најпопуларнији асиметрични метод за криптовање података је RSA алгоритам, који је добио назив по почетним словима својих изумитеља: Rivest, Shamir и Adleman. RSA и 3DES спадају у модерне врсте кључа за шифровање. DES и 3DES спадају у најпознатије алгоритме симетричних криптосистема. Више можете пронаћи у: Stalings, Wiliam (2011). *Cryptography and Network Security Principles and Practices*. Prentice Hall. Retrieved July 3, 2017 from: https://wanguolin.github.io/assets/cryptography_and_network_security.pdf

Модели тумачења сајбер тероризма

Сајбер тероризам представља спој седам кључних елемената: 1) људски (индивудални - појединац, терориста или групни - организације у чије име појединци делују); 2) IT знање (значајан ресурс савременог доба), 3) технолошки (IT средства); 4) виртуелни (сајбер простор, онлајн идентитети и онлајн заједнице); 5) насиље (насилни упад на мрежу, прибављање података и тд.); 6) страх и 7) политичка мотивисаност за остварење дугорочног циља.

Не можемо сваки напад на рачунар или мрежни систем, сајбер претње, или било које друге инциденте и различите врсте вандализма које су се одиграле у сајбер простору да уврстимо у сајбер тероризам, уколико мотив за њихово извршење није био идеолошки. Јер, сајбер тероризам и компјутерски (сајбер) криминал нису једно те исто. То су два различита појма која треба посматрати одвојено. Неретко се дешавало да медији услед недовољног разумевања разлике између ова два појма поједине догађаје погрешно описују као сајбер тероризам, иако они то суштински нису. Као пример може да послужи случај из 2000. године када је „један Аустралијанац хаковао систем управљања комуналним отпадом и „избацио“ милионе литара отпадних канализационих вода у паркове, реке и предузећа“ (Smith, 2001). Поменути случај представља сајбер криминал, а не сајбер тероризам, обзиром да је починиоц деловао вођен искључиво индивидуалним мотивима, а не жељом да промовише одређену верску или политичку идеологију. Тик и сарадници (Tikk, Kaska & Vihul, 2010, 18.) сматрају да је напад у Естонији 27. априла 2007. године био један од првих примера великих сајбер терористичких напада, чији је основни циљ био да угрози националну сигурност и дестабилизује финансијски систем ове земље и изазове што већи број нежељених ефектата на функционисање јавне управе и привреде.

У научној јавности постоје неслагања око употребе термина сајбер тероризам. Једни аутори сматрају да је употреба овог појма непримерена и превише усиљена, јер нападе изведене путем интернета и у сајбер простору не могу да окарактеришу као терор, него пре као неку непријатност. Други аутори се позивају на непредвидиве ефекте сајбер тероризма, као и његове разорне последице по државну инфраструктуру, али и на његову могућност да утиче на спољну политику и угрози кредибилитет неке владе или произведе страх и несигурност широких размера у међународној заједници.

Да бисмо могли да разликујемо сајбер тероризам од класичног

сајбер напада, потребно је да разумемо оба појма. Сајбер напад, подразумева сукоб који се одвија у виртуелном (сајбер) простору и може да буде вођен самостално или као вид подршке неком другом сукобу. Док, сајбер тероризам можемо да посматрамо као посебну врсту сајбер напада и истовремено посебну врсту тероризма. Услови који су потребни за успешно извођење сајбер напада су: „а) познавање циљаног система, укључујући функције, сервисе, конфигурацију, политике и алате заштите и администрирање; б) ефикасно коришћење програма који ће аутоматски експлоатисати рањивости за провaљивање у рачунар (ти програми су познати под називом *exploits*); ц) капацитет нападача да прикрије своје трагове да би избегао могућност да буде детектован и праћен; д) брзина напада чиме се смањује могућност да се са предузетим мерама заштите закасни“ (Вулетић, 2011, 22). Дакле, извршење сајбер напада изискује детаљну припрему нападача. Односно, подразумева да нападач прикупи што више информација о мети напада, циљаним системима, евентуалним „рупама у систему“ и рањивостима (људским, техничким и организационим), да се упозна са њиховим механизмима заштите и нивоима контроле.

Постојећу литературу која тумачи сајбер нападе можемо да поделимо у три шире категорије у зависности од аспекта са којег се тумачи сајбер напад: „технолошко - центрични модели, социјално - центрични модели и ситуациони модел“ (Hapa & Fairclough, 2017, 169 - 185). Имајући у виду да дела сајбер терориста представљају посебну врсту сајбер напада чији су основни мотиви политичке природе, претходно наведене моделе можемо да применимо и за тумачење сајбер тероризма.

Први технолошко - центрични модел тумачи сајбер нападе примарно са технолошког аспекта. Бројни аутори посебну пажњу поклањају описивањем различитих алата који омогућавају откривање сајбер напада. На пример, Бишоп тумачи сајбер нападе са аспекта „шест кључних карактеристика: суштинска природа дефекта који је проузрокован сајбер нападом, време, добитак експолатације, област / подручје сајбер напада и извор идентификације рањивости прозруковане сајбер нападом“ (Bishop, 1995). Коен са аспекта технолошко - центричног модела тумачи сајбер одбрану и предлаже тзв. „модел огледала“, на основу следећег сета карактеристика: 1. „ортогонална неиспуњеност (*Non - orthogonality*)“, 2. „корелација (*Correlation*)“, 3. „хардверска неспецифичност (*Hardwarenonspecificity*)“, 4. „опис (*Description*)“, 5. „применљивост (*Applicability*)“ 6. „непотпуност (*Incompleteness*)“

(Cohen, 1997, 29 - 46). Док, Хачинс и сарадници (Hutchins, Cloppert & Amin, 2011) предлажу „*cyber Kill-chain*“ примењујући технолошко - центрични модел наводећи следеће фазе сајбер напада: „1) извиђање (*Reconnaissance*), 2) наоружавање (*Weaponization*), 3) испорука (*Delivery*), 4) експлоатација (*Exploit*), 5) инсталација (*Installation*), 6) команда & контрола (*Command & Control (C2)*и 7) активности према циљевима (*Action on Objectives*)“ (Табела 3). Прва фаза подразумева: истраживање и прикупљање што већег броја информација, идентификацију и одабир мета, прибављање мејлинг листе (адресе е - поште), стварање социјалних веза или прикупљање информација о специфичним технологијама. Након ње следи друга фаза која подразумева прибављање средстава за успешну испоруку аутоматског алата (оружја) и остварење жељеног циља / експлоатације помоћу удаљеног приступа. У пракси је потврђена све већа злоупотреба података познатих екстензија; у PDF формату (*Adobe Portable Document Format*) или *Microsoft Office* документи. Трећа фаза се односи на начин испоруке, односно на одабир носиоца алата / сајбер оружја који изазивају компјутерске инциденте (е - mail прилози, сајтови и преносиве USB меморије и др.). Четврта фаза је експлоатација. Наступа након испоруке алата домаћину / жртви који покреће упадни код који омогућава експлоатацију оперативног система или одређене апликације. Потом следи пета фаза, инсталација која омогућава конзистентност напада упркос физичкој удаљености нападач / жртва. Шеста фаза, позната као фаза команде и контроле подразумева активну укљученост и мануелне операције нападача, тзв. „руке на тастатури“. Последња, седма фаза наступа тек након што су извршене све претходно наведене фазе. Тада нападачи предузимају акције у складу са циљевима: рушење интегритета жртава, прикупљање поверљивих информација, шифровање и др. (Hutchins, Cloppert & Amin, 2011).

Табела 3. Фазе сајбер напада (Hutchins, Cloppert & Amin, 2011, 12)

Фаза	Упад 1	Упад 2	Упад 3
Извиђање	[Листа прималаца] Бенигни PDF	[Листа прималаца] Бенигни PDF	[Листа прималаца] Бенигни PPT
Наоружавање	Тривијални алгоритам шифровања (енкрипције)		
	Кључ 1		Кључ 2
Испорука	[Email субјекат] [Email тело]	[Email субјекат] [Email тело]	[Email субјекат] [Email тело]
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Експлоатација	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Инсталација	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp		
Ц2	202.abc.xyz.7 [HTTP захтев]		
Активности и циљеви	N/A	N/A	N/A

Сајбер терористи се за извођење напада служе различитим методама. Отуда разликујемо три врсте напада: 1. класичан физички напад који је усмерен против компјутерске опреме, објекта или далековода чији је циљ да омета и онемогући правилан рад и функционисање, поузданост опреме. За ову врсту напада сајбер терористи углавном примењују конвенционално оружје (нпр. ватрено оружје или експлозив), 2. електронски напад, подразумева употребу електромагнетне енергије, односно употребу електромагнетног пулса који је усмерен против компјутерске опреме с циљем да онемогући, омета или угрози пренос и интегритет података (прегревање струје или ометање комуникација) и 3. напад на компјутерске мреже (*CNA - Computer Network Attack*) подразумева сајбер напад који је усмерен на рачунарски процесни код, његову логику и инструкције или податке. Овакав напад генерише ток штетних мрежних пакета који су намењени за ометање података или логике, а служе се слабостима рачунарског софтвера и сигурносним пропустима у систему рачунара одређене организације која је мета напада (Weiman, 2006, 155-156). Активности сајбер терористе су сложене и терористи могу да примене све претходно наведене методе и врсте напада (физички, електронски и сајбер напад усмерен на одређене компјутерске објекте и системе) ради остварења својих политичких намера. Најдеструктивније врсте сајбер напада су: напад

на *SCADA* системе, напад на „бот мреже“, „*DDoS* напад“ и „*START / STOP* напад“[3], који се одвија следећим редоследом *SCAN*, *STOP* и *START* (Табела 4). Једино се константним систематским надзором постиже ефикасна одбрана и безбедност против наведених врста сајбер напада.

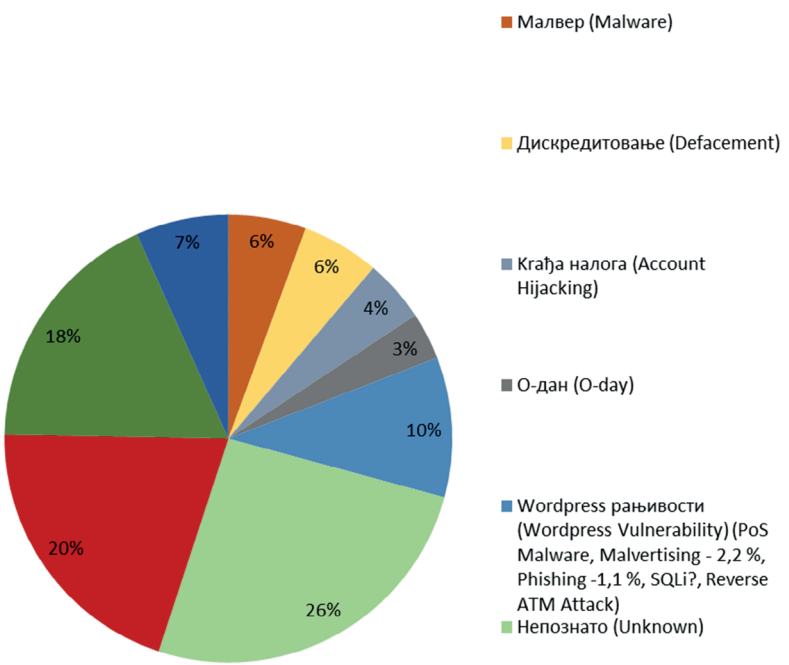
Други, социјално - центрични модел настоји да тумачи разуме и предвиди сајбер напад помоћу људског (социјалног) фактора (Табела 5). Овакав приступ подразумева идентификацију појединаца који не уживају потпуно поверење и који би могли да представљају знатан ризик по сајбер безбедност. Истакнути аутори (Greitzer & Ferrymann, 2013, 90 - 97; Kandias et al., 2013, 261 - 266; Stavrou et al., 2014, 119 - 131) који се залажу за примену овог модела нуде методе и метрике за процену и предвиђање „инсајдерских претњи“. За идентификацију / мапирање потенцијалних проблема и случајева нарушавања сајбер сигурности / поверљивости потребно је да укључимо у анализу људско понашање и интеракцију са интерфејсом, односно све односе између корисника међусобно, њихових циљева и окружења (Akhgar, Staniforth & Bosco, 2014, 51).

Табела 4. Пример start / stop напада (Yılmaz & Gönen, 2018, 98)

Функција (Feature)	**Садржај (Content) (Hexadecimal/ Decimal)**
Потпис нападача (Attack signature)	0300001e02f08072
Број секвенце (Sequence Number)	237
Идентификација (Identification)	0x0193 (403)
Извор (Source)	192.168.10.18
Изворна рачунарска мрежа (Source port)	34347
Одредиште (Destination)	192.168.0.4
Одредишна рачунарска мрежа (Destination Port)	102
Тип (Type)	Ipv4 (0x0800)
Заставице (Flags)	PSH, ACK
Верзија (Version)	4
Податак (Data)	7202000f32000004f20000000834000000000072020000

3 О поменутим нападима ће детаљније бити речи у поглављу 3.4. Последице сајбер тероризма.

Слика 1. Технике сајбер напада (Munkhdorj & Yuji, 2017, 110)



Табела 5. Социјално-центрични модел, фактори сајбер напада (Akhgar, Staniforth & Bosco, 2014, 51)

Фактори (Factors)	**Системске карактеристике (System Characteristics)**
Фактори пружаоца услуга (Service provider factors)	•Приватност, осигурање и безбедносне карактеристике (Privacy, assurance and security features)
Карактеристике корисника (User characteristics)	•Робусност (Robustness)
	•Неуспешне карактеристике (или сувишност) (Fail safe characteristics (or redundancy)
	•Склоност поверењу / поверљивост (Propensity to trust/confidence)
	•Искуство и познавање употребе интернета (Experience and proficiency in internet usage)
	•Очекивања од оног шта се пружа (Expectation of what is being provided)
	•Ниво свести о сајбер безбедносним претњама (Levels of awareness about cyber-security threats)
Сигурносни алати (Security tools)	•Знаци друштвеног присуства (Social presence cues)
	•Капацитет прилагођавања и персонализације (Customization and personalization capacity)
	•Ограничени интерфејси који омогућавају слободну употребу (нпр. способност преноса детаља преко сигурне мреже) (Constrained interfaces that allow free use (e.g., ability to convey details over a secure network)
	•Динамичка природа би требало да буде беспрекорна (и продорна) (Dynamic nature should be seamless (and pervasive)
Безбедносни задаци (Security tasks)	•Кориснички интерфејс има висок степен корисности (User interface has high degree of usability)
	• Изричите безбедносне карактеристике (Explicit security characteristics)
	• Квалитет информације/ квантитет /правовременост (Information quality/quantity/timeliness)
	• Графичке карактеристике (Graphical characteristics)
Оперативно окружење (Operational environment)	• Искуство и познавање on-line компаније (Experience and familiarity with the online company)
	• Једноставност употребе у различитом контексту (Ease of use in different contexts of use)
	• Комуникација различитих нивоа претње (Communicating different threat levels)

Поборници трећег модела, ситуациони модел приликом тумачења и разумевања сајбер напада предност дају ситуационим елеменатима, односно факторима из окружења. Међутим, адекватно тумачење сајбер напада суштински изискује примену сва три предходно наведена модела. Евалуација изведеног сајбер терористичког напада се може вршити помоћу критеријума на основу којих се учињени сајбер напад квалитативно процењује:

„1. Јачина - Одређује се по обиму, трајању и интензитету последица сајбер напада.

2. Непосредност - Односи се на брзину којом се последице манифестују.

3. Директност - Испитује ланац узрочности.

4. Инвазивност - Односи се на степен до којег операције у сајбер простору представљају циљане упаде на државу или на њене мрежне системе који штете интересима те државе.

5. Мерљивост ефеката - Односи се на чињеницу да што је више последица квантификовано и идентификовано, држава ће лакше да процени ситуацију нивоа употребљене силе током сајбер напада.

6. Војни карактер - Вероватноћа везе између сајбер операције и војних интервенција.

7. Укљученост државе.

8. Међународно право“ (Pipyros et al., 2018, 376) односно у којој мери је његово кршење.

Намеће се питање: Како да разликујемо обичан (или комбинован) сајбер напад од оног који је извршио терориста? Искуство је показало да се терористи служе разним криминалним радњама на путу до остварења свог примарног циља, који је готово увек идеолошке природе. Акгар и сарадници предлажу четири елемента: „1) интегритет информација, 2) поверљивост информација, 3) доступност ИКТ услуга (сервиса) и 4) процеси засновани на ИКТ који контролишу физичке процесе у стварном свету“ (Akhgar, Staniforth & Bosco, 2014, 14) који могу послужити као одреднице сајбер напада, односно за боље разумевање сајбер тероризма. Први елемент, „интегритет информација“ најчешће подразумева неовлашћено брисање и неовлашћене промене, што има за последицу губитак поверења у ИКТ (информационе и комуникационе технологије) и друштво. Циљеви сајбер терористa су базе података које су кључне за друштво: лична документација, документација за регистрацију возила, власничку имовину, финансијски подаци и рачуни и др. Други елемент, „поверљивост информација“ код сајбер терористичких напада подразумева повреду поверљивости великих размера када су угрожени поверљивост личних података или података од појединих организација која може да се сврста у друштвени поремећај. На пример, објављивање комплетне здравствене евиденције о ХИВ - инфицираним лицима у нацији могла би да покрене низ узнемиравања и самоубистава. Трећи елемент, „доступност ИКТ услуга (сервиса)“ се односи на отежавање, онемогућавање доступности бројних услуга које информационе и комуникационе технологије пружају, који за последицу имају

колапс ширих размера. На пример, онемогућавање услуга током дужег времена, неовлашћени прекид рада појединих система, мрежа или физички, или електромагнетни напад на дата центре и критичне компоненте ИКТ система. Четврти елемент, „процеси засновани на ИКТ који контролишу физичке процесе у стварном свету“ подразумева усмереност сајбер терористе на ометање рада нуклеарних електрана, рафинерија, саобраћаја возила и других облика транспорта, мониторинг и контролу здравља, на упад у тзв. паметне мреже и паметне градове, односно на све системе који су круцијални за функционисање у свакодневном животу (Akhgar, Staniforth & Bosco, 2014, 14).

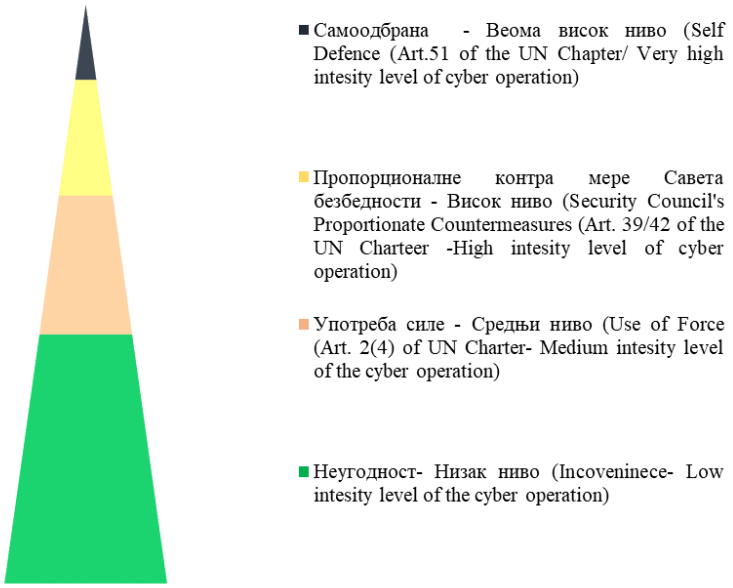
Ролинс и Вилсон наводе два кључна елемента која треба да буду испуњена како би се одређени акт сврставао у категорију сајбер тероризма: први је „ефекат, када напад на рачунарски систем изазива страх, као и код традиционалног терористичког акта; други је намера, односно постизање политичких циљева“ (Rollins & Wilson, 2007, 3). Дакле, једино „политички мотивисану употребу компјутера као оружје или као мету / циљ, од стране поднационалних група или тајних агената, чија је намера да насилно утичу на јавност или владу како би она променила своју политику“ (Wilson, 2003, 4) можемо сматрати делима сајбер тероризма.

На глобалном нивоу страх и незнање су тесно повезани са тумачењем овог појма. Отуда су УН 2008. године (United Nations, 2008) сумирале међународне инструменте који се односе на превенцију и сузбијање тероризма на међународном нивоу, међутим нису понуђени прецизни критеријуми за одређивање када одређено дело можемо да сматрамо као „употребу силе“ или као „оружани напад“, односно које мере се могу предузети и до које мере како би се одржао или обновио међународни мир и сигурност. Постоји чак „подела између оних који се сајбер тероризмом баве на: „*hypers*“- они који верују да су се сајбер напади заиста и догодили - и „*de - hypers*“ - они који верују да се таква врста напада још увек није догодила“ (Dunn - Cavelty, 2008).

Међународна група експерата је у студији *Tallinn Manual* тумачила могућности примене Приручника о међународном праву у тумачењу сајбер сукоба и сајбер форме рата. Поменута група експерата предлаже да се све сајбер активности категоризују на основу два критеријума: „интензитету причињене штете и кршењу међународног права“ (Schmitt, 2013) и нуде категоризацију сајбер напада на основу четири степена. Први напади најнижег степена угрожености су напади чији интензитет не подразумева ништа више од једноставних неугодности по функционисање државе. Следећој категорији припадају напади другог степена интензитета

где убрајамо оне сајбер нападе који се дотичу нивоа „употребе силе“, што је предвиђено чланом 2 (4) Повеље УН – а: „сви чланови ће се у својим међународним односима уздржати од претње или употребе силе усмерене против територијалног интегритета или политичке независности било које државе или било којег другог начина који није у складу са циљевима Уједињених Нација“ (Повеља УН у: Schmitt, 2013, 47). Наредна категорија су сајбер напади који припадају трећем нивоу интензитета, јер угрожавају међународни поредак и представљају претњу по међународни мир и стабилност. Овакве врсте сајбер напада подразумевају активну укљученост Савета безбедности, и позивање на Резолуцију Савета безбедности приликом утврђивања обима претње или причињене штете, агресије или кршење мира. Поступање са оваквом врстом сајбер напада захтева привремене мере (економске или трговачке санкције) и / или даје овлашћења својим мировним снагама да употреби силу. Последња категорија су сајбер операције четвртог степена, чији је интензитет мерљив оружаном нападу. У овим случајевима постоји инхерентно право на самоодбрану, према поглављу VII UN (Schmitt, 2013, 42 - 54).

Слика 2. Ниво интензитета сајбер операција према одредбама Повеље УН (Pipyros et al., 2018, 375).



Адекватна одбрана и превенција изискују добро разумевање и познавање свих појавних облика сајбер напада којима се служе сајбер терористи. Аутори наводе постојање три основне врсте сајбер напада: „једноставно - неструктурирани, напредно - структурирани и сложено - координирани“ (Jalil, 2003; Fallico, 2013) сајбер напади. Први, „једноставно - структурирани“ сајбер напади за извршење не изискују комплексне алате и вештине управљања. Отуда ова врста припада најнижем нивоу сајбер напада по свом интензитету. Најчешћи пример је брисање / уклањање података (*data remove*), где нападач поседује основне вештине и служи се алатима које је направио неко други. Други, „напредно - структурирани“ сајбер напад подразумева да нападач поседује одређене вештине које су потребне за извршење напредније врсте сајбер напада. Односно, оваква врста сајбер напада захтева активности на више система и мрежа истовремено и умеће нападача да модификује или креира основне хакерске алате. Најчешћи пример ове врсте сајбер напада су онлајн пљачке са банковних рачуна. Трећа врста сајбер напада су најкомплекснији “сложено-координирани” сајбер напади, јер подразумевају виши ниво припреме и организације за спровођење напада, употребу софистицираних хакерских алата и знања за извршење масовних поремећаја употребом компјутера. Примери овакве врсте сајбер напада су: иницирање авионских несрећа, колапса у саобраћају, нестанка струје, иницирање телекомуникацијских ломова и др.

Акгар и сарадници указују да: „сајбер терор против земље и њених грађана може да се одвија на неколико нивоа софистицираности, при чему сваки ниво захтева способности у смислу технологије и инвестиција нападача. Причињена штета је директно пропорционална нивоу улагања“ (Akhgar, Staniforth & Bosco, 2014, 168). Даље, они разликују према скали причињене штете „три основне категорије сајбер напада: 1. напад на приступну мрежу организације (*attack on the gateway of an organization*), 2. напад на информационе системе организације (*attack against the organization's information systems*); 3. напад на основне оперативне системе (*attacks on an organization's core operational systems*)“ (Akhgar, Staniforth & Bosco, 2014, 168).

У зависности од размере причињене штете разликујемо три нивоа сајбер тероризма. У првом нивоу, сајбер терористи примењују најосновније и најједноставније врсте напада:

1) *Websites* напади који подразумевају директне упаде на интернет странице и онемогућавају приступ веб страници,

ометају њен рад тако што манипулишу информацијама и подацима, док је причињена штета краткотрајна и брзо решива.
2) *DdoS* напади представљају дистрибуирано порицање услуга. Најчешће мете напада су банке, мобилни оператери, пружаоци услуга кабловске и сателитске телевизије, разне берзанске услуге, медији и др.
3) Напади на *DNS (Domain Name System)* сервере – служе да усмере проток информација путем интернета пружајући одређене локације и информације на које нападачи желе да усмере интернет саобраћај. Ово се постиже тако што се захтев корисника пребацује са његовог рачунара на локацију нападача, а не на стварну локацију коју је корисник одабрао за претрагу или рад на интернету (*surf*). Поред ускраћивања услуга клијентима, најчешћа штета је крађа информација, што доводи у питање функционалност и репутацију сервиса. Такође, терористи се служе пропагандом својих активности и циљева, те им ова врста напада служи да преусмере интернет саобраћај на одговарајућу страницу и садржаје који их промовишу.

Други ниво на скали причињене штете у сајбер простору подразумева средњи ниво сајбер тероризма. Овде убрајамо различите нападе на информационе и рачунарске системе у којима се похрањују и обрађују подаци (сервери, базе података). За извођење овакве врсте напада потребна су напреднија технолошка средства и вештине, али и приступ рачунарима изнутра, односно учествовање запослених лица у организацији којој настоји да се нанесе штета и онемогући пружање услуга. Најчешће мете напада су банке, мобилни оператери и интернет провајдери. Јасна разлика између ове врсте напада сајбер терориста и трећег најсофистицираније облика сајбер тероризма је у томе што ови напади не резултирају физичким оштећењима, али се, ипак, ослањају на виртуелне услуге и приступ њима, те могу да произведу значајну штету. Као пример може да послужи напад на компјутере нафтне компаније у Саудијској Арабији познатој под именом *Aramco* који се догодио у августу 2012. године. Нападачи су користили компјутерски вирус *Shamoon* који је онеспособио функционисање 30.000 рачунара. Иако напад није утицао на основне оперативне системе компаније, угрозио је њен рад тако што су бројни подаци организације избрисани са рачунара, што је знатно отежало и успорило даљи рад компаније у дужем временском периоду. То се потом знатно одразило на нафтну индустрију и пореметило тадашњу равнотежу моћи нафтних компанија у тој земљи.

Трећа врста сајбертерористичког напада припада трећем нивоу према интензитету причињене штете јер подразумева напад на критичну инфраструктуру, односно основне оперативне системе који пружају подршку у свакодневном животу и раду. Ова врста сајбертерористичког напада је најсложена, подразумева употребу различитих технолошких средстава и може да се одвија на неколико различитих нивоа. Такође, сајбертерористички напад трећег нивоа изискује да сајбер нападач располаже напредним способностима и вештинама за руковање опремом за извођење сајбер напада, док је причињена штета директно сразмерна нивоу улагања. Најчешћи примери ове врсте напада су напади на системе који управљају и контролишу рад индустријског сектора неке земље (гориво и гас, водовод, струја, системи јавног транспорта или банкарски системи платног промета итд.). Овакве врсте сајбертерористичких напада су најсофистицираније, јер садрже у себи моменат када се причињена штета прелива из сајбер простора у реалност (физички свет) где узрокује штету великих размера, чији ефекти могу да буду значајно деструктивни по одређену државу и њену нацију.

Џелел је увидео „пет главних типова сајбертерористичких напада:

1) упад (*incursion*);

2) уништење (*destruction*);

3) дезинформација (*disinformation*);

4) одбијање услуге (*denial service*);

5) дискредитовање сајтова (*defacement of web sites*)" (Jalil, 2003, 8). Наведени напади се разликују по тежини причињене штете и циљевима.

Учесници и мете сајбер тероризма

Главни учесници терористичких активности су терористи (извођачи и организатори терористичких активности) и жртве (цивили или циљани политички званичници). Бављење тероризмом и његовим различитим формама подразумева и разумевање појма терористе. Тако на пример, „Уједињене нације сматрају да је терориста свака особа која, делујући независно од знања неке земље, или као појединац, или као члан групе која није призната као званично тело или део неке нације, поступа на тај начин што уништава или оштећује имовину цивилног становништва или влада да би постигао неки политички циљ“ (Гаћиновић, 2011, 23).

Интензиван технолошки развој и глобално умрежавање произвеле су нови облик тероризма, који је проистекао из интеграције човек - рачунар (социјална фузија и фисија). Социјална фузија која проистиче из те релације се односи на бројне предности које рачунари дају људима (бржа и лакша комуникација, базе података, претраживање и др.). Отуда настаје *IoT – The Internet of Things* актуелна системска парадигма која подразумева испреплетану мрежу перцепција, онлајн интеракције, друштвене односе и когнитивно мишљење. *IoT* представља „савршену интеграцију новог сајбер – физичко -друштвеног мишљења (*CPST, cyber – physical – social - thinking*) у сајбер простору, што настаје као резултат међуљудске интеракције, умрежавања различитих уређаја и манипулације у њима” (Ning et al., 2016, 504 - 522). Социјална фисија пак подразумева коришћење тих предности на деструктиван начин, било аутодеструктивно (социјална изолација) или деструктивно по ширу друштвену заједницу (сајбертерористички напад и сл). Обзиром да су „интернет и друштвене мреже идеално место за спровођење терористичких активности и операција јер омогућавају географски неограничене акције и њихово брзо спровођење“ (Wagner, 2005, 7), нова генерација терориста усмерена је на коришћење ових предности приликом извођења својих операција. На тај начин примена, развој и све већа доступност технолошких алата, нарочито информационих и комуникационих технологија у рукама терориста усложњавају потенцијалне претње од поменуте савремене форме тероризма, сајбер тероризам.

Сајбер тероризам представља спој људског и технолошког елемента. Сајбер простор пружа предности које омогућавају терористима да остану анонимни и формирају лажне IP профиле и адресе. Због комплексности и напредних карактеристика ИКТ

потребни су изузетни напори, напредно технолошко знање, као и оспособљеност најсавременијим технологијама и вештинама да би се утврдио идентитет починиоца сајбер тероризма, његова намера или евентуална политичка и финансијска подршка коју је терориста као извршилац имао. Адекватна одбрана од сајбер терориста, најпре подразумева адекватно суочавање, односно идентификацију и умеће да препознамо кључне карактеристике ове врсте тероризма. Јер, потенцијални сајбер терориста може да буде свако ко има непријатељске намере, добро знање из области информационих и комуникационих технологија и приступ поверљивим IT информацијама. Односно, да бисмо разумели тероризам важно је да разумемо ум, тј. психу терориста, као и да имамо у виду њихове генералне карактеристике као што су правдољубивост и мотивисаност идеологијама, политиком, религијама, осветом, било појединачно или у комбинацији. Наша представа о терористима као душевно поремећеним људима је погрешна. „На основу расположивих научних доказа о вези између насиља и менталних болести у популацији, насиље већином није узроковано великим психијатријским проблемима као што су шизофренија, биполарни поремећај или депресија“ (Swanson, 2012).

Истраживања су показала полна, старосна и класна обележја терориста. Углавном су то мушкарци. Међутим, жене и деца су неретко изманипулисани да се придруже терористичким организацијама, отуда се такође појављују као починиоци терористичких дела. Као пример могу послужити деца војници (Glazer, 2006, 373 - 384) и осмогодишњи бомбаши у Пакистану (Mohsin, 2013) и терористичким дејствима на Шри Ланки - Тамилски Тигрови (Murray, 2010). Класна „анализа више од 150 терориста Ал - Каиде показала је средњу и вишу средњу класу, високо образованих, ожењених мушкараца средњих година“ (Wasielewski, 2007, 13 - 18). Сент Клер као актере сајбер тероризма помиње: „терористичке организације, њихове симпатизере и тражиоце сензације“ (Saint-Claire, 2011).

Круцијални актери тероризма су терористичке организације (групације). Иако су материјали терористичких група транспарентни и лако могу да се пронађу на интернету, терористичке организације су релативно „затворене“ групације терориста које су базиране на поверењу и у тајности чувају своје методе напада и пооздане учеснике. Међутим, терористичке групације су доступне на интернету и њихови учесници комуницирају преко различитих (проверених) канала комуникације, нпр. преко *Cloud* платформи и *chat rooms* и др. Терористичке организације чије активности

предњаче на интернету су:

1) Ал - Каида (*Al - Qaeda*) – Многи припадници Ал Каиде поседују добро образовање у области инжењерства и технологије. Након организованог напада у Авганистану, новембра 2001. године када су америчке снаге изненада напале активисте Ал Каиде, многи од њих су били принуђени да побегну из Кабула. Тада је пронађено много осетљивих информација и докумената, које су оперативци Ал Каиде оставили за собом, који потврђују профил терористе као добро образованих и обучених за рад на компјутерима и оперативним системима: „Техничке скице на арапском, енглеском и немачком језику, студентске бележнице на арапском, турском, курдском и руском језику показале су доследност у интересовању и широко познавање електричног и хемијског инжењеринга, атомске физике, балистике, компјутера и радио станица“ (Davis, 2002).

2) ИСИС – Америчка компанија за сајбер безбедност „*Fire Eie*“ јавно је изјавила да ИСИС користи тамну мрежу (*dark web*)[4] у терористичке сврхе. На тај начин ИСИС може да обавља трговину сајбер оружја / алата на једноставан начин, без потребе за већим ангажовањем средстава и стручности (Auwema, 2015, 82).

3) ИРА (*Irish Republican Army*) – Након економских санкција које су САД и европске земље ставиле на Иран, ИРА је спонзорисала групу терориста за извођење сајбер напада као одговор на поменуту ситуацију (Menn, 2013).

4) Тамилски тигрови (*Liberation Tigers of Tamil Eelam*) - Најсмртоноснија терористичка група Шри Ланке, основана 1976. године, забрањена у преко тридесет земаља широм света. Ова терористичка група је била главни разлог за грађански рат у Шри Ланци. *Internet Black Tigers (LTTE)* су специјализована фракција Тамилских тигрова чији је основни циљ да штете влади Шри Ланке путем сајбертерористичких операција (Vidanage, 2006, 3).

5) Популарне радикалне групе од међународног значаја, попут либанских шиита (*Shi'ite Islamic group*), Исламска држава

4 *Dark web*, познат такође и под називима *deep web, deep net, invisible web* представља тамну, скривену страну интернета којој се може приступити само кроз специјализоване претраживаче. Користи се углавном за web комуникације које се не могу пресретати, отуда 57% dark web-а заузимају илегални садржаји као што су порнографија, недозвољене финансије, трговина дрогом, оружјем, кривотворена валута, терористичка комуникација и још много тога (Moore & Rid, 2016, 7-38).

- Хезболах из Либана (*Kataib Hezbollah*), користе интернет сајтове у различите сврхе: за објављивање чланака или планираних предстојећих догађаја, за објављивање недавно снимљених видео снимака итд. (Deutsch, 1996).

Поред терористичких организација, као актери сајбер тероризма се могу јавити и симпатизери којима је блиска идеологија терористичких организација, мада нису активно укључени у онлајн терористичке делатности. Трећој категорији актера припадају тражиоци сензације (*thrill seekers*). То су они нападачи који нису идеолошки везани за одређену терористичку групацију, односно њихов примарни мотив није политички или идеолошки, већ су вођени тежњом да достигну славу. Најчешће су то хакери који желе да прославе своје име (псеудоним) чињењем одређеног сајбер напада који захтева врхунске IT вештине, што им даје славу у виртуелној заједници.

Табела 6. Удео хакера у сајбер тероризму (Sproles & Byars, 1998)

Сајбер безбедност углавном угрожавају: хакери (професионалци и аматери), незадовољни запослени, сајбер криминалци, сајбер терористичке групе и други. Спролес и Бајерс (Sproles & Byars, 1998) су спровели истраживање на узорку од 100.000 хакера и показали процентуални удео хакера у сајбер тероризму: хакери - аматери су одговорни за око 90% свих терористичких активности на интернету, 9,9 % чине потенцијално професионални хакери и 0,1 % међународно светски познати сајбер криминалци (Табела 6).

Терористи углавном регрутују нове чланове пропагирајући

своје идеје, позивајући се на наводни апел за заштиту рањивих и угрожених друштвених група, ослањајући се на осећај неправде, отуђења и понижења. Односно, терористи углавном примењују „*narrowcasting*“ методу која подразумева узак одабир циљане субпопулације, те усмеравају пропаганду према њеним специфичним демографским карактеристикама (као што су старост или пол), друштвене или економске околности (Weimann, 2008). На пример, за регрутовање малолетника путем интернета терористи се служе пропагандом која је прилагођена дечјем узрасту; у облику дечјих прича, карикатура, популарних музичких спотова или компјутерских игара и других материјала који садрже поруке којима се промовишу и прослављају терористичка дела или самоубилачки напади. Неке терористичке организације су отишле даље у својим активностима тако што су финансирале и / или дизајнирале „онлајн“ видео игре које служе као средства за врбовање, упошљавање и обуку чланова кроз промовисање употребе насиља.

У научној јавности преовладава схватање да су циљеви терориста првенствено политички (верски, националистички или сепаратистички). Међутим, познато је да су мотиви и циљеви промењиве категорије, те да терористи могу својим циљевима да припоје и циљеве својих финансијера. Различити узроци и мотиви могу да наведу појединца да се бави тероризмом, како политички, етнички, верски, тако и идеолошки, економски – криза, сиромаштво, несигурност, социјални - аномија, социјална изолованост, психолошки - карактерне црте личности, одређене фрустрације, нагомилани стрес и незадовољство постојећом животном ситуацијом, идеолошки, геополитички, територијални – етносепаратистички, националистички и комбиновани. Терористе несумњиво карактерише примена насиља у остварењу циљева, како у реалном простору – физичка употреба насиља, тако и сајбер простору - дигитална употреба насиља која се рефлектује на причињену штету у физичком свету. Поменута примена насиља је управо оно што додатно модификује првобитне мотиве терориста и распламсава даље њихове тежње да на насилан, нелегитиман начин покушају да промене постојећу друштвено - политичку стварност, изазову рушење конкретне државне власти или изнуде одређене политичке уступке. Оно што карактерише починиоце терористичких сајбер напада је јасна усмереност на мету, добра организованост и коцентрисаност напада тако да они удружено имају веће шансе да нанесу озбиљну штету циљаној мети.

Последице сајбер тероризма

Правац технолошког развоја нас упозорава да су велики изгледи да ће сајбер тероризам постати популарнија претња у будућности. Нарочито смо сведоци брзог напретка и пораста броја високо квалификованих стручњака у области информационих и комуникационих технологија, као и константно растуће потребе за стручњацима из ове области. Истовремено, погодности које савремене технологије пружају уз релативно ниске трошкове и једноставност у извршењу намећу ову врсту сајбер напада као најједноставнију и најпрактичнију опцију за реаговање од стране терориста у савременом друштву.

Чињеница је да савремене државе у знатној мери ослањају функционисање кључних (виталних) структура на савремене технологије и компјутерске системе. Због тога је највећи изазов за сајбер терористе циљање на ICT технологије које подржавају рад кључних / критичних инфраструктура. Шта подразумевамо под критичном инфраструктуром? „Скуп мрежа, ентитета, система и структура које могу оштетити одрживост друштвеног поретка или јавне службе када престану да испуњавају своје функције делимично или потпуно“ (Yagli & Dal, 2014, 911). Критичне инфраструктуре 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, сва модерна војна опрема, комуникације војске и јавне безбедности, цивилне комуникације“ (Дамњановић, 2009, 245). Мада је критична национална инфраструктура генерално добро заштићена у већини земаља, никада није на одмет побољшање нивоа сигурности ових инфраструктура и јачи вид отпора против дела сајбер тероризма. Јер, без обзира на начин на који се сајбер тероризам испољава, када је главна мета напада критична инфраструктура, последице могу да буду катастрофалне.

Вилке (Wilke, 1999) указује на озбиљност претње од сајбертерористичких напада подсећајући да неки од поменуте врсте напада могу да произведу последице катастрофалних размера, било да се појављују у виду једног великог напада на критичну националну инфраструктуру, или у виду серије координираних, наизглед независних напада. Нујен такође указује на озбиљност последица сајбертерористичког напада, наводећи да је: „тумачење последица сајбер тероризма изазов и готово немогуће без узимања у обзир његових следећих карактеристика: 1. обим ефеката (*Scope*

of Effects); 2. непредвидљивост (*Unpredictability*); 3. реверзибилност штете (*Reversible Damage*); 4. анонимност и проблем приписивања одговорности, кривице за причињену штету (*Anonymity and the Problem of Attribution*)" (Nguyen, 2013, 1098 - 1106).

Сајбер нападачи најчешће, поред директног циља као што је напад на неки одређени сервер, системе или уређаје, брисање или модификовање кода на којем систем функционише, или измена сачуваних података, такође имају и индиректни циљ који теже да остваре. Тај крајњи циљ се односи на ефекте које извршени сајбер напад производи, односно на начин на који сајбер напад може да утиче на доношење људских одлука помоћу пласираних и обрађених информација од стране сајбер терориста. Генерално посматрано, сваки сајбертерористички напад производи индиректне ефекте којима њихови починиоци теже. Јер, након извођења сајбертерористичког напада ланчано се надовезују ефекати који у неким случајевима могу значајно да подсећају на оружани напад, па чак и да изазову смртни исход. Међутим, сајбер напади се значајно разликују од традиционалних војних напада. Превасходно, јер сајбер напади подразумевају софистицираније употребу оруђа / алата и оружја (ICT технологија, компјутерски системи). Док се за извођење традиционалног војног напада употребљава оружје које изазива директну физичку штету, што подразумева и ризик од повређивања по самог извршиоца, односно нападача услед његовог незнања, непажљивог руковања, незгоде и слично. Сајбер напад се може извести „из фотеље" далеко од циљане мете напада просторно и временски и не представља реалну физичку опасност од повређивања по самог починиоца, а истовремено може да причини штету великих размера. На пример, потенцијална величина штете је таква да је довољан само један злонамерни упадни код да се причињена штета аутоматски реплицира и брзо инфицира друге системе и избрише читав сет информација у рачунару.

Поменуте карактеристике, велика неизвесност последица, потенцијално широк опсег прекида рада оперативних система и оштећења, као и висок ризик од колатералне штете, чине сајбер тероризам најактуелнијом формом тероризма у савремено доба. На пример, Сафир црв (*Sapphire worm*) који је онемогућио рад сервера у Јужној Кореји на међународном нивоу је створио проблеме тако што је ометао рад интернет услуга у Тајланду, Јапану, Филипинима, Малезији, Индији, дисконектовао хитан 911 сервис и изазвао проблеме у раду 13.000 банкомата у САД (Schneier, 2003). То је допринело одлагању канадских националних избора и авио летова

2003. године. У мају 2021. *Kolonijal pajplajn* нафтовод је био мета хакерског напада, а неколико месеци раније у фебруару 2021. године је један хакер успео да упадне у водоводни систем града Флориде и покушао у њега да убаци опасну количину хемијског средства (Tajdi, 2021). На исти начин је могуће сајбер напад усмерити на војне ресурсе, те он лако може да прерасте у напад на цивиле. Ворен наводи „четири главна циља сајбер напада које спроводе терористи: онемогућавање непријатељских оперативних способности, уништавање репутације или погрешно представљање одређене организације, нације или савеза; убеђивање нападнутих да промене своју припадност и да демонстрирају својим следбеницима да су способни да причине значајну штету својим метама“ (Warren, 2002).

Најчешћи циљ сајбер терористе је да угрозе и / или онемогуће оперативне способности непријатеља. Стога сајбер терористи примењују оне врсте сајбер напада које озбиљно могу да оштете или униште функционисање непријатеља / мете и причине значајну штету целој нацији, или изазову економски колапс и друштвену кризу. У савременом друштву маркетинг и репутација представљају виталне елементе на којима савремене организације базирају своје активности. Отуда, други најчешћи циљ сајбер терористе подразумева наношење штете уништавањем репутације или погрешним представљањем одређене организације, нације или савеза. Терористи овај циљ најчешће постижу ширењем лажних гласина путем електронских медија (е-маил, веб сајтови и др.). Обзиром да медији имају велики значај у свакодневном животу, терористи управо зато хакују електронске медије како би пренели слику о изведеним нападима, својим циљевима и мотивима широм света и тиме показали својим следбеницима и широј јавности да су способни да причине значајну штету својим метама, да представљају озбиљну претњу и шире страх. Нека дела сајбер тероризма имају за циљ да наруше постојеће партнерске везе и савезе, и приволе нападнуте да промене „страну“ којој су до тада били лојални.

Последице тероризма могу бити различите, а његови ефекти „изузетно сложени, латентни и неретко представљају стратегијски ризик по безбедност државе и грађана услед: 1. угрожавања живота људи, односно њиховог повређивања и смрти као последица терористичких напада; 2. угрожавања здравствене безбедности људи; 3. угрожавања животне средине, биљног и животињског света; 4. дестабилизације економије и економског инвестирања; 5. угрожавања енергетске безбедности земље; 6. угрожавања социјалне безбедности; 7. угрожавања финансијске стабилности државе; 8.

демографске дестабилизације државе; 9. повећања националног и верског национализма и тензија; 10. експанзије тзв. медијског криминала; 11. умрежавања тероризма и других видова криминала, од којих је свакако најопаснија спрега са организованим криминалом и са криминалним (субверзивним) активностима обавештајних служби непријатељски настројених држава; 12. повећања корупције у јавном сектору; 13. угрожавања функционалности појединих државних ресора; 14. стварања неповерења грађана у државу и државне органе; 15. стварања неповерења грађана и државе у међународне органе и институције; 16. урушавања међународних односа и имица (угледа) земље на међународној сцени" (Милашиновић & Мијалковић, 2011, 9 - 10).

Шиндер сматра да су најчешћи акти рачунарског тероризма:

„а) електронска комуникација како би се спровеле одређене терористичке активности или регрутовали нови чланови терористичке организације;

б) саботажа ваздушног саобраћаја, како би се изазвала авионска несрећа или саботажа електронских пречишћивача воде како би изазвали загађење пијаће воде;

ц) упади у болничке и здравствене системе, како би се избрисала или променила база података пацијената и прописане методе лечења или напади на инфраструктуру за напајање, што може изазвати смрт великог броја људи који су на респираторима итд." (Shinder, 2002, 19). Вајмен сматра да су ефекти сајбер тероризма најштетнији применом напада на „бот мреже" и „*SCADA* системе" (Weimann, 2015, 157). „Ботнети или бот мреже" састоје се од великог броја компромитованих рачунара који су заражени злонамерним кодом и могу се даљински контролисати помоћу команди послатих путем интернета. Стотине или хиљаде ових заражених рачунара раде удружено како би ометали или блокирали интернет саобраћај циљаних жртава. Ботнет се може користити у *DDoS* нападима, *proksi* и *spam* услугама, за дистрибуцију малвера и друге организоване криминалне терористичке активности. Ботнети се такође могу користити за: сакупљање тајних података или за нападе на кључну инфраструктуру која велики део свог рада базира на интернету, као оружје у пропагандним или психолошким кампањама са циљем да се изазове страх, застрашивање или јавна срамота. Ботнети несумњиво постају главна претња и оружје савремених сајбер терориста, углавном јер могу да се дизајнирају тако да поремете рад циљаних рачунарских система на различите и за терористе делотворне начине, и могу чак да их изнајме за своје потребе, уколико терористи не

поседују довољно техничких вештина за њихово дизајнирање (Weimann, 2015, 156).

„*SCADA - Supervisory control and data acquisition systems*“ (супервизорска контрола и прикупљање података) је врста рачунарског система који прати и контролише функционисање кључних система (критичне инфраструктуре приватне и јавне). Ови системи применом различитих алата, као што су: програмски логички контролори, даљинске терминалне јединице и други уређаји за праћење и аутоматизацију контролишу: „пречишћавање и дистрибуцију воде, сакупљање и третман отпадних вода, рад нафтовода и гасовода, пренос и дистрибуцију електричне енергије, ветроелектране, системе цивилне одбране, рад сирена, праћење и контролу система грејања, вентилације и климатизације, потрошње енергије у зградама, аеродромима, бродовима и свемирским станицама“ (Weimann, 2015, 157). SCADA системи постоје од 1960. међутим нису били добро умрежени. Експоненцијални раст мрежа информационих система који међусобно повезују пословне, административне и оперативне системе, допринео је да приступ SCADA систему буде најатрактивнији циљ сајбер терористима, обзиром да би била каква измена података који се користе за оперативне одлуке или рад ових програма имала катастрофалне последице.

Генерално, тероризам је често конципиран као облик психолошког рата. Сврха готово сваког терористичког напада, па и сајбер тероризма је да уздрма и узнемири јавност. Психолошке последице које сајбер тероризам има по жртве и ширу јавност су значајне, независно од тога да ли је сајбертерористички акт довео до губитака људских живота, или до економског губитака. Директне жртве или мете насиља нису примарни циљеви терористичког деловања, већ насилни акти служе углавном као генератори порука. „Комуникација између терориста (организације), жртава (угрожених) и главних циљева (публике) заснована на претњама и насиљу, користи се за манипулацију главним циљем, претварајући их у циљ терора, циљ захтева или циљ пажње, у зависности од тога да ли се првенствено тежи застрашивању, принуди или пропаганди” (Schmid & Jongman, 2005, 28). Према томе: „сајбер тероризам се уклапа у циљеве терориста тако што улива страх у животе непријатеља. Сајбер тероризам може да се догоди без икаквог упозорења, а нема много тога што обични цивили могу да учине да би се заштитили од таквих напада. Ова неизвесност и непостојање контроле над сопственим светом омогућавају да свет види овакав облик тероризма као ужасавајућу опцију” (Weimann, 2015, 153).

Релација између сајбер тероризма и организованог криминала

Примарна безбедносна претња једне државе у прошлости је долазила од стране супротстављених држава, војних потенцијала и коалиција. Међутим, промене на глобалној сцени донеле су измењење околности. Различити недржавни актери постали су претња по националну безбедност. Организовани криминал је комплексна криминолошка појава која постоји у различитим облицима широм света. Организовани криминал представља константну опасност која се различито тумачи у националним законодавствима, тешко га је препознати и на њега адекватно реаговати.

Поједине криминалне организације током времена у значајној мери јасно профилишу своје активности, повезују се и остварују ближу сарадњу са сличним организацијама које се такође баве инкриминисаним активностима на државном и међународном нивоу. На тај начин настаје организовани криминал, односно поменута сложена криминална форма која је налик мрежи. Отуда Абадински предлаже да је за тумачење организованог криминала неопходно да разумемо „организацију групе и њено деловање, који по њему представљају суштинске делове овог савременог феномена, па тако наводи да је организација вољна да употреби насиље или да се служи подмићивањем, ради остваривања својих циљева или обезбеђења дисциплине“ (Abadinsky у: Шкулић, 2003, 38 - 39).

Деловање организованог криминала негативно се одражава на функционисање економског система државе, њену сферу привредно - политичких односа и сектор безбедности. „Организовани криминал представља добро организовану криминалну организацију, са строгом хијерархијом, дисциплином, одговорношћу, лојалношћу и поделом задатака, чији је циљ остваривање што већег профита и легализација незаконито стечене имовине, захваљујући постигнутом степену друштвеног угледа, било на основу продора у структуре власти или успостављених веза са органима власти, државним органима, легалним пословним привредним субјектима и утицајним политичким партијама и странкама“ (Бошковић, 1998, 9). Шкулић наводи опште услове који морају да буду испуњени за постојање организоване криминалне групе: „1) бројчани састав – групу морају чинити најмање три лица; 2) одговарајући временски континуитет – група мора постојати одређено време; 3) криминална циљна усмереност – група мора деловати споразумно у циљу вршења једног или више кривичних дела за које је прописана

казна затвора од четири године или тежа казна, те; 4) генерална сврха криминалног деловања – група чини кривична дела ради: а) непосредног или посредног стицања финансијске или друге користи или б) ради остваривања и задржавања утицаја на привредне или друге важне државне структуре“ (Шкулић, 2014, 2 - 3). Кључне одреднице организованог криминала су: мрежна структура са јасно утврђеним надлежностима и хијерархијом, виолентна природа, конспиративност у деловању, лојалност припадника групе, релативна трајност (континуитет у деловању), адаптибилност. Павлићевић наводи остале карактеристике: „специјализована подела рада између припадника; спровођење мера дисциплинске контроле; коришћење насиља или сличних средстава застрашивања; коришћење комерцијалне или друге сличне пословне структуре; учешће у прању новца; транснационални карактер и спровођење утицаја посредством легитимних социјалних институција – владиних институција (министарства правде, унутрашњих послова) или привредних институција“ (Павлићевић, 2017, 36 − 37).

Организовани криминал постоји у различитим формама. Хејген наводи четири типа организованог криминала према мотиву инкриминисане активности: „1. Политичко - социјални организовани криминал; 2. плаћенички или предаторски организовани криминал; 3. групно оријентисани организовани криминал и 4. синдикални или гангстерски организовани криминал“ (Hagan 2010, 298 − 299). Неки аутори организовани криминал виде као специфичну „нову форму геополитике“ (Giraldo & Trinkunas, 2010, 393). Деловања организованог криминала и терористичких група се временом све више прожимају и преплићу. Све до појаве наркотероризма појмови организованог криминала и тероризма су тумачени одвојено. Шели и Мелцер на примеру две студије случаја кријумчарења цигарета наводе заједничке карактеристике тероризма и организованог криминала: „финансирање на незаконит начин, имају сличну организациону структуру, служе се корупцијом и наменски организују своје пословање у областима са слабом контролом од стране државних служби, користе предности савремене технологије, исте технике за прање и трансфер новца, неретко и исте извршиоце“ (Shelley & Melzer, 2008). Шмид такође наводи неколико сличности између тероризма и организованог криминала: „рационално образложење, примена техника застрашивања, претње физичким насиљем и употреба сличних тактика“ (Schmid, 1996).

Мада постоје сличности између тероризма и организованог криминала, ова два облика криминалних делатности се јасно

и недвосмислено разликују. Оно што разликује организоване криминалне групе од терористичких је превасходно: неидеолошки карактер, ексклузивно чланство са строгом специјализацијом и поделом рада, постојање строгих интерних правила. Дакле, међународни тероризам такође карактерише: међународни карактер, мрежна структура, виолентна природа, лојалност припадника групе, али оно по чему се суштински разликује од организованог криминала је његов идеолошко - политички карактер. Примарни циљ организованог криминала је „стицање профита и моћи појединачно или у целини“ (Savona, Adamoli, Di Nicola & Zoffi, 1998, 6) односно стицање користи на незаконит начин. Када је реч о организованом криминалу „највећа добит се остварује трговином наркотицима, прањем новца, трговином оружјем или организованим крађама“ (Петровић, 1998, 37 - 39).

Чак и када организовани криминал садржи политичко - социјалну компоненту (деловање у сарадњи са терористичким групама, герилским организацијама, сарадња са разним друштвено - милитантним покретима) не подразумева криминалне активности чији је примарни циљ политичко - идеолошке природе, него је у питању прибављање тренутне користи или интереса организоване криминалне групе (прање новца, организовање трговине људима, отмица, производње и дистрибуције различитих наркотика, формирање лоби група итд.). Јер је „организовани криминалитет неиделошко удружење једног броја лица, које међу собом остварују врло блиске друштвене интеракције, организовано у хијерархијској основи, од најмање три нивоа - ранга, а са циљем обезбеђења профита и моћи, захваљујући учешћу у незаконитим и законитим активностима“ (Abadinsky, 1994, 38).

Криминалне групе које припадају организованом криминалу спроводе активности којима се крше међународне регулативе, али због неусаглашеног тумачења организованог криминала у различитим земљама је знатно отежана екстерна контрола поменутих активности и њихово откривање од стране безбедносних служби. Између организованог криминала и тероризма постоје међусобне релације које се манифестују на неколико начина: коегзистирају, сарађују или конвергирају (Puttonen & Romiti, 2020). Додирна тачка између тероризма и организованог криминала је као што наводе Мијалковић и Бошковић (Мијалковић & Бошковић, 2009) финансирање тероризма, односно „прљави новац“. Односно, терористичке организације су у тесној вези са осталим криминалним делатностима и актерима да би прибавиле материјална средства која су им неопходна за реализацију

планираних терористичких активности. „Да би могла да опстане, криминална организација нужно мора да користи насиље или нека друга средства попут застрашивања, као и да успостави спрегу са државним, политичким, економским и финансијским субјектима, било корупцијом, уценом, изнудом или неким другим начином“ (Бошковић, 1998, 53). Терористи врше тешка кривична дела (нуде услуге рекетирања, баве се кријумчарењем људи и дроге и слично) да би прибавили корист за себе или организацију којој припадају и тиме наносе штету појединцима и правним лицима (банке, компаније, мењачнице, поште, златаре и др). Несумњиво оно што одређује овај облик међународног организованог криминалитета је то што је он превасходно политички обојен. Такође, тероризам је углавном у спрези са неком државом, њеним органима или ужива заштиту неке политичке партије којој помаже да се домогне или одржи на власти, а чији се интереси заснивају на иредентистичким и сепаратистичким тежњама.

Повећана употреба дигиталних уређаја и експоненцијални раст знања и могућности које примена рачунара пружају указују да ће већина будућих злочина да садржи сајбер компоненту (Табела 7).

Табела 7. Процењена дистрибуција учињених кривичних дела које садрже сајбер компоненту (Davis, 2012, 277).

Прекршај	%
Превара / фалсификовање / крађа	79.3
Кривична претња	8.5
Онлајн злоупотреба малолетника / дечја порнофрафија	4.9
Сајбер напади / сајбер *squatting*	1.9
Остало	1.8
Насилни криминал	1.3
Кријумчарење дроге	1.0

Напомена: Због заокруживања одговори анкетираних не садрже укупно 100%

Трансформативна природа савремених ИКТ доводи до значајних изазова и отвара питања етике, јавне политике и безбедности. Традиционални злочини су јасно дефинисани у кривичном закону на националном нивоу. Међутим, многи од тзв. сајбер злочина се не уклапају лако у правну регулативу (Табела 8). Отуда аутори (Correia & Bowling, 1999) примећују да је XXI век почетак нове ере изазова за проналажење и спровођење адекватних

закона.

Табела 8. Процентуално приказани проблеми који отежавају истрагу кривичних дела са сајбер компонентом (Davis, 2012, 278).

Проблем	1	2	3	4	5	Просек
Немогућност праћења комуникација на интернету	8,8	8,0	16,0	26,4	40,8	3,82
Оскудна обука	9,5	8,7	24,4	26,0	30,7	3,60
Јавна апатија / недостатак свести	10,3	12,7	31,7	27,8	17,5	3,29
Питања надлежности	15,9	19,8	24,6	16,7	23,0	3.11
Недостаци размене информација / обавештајних података	9,6	27,2	25,6	23,2	14.4	3.06
Недостатак техничке стручности због смене запослених	32.5	17.5	16.7	15.9	17.5	2.68
Недостатак стандардних оперативних процедура	21.8	21.0	34.7	13.7	8.9	2.67
Напомена:	1- у потпуности се не слажем , 5- у потпуности се слажем					

Поред претходно наведених карактеристика које доприносе да се дела сајбер криминалитета тешко откривају и доказују његово ефикасно супростављање отежава: 1) тамна бројка, обзиром да се од укупног броја учињених деликата у сајбер простору само мали процент пријављује, односно евидентира код надлежних органа; 2) недовољна информисаност и познавање ове врсте криминала; 3) релативно нов појам; 4) информациона и комуникациона технологија и њен развој нису подједнако доступни у свим државама (развијене земље имају боље могућности и приступ најсавременијим технолошким иновацијама); 5) сајбер криминал измиче строгом територијалном одређењу, јер није уско везан за територију, као традиционални облици криминала, односно одликује га транснационалност; 6) просторна прикривеност, односно отежано просторно одређење обзиром да се сајбер криминал дешава у онлајн окружењу (сајбер простору); лако превазилази просторне границе и као такав је тешко ухватљив и уочљив; 7) временска прикривеност пружа могућност вршења кривичног дела великом брзином. Од момента извршења кривичног дела до испољавања последица по жртву (физичко или правно лице) може и не мора да постоји временска дистанца; 8) прикривеност због различитих мотива, као што је на пример очување репутације. То је уједно најчешћи мотив

прикривања сајбер криминалних радњи код привредних субјеката који послују путем електронског банкарства, трговине и сл.

Друга страна медаље научно - технолошког прогреса је то што су савремене информационе и комуникационе технологије постале значајно средство за функционисање и одржавање сложених криминалних система, као што су организовани криминал и тероризам. Дакле, ИКТ су истовремено једно од најзначајнијих средстава за извршење и откривање криминалних дела. Отежавајуће околности за откривање криминалних дела која садрже сајбер компонентну чине сасвим очекивано да везе између организованог и сајбер криминала у будућности рапидно расту.

4. САЈБЕР ПРОСТОР

Сајбер тероризам обједињује у себи виртуелни сајбер простор и терористичку активност, односно то је „конвергенција између сајбер простора и тероризма (Denning, 2001, 242). Да бисмо разумели сајбер тероризам неопходно је да разумемо виртуелни простор, његове карактеристике и могућности. У литератури је у употреби термин сајбер простор и његови синоними: кибернетски простор, киберпростор, виртуелни свет, виртуелни простор, дигитални свет, онлајн свет. Иначе, појам сајбер (*cyber*), потиче од грче речи *kybernetes* што значи онај који влада, управља.

Интензивна динамика технолошког развоја, нарочито од деведесетих година довела је до све веће доступности рачунара широм света и пораста броја корисника. Терористи се служе онлајн платформама у различите сврхе: „1) психолошки рат; 2) пропаганда; 3) онлајн индоктринација; 4) регрутација и мобилизација; 5) претраживање података; 6) виртуелна обука; 7) планирање и координација, и 8) прикупљање средстава“ (Weimann, 2015, 24).

Сајбер простор представља значајан део инфраструктуре савремених развијених земаља и обухвата скоро све секторе који су значајни за функционисање савременог друштва. Дакле, сајбер простор је постао жариште иновација, рада, друштвених релација, комуницирања, криминала и ратовања, јер подразумева широк дијапазон различитих могућности и активности (офанзивних и дефанзивних) које су интересантне различитим актерима (индивидуе, друштвене групе и др.). Сајбер простор је комплексан простор који поред осталог садржи посебне мреже које су дизајниране са неком специфичном сврхом, па су као такве у одређеној мери „изоловане“ од интернета и доступне искључиво својим корисницима. Бројне могућности које сајбер простор нуди несумњиво олакшавају комуникацију и активности у сајбер простору, али управо те бројне могућности остављају простора за разне злоупотребе као што су: манипулација противником или његовим потенцијалним одлукама, циљање на одређени информациони медијум (на пример бежичну приступну тачку), преношење неке поруке (шифрована порука у информационој димензији), стварање сајбер персона (онлајн идентитет који олакшава комуникацију, одлучивање и утицање на јавност у когнитивној димензији) и др.

Дешавања, последице и неизвесности у сајбер простору се „преливају“, односно стварају позитивне или негативне ефекте у реалном (физичком) свету и на тај начин га редефинишу. Све већи ниво међузависности између физичког и виртуелног света, немилосрдно намеће изазове и отвара врата за непредвидиве рањивости, претње и

ризике којима је константно изложен сајбер простор. То је условило све већу забринутост за савремену безбедност, док се као кључна питања намећу питања: сајбер безбедности, сајбер простора и његове одбране. Тумачење, анализу и класификацију поменутих феномена додатно отежава и језичка баријера, односно то што су термини преузети из енглеског у српски језик. Израз *cyberspace* појавио се први пут у САД.

Сајбер простор је виртуелни (замишљени) простор који постоји помоћу интернета и савремених информационих и комуникационих технологија. Он коегзистира као засебна целина унутар реалног света и поседује своја правила, институције, информације (знање) и друштвену праксу. За његово функционисање неопходно је мрежно повезивање рачунарских система - интранет, *LAN, WAN* и др. Дакле, реч је о ширем појму од интернета. Интернет подразумева физичку димензију, сачињен је од физички опипљивих елемената (технолошка средства која су повезана тако да чине функционалну инфраструктуру). Док, сајбер простор представља сложенију појаву и подразумева поред физичке инфраструктуре и људску активност која чини интернет (*World Wide Web*) могућим, односно подразумева и не - физичку димензију. Основни предуслов за постизање сајбер безбедности је идентификовање елемената сајбер простора.

Структурално посматрано, сајбер простор чине три слоја. Први слој чини физички видљив и опипљив део, његова инфраструктура, мрежни и преносни уређаји подршке. Други је софтверски и односи се на део који су људи начинили као програмски систем подршке и инструкција како би сајбер простор функционисао. Трећи слој су информације које настају као резултат интеракције прва два дела, односно техничке подршке и људске интервенције - машина и људских програма, инструкција којима се подаци обрађују и креирају у информације које се потом преносе брзо и ефикасно даље без обзира на географску удаљеност. Дакле, сајбер простор је нематеријални виртуелни (*online*) простор који настаје употребом дигиталне технологије помоћу које се обавља onlajn комуникација, у „свету за себе“, који је фундаментално одвојен од реалног (стварног) света, који егзистира у *offline* моду. Многи аутори, међу њима и Вајнсток (Weinstock, 2000) указују да овај вид комуникације све више постаје део *offline* света. Међутим, поменута дигитална комуникација се значајно разликује од *offline* комуникације.

Сајбер простор је комплексан феномен који карактерише велики број корисника. Очекује се да ће његова актуелност и број корисника у будућности упоредо са технолошким развојем да расте.

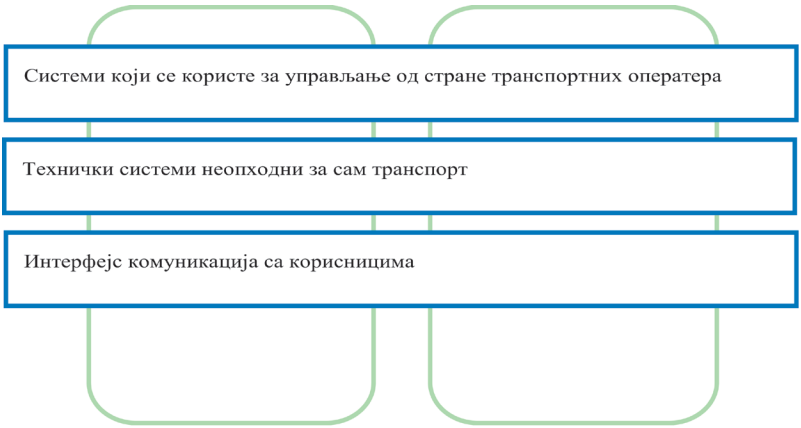
Различити актери вођени различитим мотивима делују унутар сајбер простора (појединци, организације и др.). Доган примећује две циљано орјентисане групе актера: „тимове мамаца (*troll army*) - спонзорисани су од стране државе, поседују лажне идентитете које користе као учесници у блоговима, интернет форумима и на друштвеним мрежама у циљу пропаганде, креирања перцепције јавног мњења, подривања дисидентских структура и слично; тимови за креирање групног мишљења (*swarm stream teams*) - циљно оријентисана група људи која се служи сајбер простором да агресивно шири виралне (вирусне) видео садржаје којима разбијају поруке противника или одређених медија“ (Duggan, 2015, 14).

У Речнику компјутерских термина сајбер простор је дефинисан као „окружење виртуелне реалности у коме особе комуницирају помоћу повезаних рачунара“ (Тасић, В. & Бауер, 2003, 125). 2012. године Америчко министарство одбране га дефинише као: „глобално подручје у оквиру информационог окружења које је сачињено од међузависне мреже инфраструктуре информационих технологија, укључујући интернет, телекомуникационе мреже, рачунарске системе и уграђене процесоре и контролере“ (Scaparrotti, 2014, II9, 5 a). У „Стратегији за борбу против високотехнолошког криминала за период 2019. - 2023. године“ је наведено да се „под „сајбер простором” подразумева или врста „заједнице” сачињене од мреже рачунара у којој се елементи традиционалног друштва налазе у облику бајтова и битова“ или „простор који креирају компјутерске мреже” („Службени гласник РС“, бр. 71/18). Дакле, то је виртелни простор који је сачињен од испреплетаних рачунарских мрежа из целог света којима се повезују крајњи корисници и тиме омогућава њихова несметана комуникација било путем аудио, видео, гласовних, *e-mail* или шифрованих порука. То је „нова форма менталне димензије људске егзистенције унутар које настаје симулирана реалност као последица интеракције између људског и артифицијелног интерфејса. Представља алтернативну просторну димензију унутар које се успоставља веза између различитих персоналних рачунара, рачунарских мрежа, различитих виртуелних заједница и појединаца“ (Мимица & Богдановић, 2007, 60).

Аутори (Tonhauser & Ristvej, 2019, 1593) који су се бавили анализом статистичких података о различитим облицима напада у сајбер простору дошли су до закључка да је 95% нарушавања сајбер безбедности последица људске грешке / људског фактора. Остале рањивости сајбер простора су последице лошег вођења ИКТ система и недостатак кредибилних стратегија за превенцију од сајбер напада

и за ефикасно супростављање од поменутих врста напада. Аутори наглашавају да питањем сајбер безбедности не треба да се баве само ИТ стручњаци. Указују на значај сарадње, едукације доступним лекцијама и размену најбољих пракси између заинтересованих страна које поседују сличну инфраструктуру и системе. Такође наглашавају да су кризни менаџмент и процене ризика подједнако примењиви у сајбер простору и нуде класификацију кључних система за изградњу ИКТ инфраструктуре, чије је разумевање неопходно за достизање безбедности у сајбер простору (Слика 3).

Слика 3. Класификација кључних система за изградњу ИКТ инфраструктуре (Tonhauser & Ristvej, 2019, 1592).



Аутори (Tonhauser & Ristvej, 2019) су навели да „одвајање“ ових система и држање њихових делова ван мреже би унапредило безбедност сајбер простора, јер би се избегла ланчана реакција. Међутим, нажалост увидели су да то више није могуће јер би дугорочно донело више потешкоћа него безбедносних добитака. Јер, ови системи нису само међусобно повезани, већ и међусобно зависни што значи да не могу правилно да функционишу један без другог.

Виртуелне заједнице

Интернет је омогућио успостављање виртуелне комуникације и настанак виртуелних заједница. Савремене информационе и комуникационе технологије пружају могућност да свако ко има приступ интернету може да приступи информацијама са било којег места. Постоје различите веб странице, блогови и групе за ћаскање (онлајн дискусије) у којима људи размењују жељене информације и повезују се у виртуелне (*online*) заједнице.

Виртуелна комуникација је релативно нови облик комуникације, који карактерише једноставан и брз пренос информација, било путем рачунара, бежичних *wireless* уређаја, мобилних телефона и др. Твитер (*Twitter*), Фејсбук (*Facebook*), Инстаграм (*Instagram*) и ТикТок (*TikTok*) су јавни профили чији корисници могу да објављују (постују) своје статусе готово свакодневно. Јавни профили постају важан део идентитета савременог појединца (Murthy, 2012; Boon & Sinclair, 2009). На пример Твитер (*Twitter*) функционише на следећи начин: „(1) корисници имају јавни профил у којем емитују кратке јавне поруке или их ажурирају, усмеравају на одређене кориснике или не, (2) поруке постају јавно агрегиране између корисника, и (3) корисници могу да одлуче чије поруке желе да примају, али не и нужно ко може да прати њихове поруке; ово се разликује од већине друштвених мрежа где је праћење (*following*) једних према другима двосмерно (тј. узајамно)“ (Murthy, 2012, 1061). Корисници друштвених мрежа конзумирају интернет услуге на основу својих интересовања, што их најчешће доводи у интеракцију са људима које лично не познају. На тај начин наизглед баналан *tweet* постаје важно средство помоћу којег појединац гради и потврђује свој идентитет на друштвеним мрежама.

Дакле, различите услуге на интернету пружају корисницима да формирају и ажурирају јавни или полу - јавни профил путем којег корисници могу да се повезују са другим корисницима и на тај начин формирају виртуелне заједнице. Виртуелне заједнице представљају нову друштвену форму која се разликује од класичних самим тиме јер не подразумева директне контакте „лицем у лице“, познанство и реалну присутност у простору и времену, већ се интеракције међу корисницима остварују у виртуелном простору уз неопходну употребу интернета и савремених ИКТ.

Виртуелне (онлајн) заједнице постоје у много различитих облика, окупљају чланове на различитим претпоставкама и разликују се по величини, односно броју корисника, али и фази свог развоја.

Виртуелне заједнице, као и остале друштвене заједнице током времена пролазе кроз „пет фаза развоја: 1) потенцијал, 2) спајање, 3) сазревање, 4) управљање и 5) трансформација“ (Wenger, McDermott & Snyder, 2002, 69). У првој фази виртуелна заједница представља лабаву мрежу људи који имају идеју да формирају виртуелну заједницу, њену структуру, идентификовали су и договорили одабране чланове на основу заједничког именитеља (интересовања). У другој фази, виртуелна заједница је званично покренута, почињу заједничке активности и праксе. У поменутој фази главни фокус је на утврђивању вредности. Трећа фаза развоја виртуелне заједнице је њено сазревање. Чланови виде празнине, развијају и размењују савете за ravoj нових области заједнице. У тој фази међу члановима се изградио одређени ниво поверења и познанства. Затим виртуелна заједница пролази кроз четврту фазу у којој је највећи изазов да одржи свој замах. Последња фаза је трансформација која настаје као резултат неке велике промене у пракси или организацији рада, попут догађаја као што су велики прилив нових чланова, промена руководства или значајан пад нивоа енергије који покреће потребу за обновом. Тада виртуелна заједница може да се формира изнова на новој основи или једноставно да се угаси (нестане).

Неке виртуелне заједнице повезују чланове примарно на основу сличних интересовања, без обзира на географску удаљеност и претходно познанство својих чланова, неке примарно пружају интеракцију међу познаницима, пријатељима, члановима породице или сарадницима, док се неке виртуелне заједнице фокусирају на питања која су релевантна за одређени географски регион, суседство, тему и на основу тога окупљају своје чланове. Број учесника виртуелних заједница је у порасту због бројних могућности и олакшица као што су: брза (и јефтина) комуникација на великим удаљеностима, могућност учешћа старих и/или немоћних, маргинализованих, омогућавајући људима чији се интереси не уклапају и/или превазилазе начин живота у локалној заједници да пронађу друштво и савет изван заједнице становања.

Кључна одредница виртуелних заједница је да су то групе људи које се повезују путем свог учешћа у рачунарској мрежи. Иако виртуелне заједнице настају посредством информационих и комуникационих технологија и постоје једино у виртуелном (сајбер) простору, оне су истините као и заједнице које постоје у физичком простору *face – to - face*. Онлајн заједнице поседују карактеристике заједница у реалном физичком свету и пружају осећај припадништва и сигурности код својих чланова. Такође и у виртуелним заједницама

чланови могу да манипулишу одређеним информацијама, да их добију или пруже, воде дебату, преговарају или критикују физичку реалност. Истраживања су потврдила да су интровертне и анксиозне особе знатно више учесници виртуелне комуникације (Chak & Leung, 2004) и да су чешће чланови виртуелних мрежа, јер на тај начин ублажавају потешкоће које имају у социјалној интеракцији.

Сајбер култура

Постоји много дефиниција културе. Једна од њих дефинише је као „друштвено наслеђе које појединац добија од своје групе“; „начин мишљења, осећања и веровања“, „апстракт понашања“ (Герц, 1998, 11). Генерацијско преношење културних добара и вредности на чланове заједнице је једна од основних функција културе. Иако се култура превасходно односи на друштвено наслеђене и научене обрасце мишљења одређене групе људи, заједнице или друштва, то нипошто не значи да култура не садржи компоненту индивидуалности.

Припадници различитих друштвених група развијају своје посебне врсте културе, што је у литератури познато под називом поткултура или субкултура. „Један посебан, релативно затворен сегмент опште културе, чији припадници деле заједничка уверења, обичаје и вредности, а често и начин облачења, исхране, понашања и моралне норме” (Виденовић, 2015), а разликује се и „издваја“ од културе шире заједнице којој та група припада називамо субкултура. Уз овај термин често се користи и термин контракултура, обзиром да припадници одређене субкултуре доминантне вредности неке заједнице или одбацују (не у целости), или тумаче на себи својствен начин. Иако субкултуру везујемо искључиво за културне садржаје одређене друштвене групе, слоја или средине, она не представља изолованост, него културну шароликост. Субкултура се „може аналитички рашчланити и дефинисати на следећи начин: а) у односу на универзалну културу, поткултура представља релативно заокругљену, самосвојну и идентитарну целину; б) њу чине вредности, правила и норме које чланови групе усвајају и практикују на дуже време, следе и продужавају; в) поткултуре репрезентују особености социјалних група, слојева и њихових положаја; д) поткултурне групе су креатори и власници различитих стилова“ (Божиловић, 2004, 53 - 54).

Интеракције и комуникација актера у сајбер простору подразумевају стварање виртуелних идентитета који теже да се потврде у алтернативној стварности кроз виртуелне заједнице и своју сајбер културу. Сајбер култура представља нову форму културе, односно субкултуру која је настала као резултат учесника онлајн активности. Друштвени актери су осетљиви на правила и услове поретка у реалном физичком свету, међутим виртуелне активности пружају већу слободу (формирање лажних профила) што за собом повлачи и евентуалне негативне бихејвиоралне ефекте.

У виртуелном свету је омогућено самостално обликовање животног стила и улога, односно дате су могућности за одабир идентитета, виртуелног окружења, као и могућност одабира жељеног учесника у комуникацији. „Док се питају шта желе, учесници поткултура симболички обележавају поље деловања, а самом појавом на одређеном месту они изражавају разлике у склоностима. Повезивањем са изабраном поткултурном групом, младићи и девојке теже да се издвоје од примарних друштвених заједница којима припадају и да се удаље од улога које су им намењене. Напуштајући место репресивних очекивања, бар привремено, неутралишу важење строгих захтева и отписују значај поретка који их одбија“ (Марић, 1998, 160).

Много тога што дефинишемо као део сајбер субкултуре се састоји у личном или политичком блогирању, активизму друштвених медија на платформама као што су *Facebook*, *Twitter*, *Instagram*и др. (Kahn & Kellner, 2004). Блогови су посебно дизајниране мреже за вођење дијалога и дебата, размену алтернативних информација, демократско самоизражавање и политичку критику и сл. Дела Порта (Della Porta, 2012, 49) је такође тврдила да су нове технологије побољшале комуникацијско поверење код друштвених покрета, који их углавном користе за мобилизацију истомишљеника.

Термин онлајн служи да означи читаву лепезу виртуелних привида, комуникација, свеприсутних дешавања и укључења у виртуелном простору који је добрим делом везан за имагинарно, али је истовремено део нашег савременог готово свакодневног искуства. Онлајн дешавања могу довести до пребрзог снажног емоционалног везивања и стварања илузије да се познаје особа са којом се виртуелно комуницира, углавном због имагинације која је неизоставан део процесуирања активности на интернету. Исто се дешава и са формирањем сајбер културе, која иако повезује онлајн учеснике, који се у већини случајева ни не познају у реалном свету, код својих чланови ствара истоветан осећај припадања као и када је реч о било каквој врсти субкултуре у реалном свету.

5. ЗЛОУПОТРЕБА САВРЕМЕНИХ ИНФОРМАЦИОНИХ И КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА

Научно - технолошка револуција изнедрила је савремене револуционарне технолошке изуме који су значајно променили човечанство у готово свим областима људског постојања. Интернет представља најефикаснију савремену методу комуникације, јер омогућава брзу и једноставну манипулацију подацима различите врсте (аудио и видео) и нуди широк дијапазон идеја и информација. Вајмен као „основне предности интернета 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, 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 уобличава извештавање у традиционалним масовним медијима, који све више користе интернет као извор својих информација" (Weiman у: Дамњановић, 2009, 238 - 239). Употреба интернета и савремених ИКТ постали су неизоставни део свакодневнице. Због бројних погодности које интернет и ИКТ нуде, расте и њихова примена, док истовремено расте и потенцијал за њихове различите злоупотребе. Брз проток информација на интернету омогућава брзо ширење компјутерских вируса, црва, тројанаца и других злонамерних софтвера, што уз генерално незнање корисника интернета о постојећим мерама заштите, чини да интернет буде извор многих проблема и изазова. Корисници интернета углавном не поседују довољно знања да би користили бројне услуге које интернет пружа безопасно. Штавише, „корисници интернета су углавном недовољно упознати са функционисањем рачунара, и врло често нису спремни и вољни да предузму мере заштите за које они сматрају да су сувише скупе, превише технички захтевне или да је потребно утрошити превише времена на њихову употребу" (Abrams, Podell & Jajodia, 1995, 117). Применом теорије друштвене контроле и едукацијом о правилном / забрањеном понашању, као и претњама у сајбер простору можемо значајно да спречимо или барем умањимо малициозне активности на интернету. Теорија социјалне контроле има потенцијал да пружи и / или прошири знање и свест о сајбер криминалу и осталим злоупотребама интернета (Luknar, 2022b). Јер, уколико злоупотребе на интернету измичу кривично - прекршајном процесуирању то може да има за последицу пораст насилног понашања у сајбер простору.

Интернет сам по себи није узрочник криминала, али је „једноставно моћно средство комуникације које има потенцијал

да појача и убрза криминал“ (Williams, 2008). Научно - технолошка револуција омогућила је великом броју људи приступ информацијама, што је утицало на криминогено окружење тако што га је трансформисала и створила нову форму криминала у сајбер простору (Britz, 2013, 3, 75 - 76). Већина превара на интернету су у ствари само усавршене верзије ранијих, класичних превара и криминалних дела у које је интернет донео новине. „Њихова девијантност, подржана моћном технологијом, може имати врло озбиљне и обимне последице по друштво. Дакле, свиђало се то неком или не, они постају респектабилни чланови клуба криминалаца са белом - крагном. Рађа се нова елита под називом сајбер елита. Оно што се никако не би смело превидети је висока вероватноћа обједињавања, ради заједничког деловања, ове новонастајуће елите са девијантним делом класичне моћне елите“ (Петровић & Стојановић, 2016, 13).

Најчешћи облици злоупотребе интернета су: 1) хаковање, 2) незаконито прикупљање података, 3) кривично дело пресретања података, 4) ометање података, 5) интернет рекетирање, 6) фалсификовање, 7) прање новца, 8) интернет инвестиционе преваре и 9) прекршаји на интернету везани за садржај. Хаковање је активност на интернету коју можемо тумачити двојако. Истовремено може да представља кривично дело које се врши путем интернета и подразумева нелегални упад у компјутерске системе и може да представља позитивно деловање, нарочито у сфери заштите од познатих рањивости и најчешћих напада с циљем успостављања боље сигурности рачунарских система и података. Дакле, карактеришу га различити циљеви и мотиви, а за његово извођење су потребне припремне радње, приступ заштићеним (тајним) подацима лозинкама или употреба за то предвиђених хардвера или софтвера. Други најчешћи облик злоупотребе на интернету је незаконито прикупљање података. Овде убрајамо нападе на базе података из веб апликација којима се прибављају поверљиве информације, као што су *Cross - site scripting – XSS* (Vernotte et al., 2014) и *SQL injection* (Halfond, Viegas & Orso, 2006). Наредна врста злоупотребе на интернету је кривично дело пресретања података које се односи на ометање трансфера података, информација и њихово снимање, било да се комуникација одвија путем интернета, бежичног или *wifi* (*e - mail*, *chat*, и др.) или фиксне линије. Мета напада је комуникациона инфраструктура. Такође у малициозне активности на интернету убрајамо ометање података које означава врсту напада, углавном усмерено на ометање и брисање података који су чувани у

компјутерским системима. Најчешће се изводи помоћу *Trojan Horse* софтвера, црва (*Warms*) и др. Затим следи, интернет рекетирање, односно ометање рада система. Нападачи прете *DoS* нападом (*Denial – o f -service attack*) и уцењују компаније које остварују своје пословање електронским путем, као што су: електронско банкарство и е - продавнице, пружаоци е - услуга и коцкања путем интернета и др. Најчешће вирусима и програмираним мрежама компјутера за извођење организованих *DoS* напада ометају пословање тих компанија, нападају вебсајтове и онемогућавају њихове услуге, нападају сервере или рачунарски систем. Интернет и компјутерске алатке: исеци (*cut*), залепи (*paste*) или копирај (*copy*), омогућиле су да се жељени део текста или документа исеца или копира са његове оригиналне верзије и лепи (*paste*) на лажни документ. Некадашње кривично дело фалсификовање је осавремењено употребом интернета и осталих технологија. Што је озбиљност фалсификата већа, захтева и већу умешност и познавање различитих програма на рачунару. Савремене информационе технологије и глобално финансијско тржиште омогућиле су теже праћење токова новца и његове лакше злоупотребе. Посредством интернета се такође обавља и прање новца, односно „нелегално прикривање незаконитог профита од стране појединаца, малих предузећа, корпорација, криминалних синдиката, корумпираних званичника, па чак и корумпираних влада“ (Britz, 2013, 106). Правна регулатива у вези са банкарским пословањем није уједначена свуда у свету. Тако су у неким земљама банке законом заштитиле своје пословање тзв. банкарском тајном, док су у другим земљама банке дужне да подносе редовне извештаје о свом пословању. Таква ситуација отвара простор да појединци перу новац тако што га анонимно депонују у земљу са правном регулативом која им погодује, а потом одатле могу да пребаце новац и неометано га користе у било коју другу земљу. Ни инвеститори нису остали имуни на предности које интернет пружа. Једноставно и брзо приступање различитим инвестиционим изворима, као и невероватно лака трговина хартијама од вредности учиниле су да интернет буде прихваћен као важан алат за инвеститоре. Међутим, инвестирање само по себи носи одређену дозу ризика, који су се са применом интернета у овој области увећали. То потврђује велики број и различите врсте инвестиционих превара (е - инвестициони билтени, инвестициони веб сајтови о лажним фондовима, *spam* пошта и др). Једна врста злоупотребе на интернету су прекршаји везани за садржај, који се односе на промовисање садржаја који је законом забрањен у већини земаља. То су: дечја порнографија,

садржај који подстиче ксенофобију и вређање на етничкој, расној, религијској или полној основи и др.

Дакле, злоупотребе интернета се могу јавити у различитим облицима. Можемо их систематизовати у две главне категорије: „упад у системе и *DoS* нападе“ (Nguyen, 2013, 1093). „Упад“ подразумева напад на рачунарске системе који се ослања на пропусте, односно „рупе“ у систему које нападачи користе као прилику за упад у одређени систем како би приступили његовим ресурсима и испоручили жељену алатку (вирус или малвер). Малвер је „код или софтвер који је посебно дизајниран да оштети, наруши, украде или уопште нанесе штету или нелегитимно утиче на податке, хостове или мреже“ (Nguyen, 2013, 1094). Нападачи примењују *DoS* напад да онемогуће пружање услуга одређеног система.

Терористи такође користе интернет у различите сврхе. Вајмен наводи да „активности терориста на интернету можемо да класификујемо у 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“ (Weimann у: Дамњановић, 2009, 239). На интернету се могу пронаћи разни садржаји о терористима: терористички вебсајтови, снимци терористичких напада, чак и е-обуке терориста и др.

Сајбер криминал

Експанзија аутоматизованих информационо - технолошких система производи константне изазове и безбедносне ризике. Традиционална кривична дела као што су разне врсте превара, фалсификовање, проневере новца и крађе у сајбер простору попримили су нов облик и начин извршења. Употреба компјутерских технологија за извршење кривичних дела изискује стварање нове регулативе и мера кажњавања за поменуто противправно понашање. Зато је појму општег криминалитета неопходно додати и „компјутерски криминал као обележје прогресивног криминалитета" (Ђокић & Живановић, 2005, 305 - 318).

У литератури се помињу различити називи: „сајбер криминал" (Clay, 2007, 4), „компјутерски криминалитет" (Gercke, 2012, 11), „високотехнолошки криминал" (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, „Службени гласник РС" број 61/05, 104/09), „*computer abuse* - злоупотреба компјутера, *crime by computer* - деликти уз помоћ компјутера, *computer fraud* - компјутерска превара, информатички криминалитет, сајбер криминалитет, техно криминалитет" (Јовашевић, 2011, 639) да означе посебну врсту криминалних радњи за чије извршење су коришћене ИКТ и интернет.

Сајбер криминал угрожава безбедност сајбер простора у целини, или појединих његових делова. Починиоци сајбер криминала се служе различитим средствима унутар рачунарских система како би прибавили противправну корист за себе или учинили штету неком физичком или правном лицу. Сајбер криминал обухвата: „крађу интелектуалне својине, кршење права заштите патента, тајне трговине, кршење закона о ауторским правима, нападе против рачунара којима се намерно утиче на обраду података" (Clay, 2007, CRS - 4). Могућности злоупотребе информационих технологија су велике: „Рачунар или уређај може да буде заступник злочина, помоћно средство за извршење кривичног дела или мета злочина; злочин се може догодити на самом рачунару, или на не - виртуалној локацији" (Gordon & Ford, 2006, 14). Термин сајбер криминал користи се да означи широк спектар криминалних поступака, односно не обухвата само нападе који се могу извести употребом телекомуникационих мрежа, него и нападе на саме информационе системе, компјутере, као што су: шпијунаже, откривање и пресретање тајних података и њихово неовлашћено копирање, ометање обраде података, крађу интелектуалне својине, ауторских права или патената, дистрибуцију

различитог садржаја (вируса, дечје порнографије и др.), преваре путем интернета и мејлова, мешање у онлајн финансијске услуге и бројне друге. Управо због тога је проистекао и велики број дефиниција сајбер криминала.

Бројни аутори су покушали да дају одговор на питање шта је сајбер криминал. На конгресу Уједињених нација предложена је следећа дефиниција сајбер криминала: „Криминал који се односи на било какав облик криминала који се може извршавати посредством рачунарских система и мрежа, у рачунарским системима и мрежама или против рачунарских система и мрежа“ (Gercke, 2012, 11 - 12). Наведена дефиниција нуди свеобухватно одређење сајбер криминала, односно да је то компјутерски (рачунарски криминал) којим се угрожава безбедност компјутерских система и података, а истовремено подразумева све криминалне радње које су спроведене употребом компјутера (рачунарских система), укључујући и илегалну дистрибуцију информација и других садржаја.

Према Извештају Савета Европе о организованом криминалу наведене категорије дела евидентиране су као сајбер криминал: 1) „кривична дела против поверљивости”, интегритета и расположивости, односно доступности података и рачунарских система, 2) „традиционална кривична дела извршена помоћу рачунара“ 3) „кривична дела у вези са садржајем као што су дечја порнографију, расизам и ксенофобија“, 4) „кривична дела везана за кршење ауторских и сродних права“ (Council of Europe, 2005, 40). Кривична дела против поверљивости подразумевају илегални приступ рачунарским системима, хаковање компјутера, прислушкивање, преваре корисника интернета (нпр. шпијунажа, крађа лозинке, пецање), рачунарске шпијунаже (укључујући употребу Тројанског коња и других техника), компјутерска саботажа и изнуђивање (нпр. вируси и црви, напад у виду порицања услуге, спамовање или бомбардовање е - поште). Традиционална кривична дела извршена помоћу рачунара, укључују широк распон класичних превара као што су: манипулације рачунима или билансима компанија, *online* манипулације, аукцијске преваре и *online* преваре поруџбина, незаконита употреба банкомата, злоупотреба кредитних картица, фалсификовање и други облици превара и манипулације. Кривична дела у вези са садржајем као што су на пример: дечја порнографија, расизам и ксенофобија подразумевају тражење, подстицање и пружање упутстава за понашање које је кажњиво и које подстиче различите злочине од убиства до силовања, мучења, саботаже и тероризма. Ова категорија укључује и сајбер

узнемиравања, клевету и ширење лажних информације преко интернета и интернет коцкање. Кривична дела везана за кршење ауторских и сродних права подразумева неовлашћено репродуковање и коришћење рачунарских програма, аудио / видео и других облика дигиталних радова, или података из банки и књига.

Сајбер криминал са становишта правних наука подразумева деликте који су инкриминисани законима. То је специфичан вид криминалитета који је вишеструко повезан са рачунарским мрежама. Оно што неко криминално дело одређује као сајбер криминал је то што је „извршено коришћењем сајбер технологије у сајбер домену" (Tavani, 2003, 103). Фишер предлаже употребу ширег појма „сајбер претње" (Fischer, 2005) да обухвати како инкриминисане радње, тако и оне које још увек нису проглашене кривичним делима у важећим кривичним законицима. Он дефинише сајбер претње као „злонамерну употребу технологија које припадају сајбер простору које се јављају као инструмент претње, али и као циљеви од стране великог броја актера – криминалаца, терориста, организација и држава" (Fischer, 2005, 6).

Ову врсту криминалитета одликује тесна повезаност са технологијом, из које произилази и његова динамичност и шароликост појавних облика. Упркос томе што се сајбер криминалитет јавља у различитим облицима ипак можемо издвојити његових седам основних карактеристика. Прва карактеристика сајбер криминала је да ремети заштиту и безбедност рачунарских података неког одређеног информационог система у целини или једног његовог сегмента. Друга карактеристика сајбер криминала произилази из његовог специфичног карактера и природе противправних делатности. Трећа карактеристика је то што ова врста криминалних делатности подразумева посебна знања учиниоца, специјализована за извршење кривичних дела. Четврта карактеристика је злоупотреба рачунара као средства за противправно остварење циља. Пета карактеристика је намера учиниоца да прибави за себе или неко друго лице корист, или да причини штету неком другом физичком или правном лицу. Шеста карактеристика сајбер криминала је то што физички контакт починиоца са жртвом није нужан. Седма карактеристика се односи на извршиоце сајбер криминала. То су углавном лица којима су информационе технологије физички доступне, која поседују стручно знање и практичне вештине из области рачунарских технологија, углавном су ненасилни и неделиквентни те бирају сајбер форму криминалних активности. Све се одиграва у виртуелном простору, сајбер простору (*cyberspace*) који

је „вештачка творевина која захтева високу техничку опремљеност, добру информациону инфраструктуру која је ничија и свачија својина, у коме паралелно коегзистирају виртуелно и реално и код кога је комуникација колективна“ (Matijašević - Obradović, 2014, 279 - 298). Дакле, специфичност рачунарских (компјутерских) кривичних дела произилази и из саме чињенице да се она врше унутар виртуелног (сајбер) простора, на прикривен начин; под тајним (виртуелним) идентитетом, неретко уз постојање временске разлике између момента када је извршена криминална радња и тренутка када је наступила последица таквог *online* поступања.

Сајбер криминалитет се испољава у различитим облицима (Табела 9) и зависи од следећих елемената: 1) основне мете (циљ) сајбер напада; у зависности од тога да ли је физичко или правно лице, да ли је тежња да се нанесе штета мрежи у целости или једном њеном одређеном делу, да ли је примарни циљ ометање појединих функција, да се изврши упад и др.; 2) оруђа којим се сајбер криминалци служе зарад постизања својих циљева; 3) окружења у којем се реализују сајбер напади; 4) доказа, односно употребљених технолошких средстава и интернета за његово извршење; оно што сврстава учињена криминална дела у сајбер криминал и помаже његово откривање и доказивање, 5) тежина последица и висине начињене штете.

Да је сајбер криминал растући проблем коме треба посветити више пажње у будућности потврђује савремена ситуација. Пандемија COVID - 19 вирусом се негативно одразила на сајбер безбедност. У другом извештају Европске комисије за 2021. годину наведено је о утицају пандемије на сајбер криминал: „Криминалци су брзо искористили промене које је донео рад на даљину и повећана је употреба онлајн услуга... Број сајбер превара и превара повезаних са пандемијом, коришћењем малвера (*malware*), рансомвера (*ransomware*) и *phishing* напада повећао се током пандемије, циљајући појединце, предузећа и нарочито здравствени сектор.“ (European Commission, 2021, 8). У условима пандемије повећан је број лажних веб продавница које рекламирају и продају непостојећу робу, здравствену заштитну опрему, комплете за тестирање, лажне понуде вакцина против COVID - 19 и др.

Табела 9. Облици компјутерског криминала (Бабић, 2009, 67 - 239)

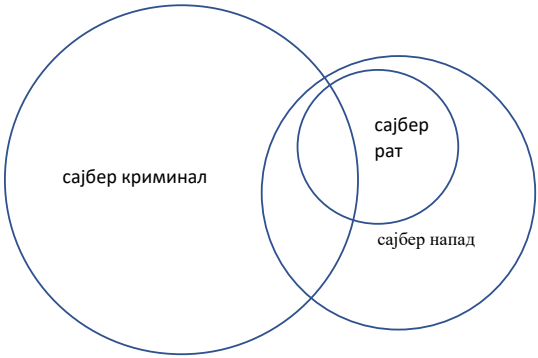
Облици компјутерског криминала	
1. Традиционални	2. Нетрадиционални
1.1. Пренос података	2.1. Хаковање
1.2. Вируси	2.2. Дечја порнографија
1.3. Тројански коњ (*Trojan Horse*)	2.3. Кибер тероризам
1.4. Сецкање (*Salami-Techniques*)	2.4. Кибер рат
1.5. Супердеструкција (*Superzapping*)	2.5. Прислушкивање и компјутерска шпијунажа
1.6. Степенице (*Trap Doors*)	2.6. Неовлашћено коришћење услуга
1.7. Логичке (програмске) бомбе	2.7. Неовлашћено копирање и репродукција компјутерских програма
1.8. Асинхрони напади (*Asynchronous Attacks*)	2.8. Неовлашћено мењање података и/или програма (компјутерска превара кривотворење исправа и оверавање неистинитог садржаја)
1.9. Стрвинарење (*Scavenging*)	2.9. Компјутерска превара
1.10. Цурење података (*Data Leakage*)	2.10. Компјутерски фалсификати
1.11. Крпљење и прерушавање (*Piggybacking & Impersonating*)	2.11. Кривотворење кредитиних картица
1.12. "Ожичавање", прислушкивање (*WireTapping*)	2.12. Компјутерска уцена и изнуда
1.13. Симулација кажњивих дела као њихова припремна фаза	2.13. Неовлашћено уклањање или уништавање података и/или, програмске и технолошке подршке (компјутерска саботажа)
	2.14. Компјутерска крађа
	2.15. Организовани хакерски криминал

Сајбер криминал и сајбер тероризам

Сајбер криминал и сајбер тероризам се разликују на основу примарног циља (мотива) спроведених активности у сајбер простору. Јер, као што примећује Фишер „сајбер криминал се углавном односи на злочине који су почињени употребом информационих технологија, нарочито интернета за остварење личне користи, а сајбер тероризам се односи на злочине који подразумевају употребу информационих технологија у политичке сврхе“ (Fischer, 2005, CRS - 10). Такође једна од упечатљивих разлика између сајбер криминала и сајбер тероризма је та што починиоци сајбер криминала настоје да остану анонимни, неоткривени, док сајбер терористи као и терористи углавном желе публицитет и да изазову страх што већих размера. „Начини на које терористи настоје да остваре жељени ниво публицитета су: 1) планирање акција које треба да имају велики значај у вестима; 2) спровођење активности које треба да оснаже сопствену пропаганду и регрутовање; 3) одабир најпогоднијег времена и локације за привлачење публицитита приликом спровођења акција; 4) издавање прогласа; 5) одржавање контаката са штампом и давање изјава; 6) признавање одговорности за одређене акције; 7) слање порука кроз значење и симболику мете или аката“ (Paletz & Schmid, 1992, 32).

Унутар сајбер простора дешавају се бројне сајбер активности које упркос томе што се изводе сличним операцијама, битно се разликују по својој суштини (Слика 4). Кључна разлика између сајбер вандализма, сајбер криминала и сајбер тероризма је мотив. „Сајбер претње, сајбер инциденти и сајбер вандализам попут оштећења сајтова нису тероризам. Сама забринутост у вези сајбер тероризма потиче од комбинације страха, незнања или од тога што се на глобалном нивоу нису суштински дефинисали, таксативно набројали акти који се могу окарактерисати као такви“ (Јонев & Бериша, 2016, 2). Може се рећи да сајбер вандали готово да и немају неки нарочити мотив, осим што теже осећају задовољства због неовлашћеног упада у неки информациони систем који је тешко пробити, јер је добро обезбеђен. Док су класични сајбер криминалци вођени мотивима личне природе, односно жељом да остваре корист (имовинску или неимовинску) себи или неком другом, или да нанесу штету другом лицу или некој институцији због личних мотива. Док су сајбер терористи вођени политичко - идеолошким мотивима.

Слика 4. Релација између сајбер активности (Hathaway et al., 2012, 833)



Јазић наводи „три врсте мотивација које одређују деловање одређених терористичких група: 1) Рационална мотивација одређује понашање терористе у смеру да пре свега размишљају о својим циљевима и могућностима, анализирајући их кроз призму „цене" коју морају да плате и могућег добитка. 2) Психолошка мотивација за спровођење терористичких аката произилази из личног незадовољства терористе сопственим животом и достигнућима. 3) Културна мотивација унутар терористичких група снажно утиче на јединство и обликовање циљева и вредности унутар терористичких група. Култура обликује вредности и мотивише људе одређене заједнице на начин који делује неразуман за посматраче са стране" (Јазић, 2010, 122 - 123). Иако је највећи број учињених терористичких аката био у знаку верског фанатизма, „основни циљ већине терористичких група је независност и држава" (Јазић, 2010, 115). Није непознато да одређени терористички покрети уживају подршку неке државе због филозофских ставова које заступају, а који тој држави одговарају. Неретко су државе финансирале терористичке операције „ради остварења сопствених спољнополитичких циљева или на унутрашњем плану ради јачања сопствене политике" (Lutz & Brenda, 2004, 14 - 16). Тада говоримо о државном тероризму, односно сајбер рату (Stytz, 2006) када терористи примењују савремене информационе технологије ради постизања виших циљева којима се утиче на спољно - политичко или унутардржавно стање. „Сајбер терористи обично имају намеру да директно или индиректно деморалишу цивилно становништво, што га разликује од сајбер рата који није директно усмерен против цивила" (Brenner, 2007, 388).

Сајбер рат је деловање државних учесника које подразумева примену информационих и комуникационих технологија, било као средства или мете напада, а које је усмерено против сајбер инфраструктуре противника.

6. ФАЗЕ ОДБРАНЕ ОД САЈБЕР ТЕРОРИЗМА

Безбедност и одбрана рачунарских система су питања од приоритетног значаја, обзиром да се савремено друштво умногоме ослања на рад и подршку информационих и комуникационих инфраструктура. Питање сајбер безбедности углавном подразумева заштиту ресурса (материјалних и / или нематеријалних) од евентуалних опасности (Kizza, 2009, 45 - 46; Solange, 2009, 3). Међутим, ово питање се све више односи на очување живота људи и одржавање међународног мира, јер се негативне последице напада који је изведен у сајбер простору лако преносе у реалност и директно утичу како на животе људи, тако и на стање у појединим државама и међународне односе. Размере потенцијалне штете варирају од: краткотрајне обуставе свакодневних активности, причињавања значајне економске штете, колапса (у саобраћају, трговини, на берзи) па све до катастрофа са великим бројем људских жртава. Причињена штета зависи од неколико фактора: нападача, односно његових циљева и мотива, способности и ресурса (знања, алата) којима располаже, постојећег система одбране и мете напада. Обзиром да на карактеристике нападача не можемо да утичемо, оно што има пресудну улогу је снажна и ефикасна одбрана. Међутим, Гудмен је изнео кратку оцену наших укупних способности да се бавимо терористима који користе сајбер простор и закључио: „да смо у већини потенцијалних циљева технолошки и процедурално слаби у сваком погледу све три фазе сајбер одбране од квалификованих, стрпљивих и постојаних нападача које вероватно неће бити лако зауставити“ (Goodman, 2007, 50). Отуда савремене директиве за достизање сајбер безбедности имају широк опсег и покривају „десет основних сектора: транспорт, енергетика, банкарство, инфраструктура финансијског тржишта, здравство, вода за пиће, отпадне воде, дигиталне инфраструктуре, инфраструктуре јавне управе и простора“ (European Commission, 2021, 3).

Имајући у виду да се технологија развија и примењује великом брзином, пред службама сајбер заштите и одбране је тежак задатак да те промене испрате и одрже исти темпо развоја. Када говоримо о одбрани од сајбер тероризма Гудмен се залаже за „три фазе одбране: 1) превенција; 2) управљање инцидентом, ублажавање напада, ограничење штете; 3) управљање последицама“ (Goodman, 2007, 46).

Корисници се међусобно повезују унутар рачунарских система због најразличитијих потреба и мотива. Одбрана од сајбер тероризма није једноставна. Праћење активности у сајбер простору отежава велики број корисника. Питање заштите рачунарских мрежа је такође проблематично, јер заштитне мере и средства тешко

могу да прате динамику развоја иновација нападача. Нападачи се углавном фокусирају на откривање рањивости, односно проналазак „рупа у систему“ и инсајдера, односно саучесника који могу да им помогну у криминалним активностима и омогуће приступ систему. Проблематику сајбер одбране усложњава унутар организацијска мобилност и сарадња са спољним сарадницима, што знатно отежава праћење активности и потенцијалних злоупотреба у овом сегменту. Отежавајућа околност је такође што терористи у сајбер простору делују преко лажног онлајн профила скривајући свој стварни идентитет. Захваљујући томе имају могућност да се инфилтрирају међу остале све до момента извршења напада. Учињена дела сајбер криминала остају великим делом непријављена због незнања, недовољно издвојених средстава за решавање потенцијалних сајбер претњи и проблема, али и због тешкоћа у прибављању валидних доказа. Потребно је радити на развоју нових мера одбране од сајбер тероризма.

Превенција

Превенција је први нарочито важан корак (фаза) одбране од сајбер тероризма. Различите државе, институције и организације нису подједнако дигитализоване. Самим тиме није подједнака ни вероватноћа претње од сајбертерористичког напада, па ни разорност последица од евентуалног дела сајбер тероризма у различитим земљама. Велике компаније су знатно дигитализоване, јер за своје свакодневно пословање користе велике рачунарске мреже, и као такве су чешће мете напада. Јер, што је систем комплекснији, онда је потенцијално рањивији. Многи информационо - технолошки системи дизајнирани су тако да на што бољи начин пруже тражену услугу / производ својим корисницима, док њиховој сајбер заштити није посвећена посебна пажња.

Сајбер тероризам за разлику од осталих облика сајбер криминала има за циљ да причини штету што је могуће већих размера. Сајбер одбрана је проблематична. Готово да је немогуће пратити динамику развоја савремених технолошких иновација и ићи у корак са њима не би ли се пружиле адекватне мере заштите. Зато аутори посебну пажњу придају превенцији и откривању најбоље методе за предвиђање сајбер напада и предлажу кључне податке који у томе могу да послуже: „1) мотивација, омогућава предвиђање највероватнијег циља сајбер напада; 2) могућност за извршење, омогућава детерминисање највероватније врсте сајбер напада; 3) време, предвиђање тачног времена када би се десио сајбер напад“ (Munkhdorj & Yuji, 2017, 110). Дејвис такође сматра да су „превенција и свест кључни елементи у смањењу преваленције девијантних аката, нарочито у борби против компјутерског криминала“ (Davis, 2012, 278). Клајн предлаже „холистичку стратегију превенције“ (Klein, 2018) која укључује сва средства, односно интегрише војни и не - војни приступ. Дакле, свеобухватна стратегија превенције подразумева да се војне и не - војне активности спроводе удружено у циљу превенције сајбер тероризма „одвраћањем и одговарањем“ потенцијалног противника да изврши дело сајбер тероризма (Klein, 2018, 29).

„Одвраћање (*Deterrence*)“ – „Упркос ограничењима да се утиче на доношење одлука потенцијалних нападача и њихових лидера, одвраћање остаје одржив концепт за превенцију сајбер тероризма“ (Klein, 2018, 30). Све док се принципи војне нужности и законска регулатива пажљиво разматрају, и војни и не - војни одговори су одрживе опције. На успешност стратегије одвраћања

умногоме утиче перцепција потенцијалног непријатеља. Одвраћање је јаче уколико постоји веродостојна претња силе и неприхватљиве последице по нападаче које им следују након било какве врсте сајбер напада. Дакле, предуслов добре превенције је одржавање сталних и агресивних операција против дела сајбер тероризма. На пример, уколико Исламска држава или руководство Ал - Каиде чврсто сматрају да ће, након чина тероризма бити изложени систематичним војним или не - војним интервенцијама које прете да угрозе њихов опстанак и базу моћи, таква перцепција их одвраћа од сајбер напада који су претња по живот.

У својој основи, стратегија одвраћања од сајбер тероризма је утицај на непријатеља и уверавање непријатеља да штетност последица након извршења сајбер напада надвладава потенцијалне користи. Током времена употребљавају се различите врсте одвраћања. Иако постоје бројне подврсте, издвајају се две главне стратегије одвраћања: „одвраћање казном и одвраћање одбијањем“ (Iasiello, 2018, 36).

„Одвраћање казном“ подразумева уверавање нападача о значају казне и одмазде за учињен напад. Овакав сценарио одмазду не ограничава на специфичне акције, односно подразумева укључивање и других средстава као што су кинетичке и економске санкције. Као добар пример може да послужи доктрина Хладног рата у којој је претња употребе нуклеарног оружја спречила намеру противника да употреби слично оружје. Овај принцип, одвраћање казном можемо да применимо у сајбер простору, где одмазда има облик дигиталних поступака као што су сајбер напад који је усмерен против потенцијалних починиоца сајбер тероризма, или предузетнички удар који изазива колапс и онеспособљава функционисање непријатељске мреже. Верује се да су САД стајале иза напада *Stuksnet* вирусом који је био усмерен на иранске нуклеарне програме који су се бавили истраживањем уранијума. Вирус је изазвао значајан застој у раду и развоју. Наведени догађај је добар пример „стратегије одвраћања казном“ у поменутом случају САД против Ирана.

„Одвраћање одбијањем“ је мање конфликтна стратегија која се заснива на покушајима да се потенцијални нападачи убеде да ће упркос уложеним напорима остати ускраћени за користи које очекују од напада. Ова стратегија представља традиционално дефанзивну форму, која када се примењује у сајбер простору подразумева обесхрабривање или фрустрирање непријатеља употребом робусне, проактивне и скупе одбране, тако да однос уложеног и добити за нападача имају негативну рачуницу. Примена ове стратегије захтева

снажну фокусираност и посвећеност владе, велика материјална улагања и сарадњу са приватним сектором како би се осигурали системи и мреже и ставили под њену контролу. Коришћење напредних безбедносних пракси и усвајање поузданих компоненти хардвера и софтвера изискују велика улагања и континуирано праћење технолошког развоја. Успешност стратегије одвраћања од сајбер тероризма зависи од неколико фактора: „комуникација, сигнализација, приписивање и пропорционалност“ (Iasiello, 2018, 37 - 41). Уколико неки од поменутих фактора није испуњен постоји ризик да непријатељство ескалира државним сукобом због неспоразума или погрешног тумачења.

Ефикасна комуникација са међународном заједницом, а нарочито противницима је један од предуслова и питање кредибилитета једне државе нације, која мора да познаје границе, односно „црвене линије“ које се не прелазе, као и у којим случајевима их је потребно прећи. Дакле, ефективна комуникација захтева постојање консензуса о оперативним нормама понашања у сајбер простору за шта је потребно уложити велики напор. Сједињене Америчке Државе и Кина нису успеле да пронађу заједнички језик у стратешком и економском дијалогу у јулу 2013. године. САД због фокуса на технологије и мреже аутоматизованих машина преферирају коришћење термина *cybersecurity* – сајбер безбедност, док земље попут Кине и Русије преферирају коришћење ширег појма *information security* - информациона безбедност (Farnsworth, 2011). Кина и Русија се залажу за ширу интерпретацију која укључује и технологије и информације које постоје и размењују се на мрежи, како би повећали контролу садржаја и информација којима њихово грађанство има приступ, док САД подржавају политику слободе интернета. Без заједничког језика, две стране остају у неслагању и не успевају да постигну консензус о томе како би интернет требало користити на одговарајући најбезбеднији начин. Слабости у комуницирању отежавају слање јасних порука у сајбер простору што може да повећа тензије.

Сигнализација се примењује дуже време у области међународне политике, преговорима у рату, кризи, као и међународним економским преговорима (Walsh, 2007, 441). Без обзира када се примењује, у миру или рату, кључни елемент било које стратегије сајбер одвраћања укључује способност да се намере правилно прикажу и одашиљу до жељеног пријемника. Без могућности сигнализирања повећава се ризик погрешног схватања или тумачења, што стратегију „одвраћања казном“ може да учини неефикасном. На пример, пре извршења

стратегије „одвраћање казном“, држава која се брани мора јасно да сигнализира своје незадовољство агресору тако да га он правилно тумачи и разуме тако да потенцијални трошкови за предузимање одређеног сајбер напада далеко превазилазе потенцијале предности. Даље, да би сигнализација била ефикасна, држава мора да има успостављено радно тело које веродостојно спроводи успешну и деструктивну сајбер одмазду. Уколико противник не верује у кредибилитет државе, сигнализација не може да буде успешна. Као и комуникација, сигнализација у сајбер простору може лако да се погрешно интерпретира, игнорише или чак не примети од стране агресора. Сигнализација може да се спроводи отворено, прикривено или путем дипломатских, економских или војних канала.

Приписивање одговорности у сајбер простору је изузетно тешко јер сајбер простор пружа могућности својим корисницима да прикривено делују. „Спектар одговорности државе - *spectrum of state responsibility*“ (Healey, 2012) је специјално дизајнирана алатка која служи да помогне аналитичарима да припишу одговорност за одређени сајбер напад са прецизношћу и транспарентношћу на основу десет категорија, где је свака од њих обележена различитим степеном одговорности. Да би се идентификовали агресори у сајбер простору, техничка анализа није довољна с обзиром на чињеницу да многи непријатељски актери спроводе исту тактику, технике и процедуре, користе исте алате, или се баве сличним операцијама за спровођење злонамерних активности. Дакле, „иако су технички подаци корисни за одређивање нивоа вештина и ТТП - а (технолошке тактике, технике и процедуре) сајбер нападача, они су делимично делотворни за приписивање, јер не узимају у обзир понашање, особине, намере, мотивације или жеље актера, нити пружају предвиђање будућих напада и циљева“ (Iasiello, 2012, 5). Постоје ограничења поменуте технике приписивања дела сајбер тероризма починиоцима: „приписивање са закашњењем, неуспело приписивање и одсуство приписивања“ (Iasiello, 2012, 5 - 6). „Приписивање са закашњењем - Техничка анализа захтева време. Потребно је да се утврди да ли је инцидент стварно злонамеран, затим да се идентификује рачунар са којег је проистекла малициозна активност (познато је да починиоци користе ботнете - мрежу компромитованих рачунара које контролише починиоц). Поменута процедура траје, одлаже се на неко време како би се прикупили сви подаци, што оставља простора нападачу да може да побегне, односно нестане пре него што му се припише злочин. Неуспело приписивање може уследити због ограничених способности техничке опреме, људске

грешке или стручности починиоца, техничка анализа није увек у могућности да обезбеди успешну идентификацију починиоца. Одсуство приписивања се може догодити због бројних разлога који даље могу да доведу до погрешне идентификације локације или идентитета починиоца: неисправан софтвер, неисправни подаци, нејасни или погрешно тумачени подаци“ (Iasiello, 2012, 5 - 6).

Пропорционалност у сајбер простору подразумева да причињена штета сајбертерористичким нападом треба да буде сразмерна казни. Практично је то тешко постићи због различитих разлога. Када национална држава делује независно од једне моћне међународне организације као што су Уједињене нације, ризикује да угрози дипломатске, чак и економске односе. Због тога је потребно да пре доношења одлуке о одмазди (сајбер или не - сајбер одмазди), држава добро процени последице и потенцијалну штету и размотри понашање међународне заједнице.

„Одговарање (*Dissuasion*)“ је поред одвраћања значајан део холистичке стратегије превенције. То је „настојање да се утиче на руководство потенцијалних непријатеља тако што се обесхрабрују иницијативе војних надметања“ (Klein, 2018, 30). Поступак одговарања је делотворан пре него што се претња манифестује. Јер, одговарање укључује „активности обликовања“, које су типично не - војне по свом обиму и спроводе се у миру, односно једино изван потенцијалне опасности од војне акције. Стратегија која укључује одвраћање усмерена је на приказивање сајбер напада као бескорисног.

Бослер и Холт су спровели истраживање да представе перцепцију полиције о њиховој тренутној способности да одговоре на дела сајбер криминала и изнели су следеће предлоге за побољшање друштвеног одговора на сајбер криминал: 1) „корисници интернета треба да буду пажљивији када користе интернет, 2) теже казне за сајбер криминалце, 3) тежа кривична гоњења за сајбер криминалце, 4) јасније законодавство против сајбер криминала би повећало успешност гоњења и истраге, 5) специјални форензички алати и технологије, 6) повећање средстава за обуку агенција које су у служби закона, 7) стварање боље сарадње између државе и савезника по питању сајбер криминала, 8) рад са провајдерима (нпр. *AOL*) како би се надгледао интернет, 9) боља едукација јавности у вези са сајбер криминалом, 10) сарадња са пословном заједницом ради побољшања извештавања и истраживања криминала, 11) наменски структуриране локалне јединице за сајбер криминал, 12) боље методе за откривање сајбер криминала, 13) више рачунарских

обука за службенике, 14) повећање менаџмента како би се развило праћење на регионалном нивоу, 15) рад са грађанима“ (Bossler & Holt, 2012, 175).

Поменути предлози применљиви су и када је у питању превенција сајбер тероризма. Дакле, потребно је да се јавни и приватни сектор заједно ангажују и сарађују на остваривању сајбер безбедности, удружено применом различитих метода одбране. Односно, потребно је да се компаније из приватног сектора које тесно сарађују са државним виталним структурама, као што су приватне безбедносне агенције, фондације за остваривање грађанских права и др. значајније укључе и информишу о претњама од сајбер тероризма, као и о другим врстама сајбер криминала. Као пример добре праксе може да послужи Холандија. На пример, организација *Nederland ICT* окупља нешто више од 550 информационо - комуникационо технолошких компанија, међу којима су неке од водећих у Холандији (*Microsoft*, *Google Holandija*, *UPC*, *CGI Holandija*, *KPN IT Solutions*). Поменута организација поседује своју саветодавну групу експерата која се бави проблемима и развојем сајбер сигурности.

Добра превенција подразумева: 1) усаглашавање прописа и кажњавања дела сајбер тероризма на међународном нивоу, 2) развој истраживачких јединица за сајбер криминал на локалном нивоу, 3) добра координација приватног и јавног сектора, 4) примена одређених стандарда, поступака и процедура ради боље безбедности система, 5) предузимање одређених мера заштите (редизајнирање постојећих система, физичко или сајбер пресретање напада, прислушкивање, постављање сензора и др.), 6) примена различитих техника (*firewalls* и *password)* као филтера за кориснике којима је дозвољен приступ, тајни или јавни кључ за шифровање, различити системи за откривање упада и др.), 7) планирање (финансијско, истраживачки пројекти за изналажење нових технологија одбране и заштите), 8) подизање свести о евентуалној претњи од сајбер тероризма, 9) савесна употреба и имплементација савремених ИКТ, 10) едукација.

Управљање инцидентом

Рачунарски системи функционишу аутоматизовано, тако што га правилно задата функција покреће или збуњује - наноси штету или уноси у њега неисправан код за „лоше“ функционисање. Да би информационо - комуникационе структуре функционисале неопходно је постојање два кључна елемента: физички – опрема (машина) и људски елемент – који спроводи неколико технолошких поступака и задатих наредби које се исписују програмским језиком уз употребу одговарајућих програмерских алата.

Како би се опасност по рачунарске системе свела на минимум најпре је неопходно створити заштиту, односно неку врсту баријере, помоћу које ће се ограничити или онемогућити приступ „спољним“ неауторизованим корисницима да манипулишу подацима и изводе малверзације. То се најчешће постиже постављањем одређеног система лозинки (*password*) или *firewall* којима се ограничава приступ на ауторизоване кориснике. Такође, од велике важности је постављање сензора који служе да правовремено детектују напад и упозоре да је напад отпочео. Неки аутори (Janczewski & Colarik, 2008, 274 - 276) сматрају да је због велике количине података немогуће контролисати целокупан проток информација, па је зато веома важно поставити системе за надгледање на одговарајуће место. Ови системи помоћу којих се надгледа интернет саобраћај могу да обављају различите функције (прикупљање података, снимање, њихово филтрирање и алармирање у случају напада).

Сајбер напад се најчешће открива методама који прате сигнале и детектују аномалије. Док се одбрана, односно одређени систем противмера у оваквим случајевима примењује против предстојећег сајбер напада једино у случају његовог детектовања. Технике откривања сајбер напада и контрамере се усавршавају у складу са до сада познатим, односно откривеним методама за извођење сајбер напада. Постојећи системи због својих ограничења, нису више у могућности да открију све сајбер нападе са високим степеном прецизности и тачности. Зато у већини случајева администратори система ни не примете да су били изложени нападу или покушају напада. Дакле, сајбер напад постаје откривен, тек када је причињена значајна штета која не може да прође неопажено. Управо због тога системи одбране нису довољно припремљени на предстојеће нападе од стране сајбер терориста.

Нападачи најчешће користе *feed* - ове, врсту јавних домена који подразумевају више техничких аспеката за разлику од уобичајених

друштвених података. То је одређени след садржаја који се често ажурира на рачунару или мобилном телефону кроз који можемо да се „крећемо“. Садржај се приказује у сличним блоковима који следе један другог. Као пример може да послужи изглед мреже на рачунару који се претвара у *feed* (Слика 5) или изглед прегледавања на мобилном уређају.

Слика 5. Пример *feeda* који садржи текст и слике (Блиц, 6.6.2022)

Бројни аутори предлажу употребу *fedd* - ова за предвиђање могућих сајбер напада или одређене врсте напада (Holm, Ekstedt & Andersson, 2012, 825 - 837; Bollen, Mao & Zeng, 2011, 1 - 8). *Twitter feed* - ови могу да буду добар извор за прикупљање информација о сајбер нападима. Болен и сарадници претпостављају да се неке промене које су усмерене против жртве напада у сајбер простору дешавају непосредно пре извршења самог напада. Отуда предлажу следеће поступке за његово предвиђање: „1. Прикупљање архиве сајбер инцидената који су се догодили у прошлости коришћењем *feed* - ова, 2. Прикупити изворе рањивости који су експлоатисани у инцидентима. Сакупљање друштвених извора (чланци, вести, твит - ови) који се односе на сваку жртву у архиви, 3. Детектовати обрасце који се понављају посматрано из углова угрожености. Откривање неког образца упоређивањем друштвених извора са

жртвом, који су објављени непосредно пре напада помоћу *feed* - а и оних који су објављени у другим периодима, 4. Обучити модел за учење машина на узорку откривеном у претходном кораку, 5. Унос дневних друштвених садржаја у обучени модел и провера да ли се шаблон појављује у дневним изворима. Откривени узорак у петом кораку ће бити резултат предвиђања“ (Bollen, Mao & Zeng, 2011, 119). За предвиђање сајбер напада може да послужи и потенцијална мотивација за његово извршење (Munkhdorj & Yuji, 2017). Ради постизања сигурности, администратори мреже треба да аутоматизују анализу дневника како би препознали нападе који су у току, или трендове који указују на покушаје упада. На пример, низ неуспелих покушаја пријављивања може да укаже на то да неко покушава да погоди лозинку и добије неовлашћени приступ мрежи. Администратори мреже су задужени за њену безбедност, те је већина њих добро упозната са ризицима. Администратори предузимају разне мере како би спречили нападе на њихове мреже и рачунаре. Гудмен (Goodman, 2007, 49) сматра да организације треба да креирају сопствене сигурносне политике и планове одбране који покривају широк спектар одбране од могућих сајбер напада који представљају потенцијални ризик за одређени тип организације. Такође сматра да су веома корисне практичне вежбе, али их организације углавном избегавају зато што су скупе и узнемиравајуће, јер су многи информациони системи деликатни, па се њихови власници плаше да ће нешто поћи наопако.

Санирање последица

Суочавање са сајбертерористичким нападом не значи само поменуте мере заштите и његово откривање, него и управљање последицама напада, тако да се оне: што је могуће више ублаже и ограниче, причињена штета сведе на минимум, заштите ресурси и информације, поврати што већи број података (*backup*, *recovery* функције) и прикупи што је могуће више информација о извршеном нападу (ревизорске функције) како би се открили починиоци и предупредили напади те врсте у будућности. Након сајбертерористичког напада у овој фази одбране постоје две примарне процедуре одбране. То су: „опоравак (*recovery*) и одговор (*response*)" (Goodman, 2007, 50). Следеће поступке убрајамо у опоравак: „уклањање или затварање непријатељских ентитета; процена штете, шта је сломљено или измењено, а шта није; аутоматски процеси за процену и брзу и ефикасну рационализацију онога што је остало; утврђивање приоритетних функција које треба да се реконструишу; враћање на стање пре напада без уништења доказа" (Goodman, 2007, 50).

Добро планирани и пажљиво извршени напади, као што су на пример корумпирање података или злонамерни код представљају највећи изазов за опоравак. Јер, организација може дужи временски период да буде изложена замаскираном, нетранспарентном нападу, што знатно отежава *back up* и проналажење одговарајуће резервне копије података, и откривање свих штетних трансакција. Опоравак се односи на пасивни облик одбране, јер подразумева реконституцију оштећеног ИТ система нападом, како би се организација што пре је могуће оспособила за уобичајено функционисање. Одговор (*response*), пак, подразумева активни облик одбране јер се односи на идентификацију и кажњавање починиоца сајбертерористичког напада, и потпуније информисање о опасностима на основу пређашњег искуства зарад ефикасније одбране и заштите од поменуте врсте напада у будућности. Одговор (*response*) подразумева следеће поступке: „проналажење правог кривца: снажни прецизни трагови и форензички алати, нека врста "отиска прста"; измерена одмазда: правни принципи и пропорционалне одмазде; асиметрије: шта учинити са нападачима са мало ИТ средстава или рањивости?; ескалација: процена штете како би одлучили да ли желимо да пошаљемо јаку поруку" (Goodman, 2007, 50).

7. МЕРЕ ОДБРАНЕ ОД САЈБЕР ТЕРОРИЗМА

Сајбер тероризам треба истраживати као и било који други случај који укључује дигиталне доказе. Да би прикупљени дигитални доказни материјали били прихватљиви на суду морају да задовољавају одређене форензичке стандарде и протоколе, који се примењују за идентификацију, прибављање, располагање и испитивање електронских доказа како на националном, тако и на међународном нивоу. Ово је нарочито важно, јер истраживање и решавање случајева сајбер тероризма подразумева поред ангажовања државних (националних) судова и укључивање трибунала и међународних судова и институција.

Сајбер терористи се служе различитим техникама како би замаскирали свој идентитет и остали анонимни. Помоћу прокси сервера сакривају *IP* адресе. Такође сакривају кораке којим је напад изведен и служе се фалсификованим *IP* адресама. Поменуте радње им обезбеђују значајније нивое анонимности, који отежавају улазак у траг починиоцима сајбер тероризма. Ниво вештина починиоца се не може лако проценити, јер починиоци углавном бирају датотеке на основу њихове рањивости и оне које не захтевају употребу сложених хакерских вештина и алата за њихову експлоатацију. Техничка анализа има своја ограничења и не може да продре дубље тако да пружи одговоре на питања: зашто је нападач одабрао специфични рачунар; који је ниво ризика претпоставио пре извршења напада и др. Односно: „тренутно успостављена аналитичка методологија: процес аналитичке хијерархије (*AHP*), анализа конкурентних хипотеза и *Delphi* технике, није адекватна за адресирање суптилних нијанси сајбер проблема“ (Iasiello, 2012, 4).

Шта процес аналитичке хијерархије (*AHP*) подразумева? *AHP* је структуирана техника која се примењује за доношење сложених одлука (Iasiello, 2012). Методологија је сувише статична и захтева варирање алтернатива у фиксну, пондерисану хијерархију. Сајбер сценарији су више динамичнији и не могу лако да се уклопе у систем рангирања. Процес аналитичке хијерархије се фокусира на „ефекте“ сајбер активности анализирајући хипотезе о томе шта је тачно или шта је вероватно да ће се догодити, а не фокусира се на мотиве за извођење сајбер активности.

„Анализа конкурентних хипотеза (*ACH*)“ (Iasiello, 2012) се заснива на идентификацији и анализи алтернативних хипотеза, а не само на један „највероватнији“ закључак. Међутим, као и процес аналитичке хијерархије, анализа конкурентних хипотеза није у стању да узме у обзир динамичну природу сајбер простора и свих дешавања у њему, те отуда он остаје сива површина. Јер, основна

структура анализе конкурентних хипотеза не узима у обзир шта се крије „иза“ доказа о извршеном сајбер нападу, него служи само за проналажење доказа. Такође, ова анализа укључује превелик број хипотеза, па је скоро немогуће одредити број сајбер актера који су заслужни за сваки покушај или успешно спроведен упад у мрежу.

„Delphi техника (*DT*)“ (Iasiello, 2012) је фокусирана прогноза која може да помогне предиктивним анализама; није одрживи алат истраживања, већ служи као подршка студијама са боље успостављеним и поузданијим методама. Крајње гледано, аналитичари су приморани да је примењују у својим анализама приликом употребе методе „инстинкта“ за изношење претпоставки на основу обимних доказа (Iasiello, 2012, 4 - 5).

Како би сајбер одбрана била што успешнија Бериша и Баришић сматрају да је потребно да се формира „један централни ауторитет који би координирао одговором на националном нивоу. У начелу национални тим за одговор на инцидент чини група експерата за информациону безбедност који проучавају рањивости рачунарских система“ (Бериша & Баришић, 2016, 7), односно тзв. „тим за одговор на инцидент (*Computer Incident Response Team – CIRT, Computer Emergency Response Team – CERT*)“ (Бериша & Баришић, 2016, 7).

У одбрани од сајбер тероризма неминовна је употреба компјутера, међутим потребно је покренути дубље механизме одбране као што су: системски приступ проблему, едукација, креирање политике која широко покрива проблем сајбер тероризма, интеграција међународних и националних мера одбране и стандарда, потребно је да се већа пажња посвећује „порукама“ које се онлајн емитују и др. Дакле, потребно је да одбрана од сајбер тероризма буде што је могуће свеобухватнија и слојевита. Јер, „активна сајбер одбрана подразумева проактивне мере за сузбијање непосредних ефеката сајбер инцидента, док је пасивна одбрана усмерена на производњу сајбер средстава који пружају ефикасан отпор сајбер нападима“ (Farwell & Rohozinski, 2012, 109).

Активна одбрана од сајбер тероризма

Активна сајбер одбрана подразумева укључивање људског елемента у сам процес, односно аналитичаре који обављају низ активности с основним циљем да пруже одбрану од сајбер напада. Розенцвајг је дефинише као „синхронизовану правовремену способост да се открију, анализирају и смање претње. Активна сајбер одбрана ради на брзини мреже, користећи сензоре, софтвер и интелигенцију да открије и заустави штетне активности пре него што допру до мрежа и система“ (Rosenzweig у: Dewar, 2014, 9). У циљу спровођења активне сајбер одбране аналитичари спроводе различите активности као што су: надгледају и примењују знања унутар мреже, проналазе адекватне одговоре, усавршавају се како би се што је могуће ефикасније изборили са претњама од сајбер тероризма, прате дневнике активности који аутоматизовано прикупљају информације које им помажу да детектују нападе или покушаје упада у систем. Поменути аналитичари сајбер безбедности најчешће су специјализовани за одређену област или домен (тестирање, праћење инцидента и реаговање, анализа малвера, управљање ризиком и прикупљеним информацијама о опасностима и др). Генерално посматрано активна сајбер одбрана укључује: „1) експлоатацију; 2) контранапад; 3) предухитрујући напад (*preemptive attack*); 4) превентивни напад (*preventive attack*)“ (Wong, 2011, 19).

Први поступак активне сајбер одбране подразумева експлоатацију рачунарских система који су мете сајбер напада. Пасивне мере одбране могу током сајбер напада или након његовог извршења да открију *IP* адресе директно са којих је покренут напад. Међутим, нападачи све више усавршавају технике напада. Савремени напади су све софистицираније и настају као коначни резултат ланчаних реакција које су производ умрежених хакованих компјутера, што значајно отежава могућности да се утврди право порекло напада и уђе у траг првобитном извору напада. Зато неки аутори предлажу *IP traceback* (Belenky & Ansari, 2003, 162). Међутим, ова техника још увек није заживела због: неекономичности јер треба да се имплементира на што је могуће више *ISP* - а да би резултати били што прецизнији и тачнији. Такође има проблема са компатибилношћу и перформансама. Ревизијом сајбер напада се целокупан поступак којим је извршен напад враћа уназад све док се не открије последња *IP* адреса рачунара са којег је напад проистекао. Потом форензичари идентификују власника рачунара, тако што „истражују документе сачуване на рачунару, вебисторију,

кеш датотеке, е - пошту итд.“ (Keith, Bejtlich & Rose, 2008, 205 - 300). Дакле, експлоатација подразумева детаљну анализу сајбер напада.

Контранапад је врста активне сајбер одбране која подразумева супротстављање нападачу еквивалентним сајбер нападом. То не само да одбија тренутни напад, него спречава нападача да покрене даље нападе. На пример, у јануару 2000. године на самиту Светске трговинске организације (СТО) сервер је био мета *DoS* напада од стране активистичке групе *E – hippies* чије је седиште у Великој Британији. Међутим, компанија *Conkion Inc.* је била у стању да прати *IP* адресе са којих је проистекао напад на СТО сервер и уместо да га филтрира, долазни напад је преусмерио назад на сервер нападача и онемогућио га на неколико сати.

Предухитрујући напад као и контранапад спадају у „*hack – back* активности“ (Boebert, 2010, 48 - 49). Предухитрујући напад је „предузимање силе против напада за који се верује да је неизбежан на основу доказа да је непријатељска акција почела или ће ускоро почети“ (Wong, 2011, 25). Дакле, ова врста активне одбране подразумева реакцију на основу претпостављеног сценарија, односно „спровођење напада на мрежу или систем у очекивању да ће тај систем извршити напад на ваш“ (Wong, 2011, 25). Предухитрујући напад има за циљ да ослаби и онеспособи непријатеља тако да он не може да спроведе планирану офанзиву. „Свест потенцијалних нападача о таквом „сајбер патролирању“ само по себи делује као одвраћање“ (Boebert, 2010, 49) од њихове намере, јер су изложени додатним сигурносним изазовима, па самим тиме и неизвесношћу у погледу степена до ког су они сами угрожени. Превентивни напад је сличан претходно поменутом предухитрујућем нападу. Разликују се, по томе што превентивни напад подразумева „употребу силе против очекиваног напада која је заснована на процени постојећих или потенцијалних средстава које ће нападач користити за напад у будућности или да изазове друге врсте штете“ (Sofaer, 2010, 9).

Претходно наведени поступци активне сајбер одбране засновани су на познатој и валидној технологији коју користе и сами нападачи, те не постоје значајније техничке препреке за њихову примену. Евентуалне препреке које се могу јавити су законске и политичке природе. Тако је правно питање власништва над нападнутом / оштећеном машином дискутабилно. Може се тврдити да право над машином која постоји на интернету наслеђује власник физичког хардвера. Међутим, сајбер терористи могу да користе украдену машину за извршење злочина.

Ограничења поменутих мера активне сајбер одбране су

врло контроверзна, јер се њиховим спровођењем могу прекршити одређени међународни закони. Отуда Денинг наводи „етичке и легалне принципе спровођења активне сајбер одбране: 1. власт; 2. имунитет треће стране; 3. нужност; 4. пропорционалност; 5. људско учешће; 6. грађанске слободе“ (Denning, 2014, 111). Први принцип „власт“ подразумева да активну сајбер одбрану могу да спроводе само органи који су за то овлашћени, односно прихваћени од стране власти да раде у складу са законом. Други принцип, „имунитет треће стране“ подразумева заштиту трећег лица. Односно, активна сајбер одбрана не сме да угрози оне који су жртве сајбер напада. Трећи принцип „нужност“ значи да се мере активне сајбер одбране спроводе једино када је то неопходно, у случајевима нужности. Четврти принцип „пропорционалност“ значи да активну сајбер одбрану не треба спроводити уколико причињена штета и остварена корист нису пропорционалне. Било која врста активне сајбер одбране, чак и аутоматизовани облици у одређеној фази захтевају повремено ангажовање људи. Пети принцип „људско учешће“, подразумева ограничавање људског фактора, јер није пожељно, ни практично укључити људе у све фазе активне сајбер одбране. Шести принцип „грађанске слободе“ је усмерен на поштовање грађанских права корисника мрежа, оних који су мете или жртве напада, али и осумњичених (Denning, 2014, 111 - 112).

Иначе, „активну сајбер одбрану чине четири карактеристике: обим ефекта, степен сарадње, врсте ефеката, степен аутоматизације“ (Denning, 2014, 109). Прва карактеристика, обим ефекта разликује интерну и екстерну одбрану. Интерна одбрана је она чији су ефекти ограничени на мрежу која је предмет одбране. Док, екстерна одбрана подразумева ефекте који превазилазе мрежу. Друга карактеристика, степен сарадње, прави разлику између активне сајбер одбране која се одвија у складу са одобрењем и сагласношћу за спровођење појединих мера активне одбране и оних које то нису. Даље, на основу врсте ефеката разликујемо четири типа активне сајбер одбране у зависности од: 1. дељења, подразумева активности којима се дистрибуирају информације о нападу (*IP* адресе са којих је напад извршен и др.), 2. прикупљања, подразумева активности које су усмерене за прибављање што већег броја информација о претњи и њеним ефектима, 3. блокирања ефеката непријатељских активности, 4. превентивних ефеката којима се онемогућавају извори који се користе за напад. Степен аутоматизације је последња четврта карактеристика активне сајбер одбране која се односи на то у којој мери је неопходно укључивање људског фактора, односно који је

степен људског ангажовања.

Роберт Ли помиње циклус активне сајбер одбране (Слика 6), који се састоји из четири фазе: „1. претња, 2. идентификација промена и надгледање безбедности мреже, 3. реаговање на инцидент, 4. претња и руковање окружењем“ (Lee, 2015).

Слика 6. Циклус активне сајбер одбране (Mandt & Lee, 2016, слајд 13)

Прва фаза циклуса активне сајбер одбране је „претња“ која служи за идентификовање реалних опасности којима је изложена организација. То подразумева прикупљање обавештајних информација о мисији и окружењу организације. Компанија или организација може да прикупља информације о одређеном сајбер инциденту „локално и удаљено“ (Lachow, 2013, 5 - 6). Локално прикупљање информација подразумева употребу разних техника активне сајбер одбране унутар својих граница. Док, удаљено прикупљање информација подразумева да одређена компанија или организација сарађује са другим организацијама и има приступ њиховом серверу што јој омогућава да прикупља информације ван својих граница.

Друга фаза циклуса посвећена је идентификовању промена како бисмо увидели озбиљност претње и покренули адекватан одговор. Трећа фаза, подразумева адекватно „реаговање на инцидент“ (Mandt & Lee, 2016) у зависности од обима претње, као и праћење

примењене процедуре реаговања како би се искоренила опасност. Четврта последња фаза активне сајбер одбране подразумева измене на мрежи, односно њено усавршавање тако да буде отпорна и сигурнија на дотадашње претње којима је била изложена. Активна одбрана омогућава организацији да адекватно и брзо реагује на безбедносне ризике и минимизира штетне последице и губитке.

Пасивне мере одбране од сајбер тероризма

Сви корисници интернета, било да је у питању појединац или организација, требало би да примењују пасивне мере одбране (сет одбрамбених система), јер оне пружају константну заштиту или увид у претње од сајбер тероризма помоћу алатки уз минималне потребе за сталним надзором и интервенцијом људи. Начешће су то системи који захтевају периодично одржавање и крпљење (*patching*) као што су: заштитни зидови и различити системи заштите који служе за откривање (*IDS*) или спречавање упада (*IPS*), спречавање пропуштања података (*DLP*), антивирусни софтвер, *malvare* системи, филтери за *spam* и др.

Шта подразумева пасивна сајбер одбрана? „Пасивна сајбер одбрана обухвата криптографију и стеганографију (аналогно употреби камуфлаже и прикривања авиона), сигурносни инжењеринг и верификацију, конфигурацију надзора и управљања, процену рањивости и ублажавање, процену ризика, резервно копирање и опоравак (*back up*) изгубљених података, едукацију и обуку корисника“ (Denning, 2014, 109). Дакле, укључује: „*firewalls*, сајбер „хигијену“ која тренира и едукује радну снагу како би се заштитили од грешака или прекршаја који могу да доведу до сајбер упада, сензорну технологију која служи за детекцију „*honey pots“,* или мамце који служе за диверзију и управљање ризиком сајбер простора кроз колективну одбрану, паметно партнерство, информатичку обуку, већу свесност о ситуацији и успостављање сигурних, отпорних мрежних окружења“ (Farwell & Rohozinski, 2012, 109). Из претходног можемо закључити да пасивна сајбер одбрана подразумева сплет комплексних механизама одбране. Међутим, бројни механизми које пасивна одбрана укључује су суштински пасивни, али постају активни онда када у себе укључују елементе за онеспособљавање откривених претњи. Пасивну сајбер одбрану већ неко време примењују организације које воде рачуна о безбедности свог пословања.

Нове стратегије одбране од сајбер тероризма

Сајбер напади су временом постајали све озбиљнији и сложенији, а последице све теже, зато је ослањање на актуелне системе одбране постало недовољно за континуирано праћење и анализу система и података. Да би одбрана од сајбер тероризма била ефикасна потребно је константно усавршавање постојећих и потрага за новим стратегијама и идејама. У потрази за новим идејама, Ајасиело је испитао могућности примене досадашњих модела државне одбране на сајбер домен. Испитао је: „стратегију за нуклеарно одвраћање (*Nuclear Deterrence*), стратегију одвраћања од тероризма (*Terrorism Deterrence*), стратегију одвраћања од претњи непријатељских држава (*Rogue States*)“ (Iasiello, 2018, 41 - 45).

„Нуклеарно одвраћање (*Nuclear Deterrence*)“ - У својој основи ова стратегија има за циљ да спречи употребу нуклеарног оружја, те се примењује једино на државе које располажу нуклеарним наоружањем. Почетком седамдесетих година, за време хладног рата између САД и Совјетског Савеза ова стратегија се показала као врло успешна. Стратегија нуклеарно одвраћање се заснива на теорији „*mutually assured destruction*“ (Payne & Walton, 2002, 169), односно сигурном узајамном уништењу земаља које се усуде да покрену употребу нуклеарног оружја. Отуда ниједна од поменутих земаља упркос бројним несугласицама и заоштреним односима, није одлучила да користи нуклеарно оружје и ризикује почетак нуклеарног рата који би имао разорне последице глобалних размера. Милвенон и Ретреј примећују сличности које постоје између сајбер и нуклеарног сукоба: „1. Оба делују на сва три нивоа војних операција: стратешки, оперативно и тактички, и њихови ефекти имају потенцијал у распону од малих до популационих размера. 2. оба имају капацитет да створе велике, чак и егзистенцијално, деструктивне ефекте. 3. оба се могу спроводити између националних држава, између нације - државе и недржавних актера, или између хибрида који укључују националне државе и не - државне заступнике. 4. нуклеарни и сајбер конфликт може да представља одлучујући пораз непријатеља, тиме што он негира потребу за конвенционалним ратовањем. 5. оба могу намерно или ненамерно да узрокују каскадне ефекте изван оквира првобитног циља напада“ (Mulvenon & Rattray, 2012, 18). Поред сличности постоје и разлике између сајбер и нуклеарног сукоба: „1. Националне државе углавном не преузимају одговорност за предузете непријатељске акције у сајбер простору. 2. Није било застрашивања тиме шта може да учини сајбер напад; инциденти

попут *STUKSNET* - а и малвера који је уништио 30.000 хард драјвера нафтне компаније у Саудијској Арабији су довели до значајних поремећаја, али нису били довољни да озбиљно утичу на операције у нуклеарном погону или нафтној компанији. 3. Изузетно тешко је идентификовати починиоца у сајбер простору; што не би био случај приликом покретања нуклеарног оружја и, 4. Развој нуклеарног оружја се може пратити, а за разлику од њега, не постоји слична транспарентност за производњу сајбер оружја у држави, нити надзорна међународна агенција која прати такве развоје" (Iasiello, 2013, 398). Поменуте разлике између сајбер и нуклеарног сукоба указују да стратегија за нуклеарно одвраћање није примењива у сајбер простору (Iasiello, 2018, 42).

„Стратегија одвраћања од тероризма (*Terrorism Deterrence*)" - Ова стратегија се показала успешном у неколико случајева. На пример, када терористичка организација преузима атрибуте националне државе, односно када поседује имовину која се одмаздом може оштетити, тада може да се утиче на вођство терористе тако да оно ограничи своју политику и деловање зарад очувања ресурса које организација поседује. Убиство терористичког лидера највишег ранга, такође може ефикасно да одврати терористе од планираних активности, али само на одређено време док се поново не организују. Како би стратегија одвраћања била успешна, противничка страна „мора да разуме (имплицитну или експлицитну) претњу и доносе одлуке које су резултат калкулације трошкова и користи" (Trager & Zagorcheva, 2005 - 2006, 87). Неуспели покушаји да се спречи истрајни противник указују да има много више препрека, него користи од ове стратегије. Када се ова стратегија примени на сајбер домен, који није нужно везан за једну исту локацију намеће се питање: Како да делујемо на појединца или групу терориста у сајбер простору без поуздане информације ко су они заправо или где живе? Још један фактор који компликује примену ове стратегије у сајбер домену је мотивација. Може се рећи да терориста који делује у сајбер простору цени сопствени живот, обзиром да се служи сајбер оружјем и виртуелним идентитетом. Дакле, он није директно угрожен. Док, терористи који делују оперативно у реалном / физичком свету компромитују себе и спремни су да изгубе властити живот зарад остварења циљева организације.

„Стратегија одвраћања од претњи непријатељских држава (*Rogue State*s)" се примењује ради очувања националне безбедности. САД примењују ову стратегију одбране у односу према Сирији и Северној Кореји. Како би стратегија одвраћања била што ефикаснија,

развијена је њена посебна форма – „прилагођена одвраћања (*tailored deterrence*)“ (Knopf, 2013). То су специјално дизајниране стратегије одвраћања према обавештајним информацијама о свакој држави или ситуацији понаособ, чија је сврха да циљано делују на психолошке профиле лидера и њихове одлуке. Примена ове стратегије у сајбер окружењу није погодна, због сложености и разноликости учесника у сајбер нападу. Терористи не функционишу као непријатељски настројена држава чија је крајња сврха стабилност сопственог режима и очување лидерства.

Либицки наводи да је основни циљ сајбер одбране да смањи „ризик од сајбер напада на прихватљив ниво по прихватљивим ценама“ (Libicki, 2009, 32). У вези „стратегије одвраћање помоћу казне“, потребно је да национална држава пре било какве одмазде ни у ком случају не заговара увредљиве радње, него једино пажљиво одабране поступке у одбрамбене сврхе. Ајасиело сматра да успешна стратегија одвраћања помоћу казне почива на „три основна аксиома: 1. приписивање (*Attribution*), 2. поновљивост (*Repeatability*), 3. успех (*Success*)“ (Iasiello, 2018, 46). Пре покретања било каквог контраударца неопходно је познавати: идентитет починиоца, његову намеру, мотивацију, начин извршења напада, мету напада и коначни циљ. Односно, како би приписивање било што прецизније потребно је имати одговоре на што већи број питања: „Да ли је сајбер терориста повезан са националном државом? Да ли делује самостално или је добио наређења одозго? Да ли одмазда пропорционално одговара причињеној штети? Да ли је коначни циљ напада национална држава или је циљ нешто друго? Да ли је намера нападача била да: уништи, деградира, оспори или нешто друго? Да ли је напад имао другу сврху осим оне која се види на површини?“ (Iasiello, 2018, 47). Даље, не може једна иста стратегија да се примењује за сајбер одбрану од различитих врста напада, нападача и циљева. Успех зависи од примењене тактике. Односно различите тактике кажњавања треба примењивати пре, током или након што се одређени сајбер напад десио.

Обзиром да је „домен сајбер простора инхерентно нестабилан“ (Mulvenon & Rattray, 2012, 23), Удружење за испитивање сајбер конфликата (*Cyber Conflict Studies Association*) предлаже пет нивоа одбране: „1. стратегија, 2. војска и оперативa, 3. недржавни актери у сајбер простору, 4. домаће и међународно право, 5. приступи за ублажавање сајбер конфликата“ (Mulvenon & Rattray, 2012, 17 - 27).

Бегс и Батлер сајбер одбрану рашчлањују на још више нивоа, односно девет тачака. Отуда они наводе да ефикасна борба против

сајбер тероризма треба да се одвија према безбедносном плану „*SPECTR FCC*: *Strategy* (стратегија), *Policy* (политика), *Education* (обука), *Communication* (комуникација), *Technology* (технологија), *Responsibility* (одговорност), *Funding* (финансирање), *Commitment* (посвећеност) и *Co - operation* (сарадња)“ (Beggs & Butler, 2004, 389).

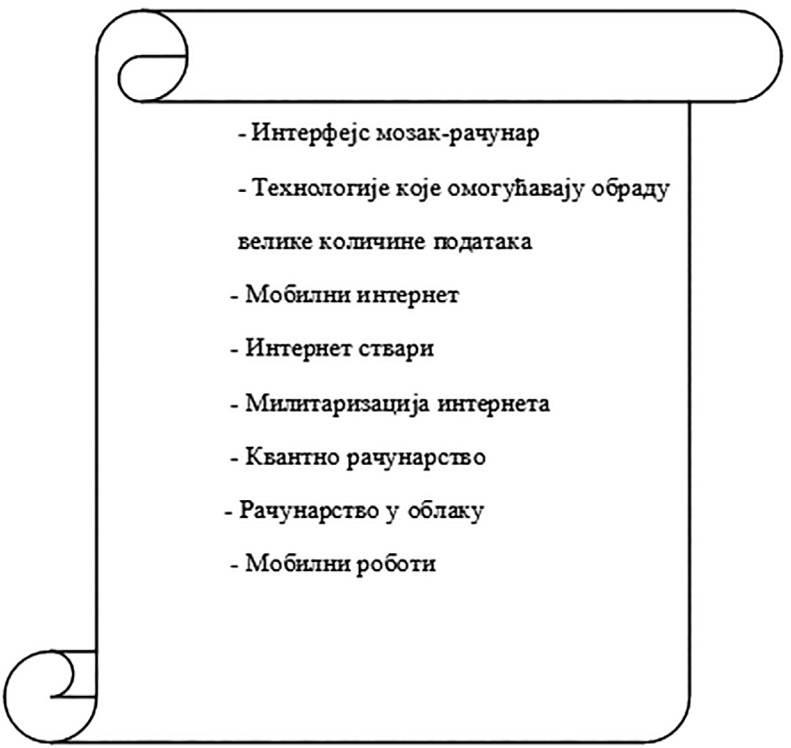
Нове идеје одбране од сајбер тероризма се проширују на улогу недржавних актера. Досадашње схватање о доминацији државних актера у суочавању са сајбер сукобима и изазовима је погрешно. Приватни сектор поседује процентуално више глобалних рачунарских мрежа. Потребна је тесна сарадња између државног и приватног сектора, нарочито са приватним специјализованим јединицама за сајбер област. Приватни сектор треба да пружи отпор сајбер тероризму, спречи или избегне напад.

На који начин организације треба да спроводе своју одбрану од сајбер тероризма? Основа добре борбе против сајбер тероризма је планирање. Донешене стратегије треба да се имплементирају редом у складу са циљевима, према вишегодишњем плану. Политика је други неизоставни део безбедносног плана јер омогућава запосленима у организацијама да се информишу о правилима понашања, да их разумеју и примењују у свакодневним радним активностима и на тај начин подрже функционисање безбедносних механизама. Обуке пак, омогућавају руководиоцима и менаџерима да прате трендове и развој безбедносних механизама, што је неопходно имајући у виду динамичност сајбер домена. Четврта ставка је добра комуникација како између организација, тако и унутар саме организације, док је примена напредне технологије једна од ставки, али не и најзначајнија, обзиром да су технолошке рањивости узрочници сајбер напада. Неизоставни део безбедносног плана је одговорност, односно сви запослени унутар организације треба да се опходе одговорно према подацима и усвојеним механизмима заштите. Ефикасна одбрана од сајбер тероризма подразумева финансирање безбедносних механизама и обуку запослених. Неопходно је да сви запослени буду подједнако посвећени очувању сајбер безбедности и да одржавају сарадњу са другим организацијама, ради размене искуства и проблема у овој области. Обавеза државе је да претње и сајбертерористички напад благовремено открије, гони и процесуира. Ефикасна одбрана од сајбер тероризма подразумева сарадњу између приватног и државног сектора. Тако да је потребно да приватни сектор активно сарађује и доставља податке држави о сајбер инцидентима и сумњивом понашању у сајбер простору.

Подједнако државни, приватни сектор и појединци деле

одговорност за безбедност информационих система. Неопходна је сарадња да би се сајбер простор ставио под јединствени безбедносни оквир, који треба да „укључи заједничку стратегију и визију различитих економских, техничких и комерцијалних питања сигурности“ и „све слојеве безбедности: обука и свесност, превенција, истраживање и откривање, реаговање и опоравак“ (Alqahtani, 2016, 13). Поред тога, потребно је фокусирати се на стварање успешне сарадње између тимова који су специјализовани да пружају решења у области сајбер безбедности (Sommestad, 2012).

Слика 7. Процењене главне области које ће се развијати у будућности, а захтевају посебну пажњу и сајбер безбедносне мере (Alqahtani, 2016, 13).



8. МЕЂУНАРОДНА САРАДЊА У БОРБИ ПРОТИВ САЈБЕР ТЕРОРИЗМА

Међународна правна регулатива

Проблематику сајбер безбедности компликује постојање три суштинска проблема (технички, политички и правни) који постоје од самог настанка информационих и комуникационих технологија. Дакле, први проблем је техничке природе. „Основни технички проблем лежи у срцу сајбер простора, пошто основна архитектура никада није била дизајнирана имајући на уму безбедност; штавише првобитни дизајнери нису никада ни помишљали да ће се мрежа користити у злонамерне сврхе“ (Mulvenon & Rattray, 2012, 1). Приоритети првобитних дизајнера су били примењивост и лако повезивање корисника (конекција), технолошке иновације које олакшавају живот. Други проблем је политичке природе јер „је еволуција технолошке архитектуре знатно превазишла одговарајући скуп идејних, доктринарних, организационих, и правних структура, што резултира реактивном и атавистичком динамиком политике, где се садашње идеје и организације често баве јучерашњим проблемима без флексибилности да се баве будућим проблемима на основу најављених технолошких иновација“ (Mulvenon & Rattray, 2012, 1). Трећи проблем је правне природе. Примена законодавства на интернет и правно регулисање његових бројних могућности дилема је правника широм света. Стављање дигиталног под правни оквир, као и примена „аналогних“ територијалних закона на неодређене дигиталне границе бесконачне глобалне комуникационе мреже, „чини се да је превише за наше конвенционалне правне системе“ (Akhgar, Staniforth & Bosco, 2014, 3).

Рањивост сајбер простора отвара могућности за извршење сајбер тероризма, па је потребно регулисати све активности које се спроводе у или у вези са сајбер простором. У ту сврху Котим (Cottim, 2010) предлаже пет јурисдикционих теорија и приступа:

1. „Територијална теорија“ - место где је кривично дело почињено, у целости или делимично одређује јурисдикцију. Слабост овог приступа огледа се у томе што је он заснован на претпоставци да држава има неупитно суверенитет над територијом која је предмет расправе, што није нимало лако потврдити обзиром на флуидне границе сајбер простора. Иначе, ова теорија има своје корене у моделу државног суверенитета према којем су успостављени Вестфалски мировни споразуми (Beaulac, 2004, 181).
2. „Теорија националности (или активне личности)“ - заснована је првенствено на националности починиоца кривичног дела.

3. „Теорија пасивне личности“ - Док се „теорија националности“ бави националношћу починиоца, „пасивна теорија личности“ се бави националношћу жртве. Котим ово назива „подручје сајбер криминологије“ и као добар пример овог приступа наводи случај када је један руски држављанин осуђен на суду у Хартфорду у Конектикату због хаковања рачунара у Сједињеним Америчким Државама.

4. „Теорија заштите“ (такође позната као „принцип сигурности“ и „теорија о повређеним форумима“) - бави се повређеним националним или међународним интересима и додељивањем надлежности држави која остварује интерес, било национални или међународни у ситуацији проузрокованој нападом. Котим наводи да се ова теорија ретко примењује, углавном код злочина попут фалсификовања новца и вредносних папира.

5. „Теорија универзалности“ – ослања се на принцип универзалности који је заснован на међународном карактеру кривичног дела који омогућава свакој држави да тражи надлежност за учињена кривична дела, чак и ако та дела немају директног утицаја на ту државу. Иако делује да ова теорија има највише потенцијала за примену у сајбер простору, Котим указује да постоје њена два кључна ограничења. Прво ограничење је то што држава мора да има оптуженог у притвору када захтева надлежност под претпоставком да је учињено кривично дело. Док је друго ограничење то што злочин треба да буде „нарочито увредљив за међународну заједницу“. Постоје значајне практичне потешкоће које отежавају дефинисање параметара принципа универзалности и могућности проширења овог принципа на област сајбер простора и активности у њему. Теорија универзалности се углавном примењује код кривичних дела пиратерије и код илегалне трговине робом.

Као што примећује Хафнер (Hafner, 1998) иако је интернет мрежа настала 1960 - их година, сајбер сукоби нису били виђени као забрињавајућа претња све до краја 1980 - их, када су два значајна догађаја подстакла забринутост око сигурности и поузданости на интернету. Први догађај је био 1987. године када је истраживач Клиф Стол (Stoll, 2005) открио хакера који је користио мрежу националне лабораторије „Lawrence Berkeley“ да би хаковао друге мреже укључујући војне базе и одбрану. Крајем осамдесетих је Роберт Морис, први пут пустио „црва“ (Orman, 2003) и тиме угрозио безбедност интернета, након чега је осуђен на основу Закона о

рачунарским преварама и злостављању, упркос његовим изјавама да је желео да измери величину интернета и да није био злонамеран. Дакле, са закашњењем тек након 80 - тих година започиње еволуција кривичног права у области сајбер безбедности. Као што наводи Сибер (Sieber, 1994, 25 - 28), 1992. године усвојене су основне смернице за санкционисање злонамерне употребе рачунара у Немачкој. Према наводима Шјолберга (Schjolberg, 2014, 24 - 31) први закони којима се инкриминише злоупотреба рачунара усвојени су крајем XX века у многим земљама (Италија, САД, Велика Британија, Аустралија, Немачка, Данска, Шведска, Норвешка, Аустрија, Француска, Холандија, Шпанија, Финска и др).

Сведоци смо свакодневног развоја информационих и комуникационих технологија који се одвија толико великом брзином да га готово једва примећујемо. Сваке године излазе нови, савременији модели паметних телефона, рачунарске опреме и друге врсте уређаја, чију примену брзо и олако прихватамо. Технолошки развој је проширио могућности за злоупотребу савремене технологије. Правна регулатива и међународна сарадња нису ишли у корак са овим развојем, што такође примећује и Шмит када наводи: „Нажалост, постојеће правне норме не нуде јасан и свеобухватан оквир унутар којег државе могу да обликују политичке одговоре на опасност од непријатељских сајбер операција“ (Schmitt, 2010, 152). Јер, убрзан развој информационих и комуникационих технологија изискује константне напоре, едукацију и друга улагања за праћење нових изазова у области IT индустрије. Зато само неколицина земаља поседује адекватне правне регулативе које омогућавају ефикасно санкционисање и кажњавање сајбер криминала и сајбер тероризма. То је подстакло намеру држава да прилагоде законску реглуативу савременим ризицима и да постојеће кривичне законе употпуне новим одредбама, не само на нивоу једне државе, него и на међународном нивоу у области сајбер безбедности. Међутим, формирање правне основе на међународном нивоу је процес који траје и захтева шире, свеобухватније размишљање о узроцима и динамици сајбер тероризма.

Међународно хуманитарно право према Бјанкију пружа „регулаторни оквир“ и „ефикасне“ механизме „за кажњавање терористичких акција“ (Bianchi, 2011, 21). Односно, међународно хуманитарно право „осуђује терористичка дела и на међународном и унутрашњем плану и нуди систем за гоњење и кажњавање“ (Condorelli & Naqvi, 2004, 37).

Међутим, резултати истраживања потврдили су да „владе,

када су под претњом тероризма, крше нека од права која желе на првом месту да заштите“ (Dreher, Gassebner & Siemers, 2010, 88). Супростављање тероризму генерално, може да „створи опасну и погрешну слику о релативности људских права, и скоро неизбежно подразумева интрузивни надзор и губитак приватности, ограничено кретање у земљи и иностранству и одузимање основних права и заштите у систему кривичног правосуђа“ (Jones & Howard - Hassmann, 2005, 62 - 63). Међутим, „упркос забринутости многих заговорника људских права, владе не реагују увек на терористичке нападе ограничавањем права. Уместо тога, однос је компликованији, јер терористички напади подстичу ограничења неких права, али не и других. Друго, кршење људских права од стране влада може да буде снажан предуслов за касније терористичке нападе“ (Piazza & Walsh, 2010, 407).

Сајбертерористичка дела по природи могу или не могу да покрену оружани сукоб, у зависности од конкретних околности. Када је у питању тумачење и примена закона једне конкретне државе преко њених административних граница јурисдикције, суочавање са сајбер тероризмом је дискутабилно, јер је линија раздвајања између употребе силе и међународног хуманитарног права замућена. Отуда Шмит наводи четири кључна питања везана за регулисање сајбер операција кроз призму међународног права:

> „1) Када сајбер операција представља недозвољену *употребу силе* којом се крши Повеља Уједињених нација, члан 2 (4) и међународно обичајно право?;
>
> 2) Када сајбер операција представља *претњу и кршење мира или поступак агресије* тако да Савет безбедности може да дозволи пружање одговора за то?;
>
> 3) Када сајбер операција представља *оружани напад*, такав да може држава - жртва да се брани, чак и кинетички, у складу са правом на самоодбрану из члана 51. Повеља УН и према обичајном међународном праву?;
>
> 4) Када се сајбер операција подиже до нивоа *оружаног сукоба*, тако да га међународно хуманитарно право регулише као ратне активности?“ (Schmitt, 2010, 152).

Шмит (Schmitt, 1999, 18) је идентификовао низ фактора помоћу којих се економска и политичка принуда могу ограничити од употребе оружане силе. Примена ових фактора на сајбер домен може да утиче на процену државе о томе да ли одређене сајбер операције представљају употребу силе:

1. „Тежина последица“ - Процена озбиљности штете у

зависности од скале, опсега и трајања последица. Да ли причињене штете представљају само мању непријатност или провокацију за појединца и / или имовину? Или је више екстремна и утиче на критичне националне интересе? (Schmitt, 1999, 18).

2. „Моменталност“ - У зависности од временског аспекта, односно појављивања штетних последица: непосредно или одложено и споро штетно дејство. Када се штетне последице одмах манифестују, пред државом је задатак да брзо реагује (Schmitt, 1999, 18).

3. „Директност“ - Односи се на ланац узрочности. Што је веза између почетног чина и последица слабија, мања је вероватноћа да ће држава сматрати актера одговорним за кршење забране употребом силе. На пример, евентуалне последице економске кризе одређују тржишне снаге, приступ тржиштима и др. Каузална веза између иницијалних аката и њихових ефеката је индиректна. Насупрот томе, код експлозије су узрок и последица директно повезани (Schmitt, 1999, 18).

4. „Инвазивност“ - Што је циљани систем сигурносно боље обезбеђен, то је већа забринутост у погледу продирања у систем. Конкретан пример је сајбер шпијунажа која иако је веома инвазивна, не представља употребу силе (или оружани напад), већ се према међународном праву третира као недозвољен физички продор на територију циљане државе, као у случају ратног брода или војног авиона који прикупља обавештајне податке из њеног територијалног мора или ваздушног простора (Schmitt, 1999, 19).

5. „Мерљивост“ - У интересу државе је да измери што је могуће прецизније количину причињене штете. Разматрано са аспекта међународног права, економска принуда може да изазове значајне патње, али не представља употребу силе. Са друге стране војни напад се класификује на основу измереног степена разарања. Тешко је идентификовати или квантификовати штету која је причињена у сајбер простору (Schmitt, 1999, 19).

6. „Претпостављени легитимитет“ - Међународно право изричито забрањује одређена дела, а она која нису забрањена претпоставка је да су легитимна. Било у домаћем или међународном праву, примена насиља сматра се нелегитимном, с посебним изузетком када је у питању самоодбрана (Schmitt, 1999, 19).

7. „Одговорност“ - Законом се уређује када ће држава да буде одговорна за сајбер операције. Што је чвршћа веза између одређене државе и операција у сајбер простору, то ће бити већа вероватноћа да ће остале државе то карактерисати као употребу силе, што доводи у питање међународну стабилност (Schmitt, 2010, 916). Зато је потребно посебну пажњу усмерити на војну политику, која би према наводима Кара: „требало да буде усмерена ка увођењу међународних правних механизама који би омогућили спречавање потенцијалних агресора да неконтролисано и потајно користе сајбер наоружање“ (Carr, 2010, 168). Технолошки развој је изнедрио нове форме сајбер алата / оружја чије последице могу да буду деструктивне исто као и приликом употребе регуларног оружја. Отуда бројни аналитичари (Weigant, 2013; Rauscher, 2013) указују да је ратни закон постао неадекватан и предлажу да се повећа регулација сајбер простора.

Сајбер тероризам је посебна форма тероризма. Скоро да и не постоји светски регион у којем није разматрана борба против тероризма. Међутим, иако су многе земље потписнице бројних конвенција и протокола из области тероризма и његових различитих појавних облика, практична примена није нимало једноставна. Као што примећују Комлен Николић и сарадници, основне препреке за сузбијање сајбер криминала на међународном нивоу су: правна неусаглашеност око дефинисања радњи и облика извршења појединих кривичних дела; недовољна обученост лица задужених за поступање у предметима сајбер криминала (полиције, тужилаца и судија), неусклађеност правила истраге кривичних дела сајбер криминала и неусклађеност или одсуство механизама правне помоћи и споразумне екстрадиције на међународном нивоу (Комлен Николић и др., 2010, 31).

Имајући у виду да је сајбер тероризам претња међународних размера, велики број међународних организација се бави сајбер безбедношћу ради свеобухватнијег и квалитетнијег супростављања овом проблему. Донет је велик број докумената и организован је велики број конференција које разматрају питање сајбер безбедности на међународном нивоу. Документа која су настала као резултат ранијих заседања много пута су представљана у литератури. Зато ћемо за ову прилику навести само неке од актуелних договора и конференција, новијег датума која се баве проблемом безбедности у сајбер простору.

Договор ЕУ за подручје сајбер безбедности за 2019. годину

(*EU cybersecurity organizations agree on 2019 roadmap*) (Enisa, 2018 - European Union Agency for Network and Information Security) настао је након састанка који је одржан 6. новембра 2018. године између директора: Меморандума о разумевању (MoU - *Memorandum of Understanding*), Агенције Европске уније за сигурност мреже и информисања (ENISA), Европске агенције за обелодањивање (EDA - *European Defence Agency*), Еуропола, Компјутерског тима за хитно реаговање (CERT - *Computer Emergency Response Team for the EU Institutions*). Циљ састанка је био међусобна сарадња и размена информација о релевантним дешавањима, процена постигнутог напретка у области сигурног и отвореног сајбер простора. Како би побољшали међусобну размену информација договорено је да фокус будуће сарадње буде на заједничкој обуци и сајбер вежбама, заједничким пројектима и догађајима којима се допуњава рад поменутих организација и избегава дуплирање напора.

Европска Комисија је 16. децембра 2020. године изнела Предлог директиве о отпорности критичних субјеката (*CER -Proposal for a Directive on the resilience of critical entities*, 2020) и Предлог директиве о мерама за висок ниво сајбер безбедности широм ЕУ (*Proposal for a Directive on measures for a high common level of cybersecurity across the Union,* 2020). *CER* има за циљ да унапреди пружање услуга неопходних за одржавање виталних друштвених функција или економских активности на унутрашњем тржишту повећањем отпорности критичних субјеката који пружају такве услуге. Предложеном директивом опсег деловања ЕУ не ограничава се само на отпорности критичне инфраструктуре, већ се протеже даље од ових мера и укључује секторске и међусекторске мере, између осталог, за заштиту од климе, цивилну заштиту, директна страна улагања и сајбер безбедност. Овај предлог је у блиској вези са предложеном Директивом о мерама за постизање високог заједничког нивоа сајбер безбедности широм Уније. NIS2 Директива (NIS2 - *The Network and Information Security*) има за циљ да повећа отпорност информационо - комуникационих технологија. NIS2 (NIS2, 2021) ће заменити ранију NIS Директиву ради остварења веће међуповезаности између физичког и дигиталног света кроз законодавни оквир са снажним мерама отпорности, како за сајбер тако и за физичке аспекте, како је наведено у Стратегији безбедносне уније. Директива NIS је допринела: 1) побољшању способности сајбер безбедности на националном нивоу тако што је од држава чланица захтевала да усвоје националне стратегије сајбер безбедности и да именују органе за сајбер безбедност; 2) повећана је сарадња између

држава чланица на нивоу Уније успостављањем различитих форума који олакшавају размену стратешких и оперативних информација; и 3) побољшала је сајбер отпорност јавних и приватних субјеката у седам специфичних сектора (енергетика, транспорт, банкарство, инфраструктура, финансијско тржиште, здравство, снабдевање и дистрибуција воде за пиће и дигитална инфраструктура) и у три дигиталне услуге (онлајн тржишта, онлајн претраживаче и услуге онлајн рачунарства) захтевајући од држава чланица да обезбеде да оператери основних услуга и провајдери дигиталних услуга испуњавају захтеве за сајбер безбедност и пријаву инцидента.

16 - 18. децембра 2021. године - датум одржавања Конференције Међународне телекомуникационе уније (*ITU Plenipotentiary Conference* 2021) (ITU, 2021). Међународна телекомуникациона унија (ITU- *International Telecommunication Union*) створена је 2005. године на Светском самиту о информационом друштву. ITU на сваке четири године сазива конференцију за своје државе чланице на којој се доносе одлуке о њеном даљем раду и израђују стратешки и финансијски планови који имају за циљ да утичу на развој информационих и комуникационих технологија широм света. Један од ITU пројеката је Индекс глобалне сајбер сигурности (*GCI - Global Cybersecurity Index*) који служи за мерење и унапређење сајбер безбедности националних држава. Форум за управљање интернетом, (*IGF*- I*nternet Governance Forum*) је посебно формиран орган који нема мандат да међународне уговоре и остала правна документа усваја, али представља базу одлука коју усвајају друге инситуције за управљање интернетом. Такође, једном годишње се организује Светски форум информационог друштва (*WSIS - The World Summit on the Information Society*), чији је основни циљ изградња поверења и сигурности за коришћење информационих и комуникационих технологија. Марта 2018. године поменути форум је доделио Србији престижну награду за допринос и стварање повољног окружења за развој информационог друштва. WSIS је глобална платформа која се бави одрживим развојем информационог друштва тако што подстиче партнерства, размену информација и најбољих пракси, стварање знања истовремено идентификујући трендове који се појављују у ИТ области. Тема форума који је одржан 17 - 21. маја 2021. године била је „ИКТ за инклузивно, отпорно и одрживо друштво и економију" (WSIS forum, 2021). Током одржаног састанка нарочито су се издвојила питања: сајбер безбедности, изградње капацитета и оснаживања жена у ИКТ.

APECTEL (APEC Telecommunications and Information Working

Group) је након десетог заседања у марту 2015. године развио стратешки акциони план за период 2016 - 2020. год. Који је имао за циљ да обезбеди да што више људи у азијско - пацифичком региону има безбедан приступ интернету и савременим IT технологијама. Неколико земаља чланица Лиге арапских држава која датира из 1945. године усвојило је законе о сајбер криминалу (Пакистан, Саудијска Арабија и Уједињени Арапски Емирати (UAE). На онлајн заседању 2020. године домаћин је био Нови Зеланд. Према новом акционом плану за период 2021 - 2025. године APEC (APEC, 2021) ће наставити да ради на повећању поверења у ИКТ и њихову примену промовишући важност сајбер безбедности, сарадње и размену знања. Акционим планом се подржава капацитет свих релевантних актера у привредама APEC - а да управљају ризицима, стварају отпорне мреже и омогућавају поуздано окружење за трансакције и комуникације.

Мултилатерална сарадња је неопходна за успешно суочавање са проблемом сајбер тероризма, јер као што примећује Грабоски: „Дигитални криминал не познаје границе између држава“ (Grabosky, 2007, 15.). Зато „борба против високотехнолошког криминала треба да буде или глобална или нема смисла“ (Broadhurst, 2006, 414). Приметно је појачано интересовање за сарадњом по питању сајбер безбедности, како од стране међународних организација тако и појединих земаља. Борбу против сајбер тероризма треба тумачити са становишта теорије „црног лабуда“ (Nicholas, 2007) која се односи на непредвидиве и мало вероватне догађаје који имају снажан утицај на људску заједницу и који након првог догађања постају вероватнији и предвидљивији.

Општи оквир мултилатералне сарадње за супротстављање сајбер тероризму прописује механизме за пружање међународне кривично - правне помоћи. Сарадња се одвија на сва три нивоа: макро - ниво, подразумева уговорну сарадњу између држава и међународних организација, мезо - ниво се односи на кооперативност државних органа који су специјализовани и надлежни за *ad hoc* потребе и микро - ниво подразумева непосредну и неформалну сарадњу надлежних органа једне државе (Bryant & Stephens, 2014, 112 - 113).

Мултилатерална сарадња

Регулације које се односе на суочавање са проблемом тероризма индиректно се односе и на проблем сајбер тероризам који је његова посебна форма. Уједињене нације су такође препознале сајбер тероризам као једну од најзначајнијих опасности која прети савременом човечанству. Уједињење Нације су дале велики допринос по питању безбедности и одбране од тероризма и доносиоци су бројних међународних докумената, резолуција и других докумената почев од 30 - тих година XIX века. Након атентата 9. октобра 1934. године у Марсељу донешена је резолуција којом се забрањује „било какво уплитање у политички живот друге државе“ (Chandan, 1935, 405). У периоду од 1. до 16. новембра 1937. године у Женеви је одржана Међународна конференција посвећена тероризму. Од прве половине XIX века до данас донешена су бројна документа која су резултат бројних седница, заседања и конференција. Како се тероризам временом усложњавао, тако су и УН прописивале нова документа и формирале органе за супростављање тероризму. Након терористичког напада на Њујорк и Вашингтон Уједињене нације су донеле одлуку за оснивање Комитета за борбу против тероризма 2001. године.

Кофи Анан је као вршилац дужности генералног секретара УН предложио светским челницима да прихвате заједничку дефиницију тероризма и договоре услове под којима међународна заједница може да употреби силу ради одбране мира и сигурности. Такође, УН су доносилац Глобалне антитерористичке стратегије (*UN Global Counter - Terrorism Strategy*) која је јединствени инструмент за супростављање тероризму на међународном нивоу. Ова стратегија се изнова разматра на сваке две године, како би пратила тренд развоја тероризма и базира се на: четири основна стуба: први - откривање услова који погодују ширењу тероризма, други – превенција и сузбијање тероризма, трећи - изградња државних капацитета и јачање улоге Уједињених нација и четврти – осигурање владавине људских права и закона (UN Global Counter - Terrorism Strategy, 2006).

Уједињене нације се активно баве проблемом тероризма. Током јуна и јула 2021. године је одржана двонедељна конференција на тему борбе против тероризма на којој су учествовали руководиоци агенција земаља чланица. Основни циљ конференције је изградња новог партнерства и јачање мултилатералне сарадње у борби против тероризма (United Nations, 2021). На поменутој конференцији су

идентификована стара и нова питања, продубљено је разумевање постојећих проблема и изазова, истражене су могућности за проналазак ефикаснијих одговора у борби против тероризма. Уједињење нације настоје да обезбеде антитерористичку платформу за стручњаке из различитих географских, мултикултуралних и родних миљеа ради посвећене размене знања у циљу унапређења глобалног и вишеслојног приступа који је неопходан за борбу против тероризма и насилног екстремизма. Уједињене нације су једна од водећих међународних организација која озбиљно и континуирано улаже напоре за супротстављање поменутом проблему.

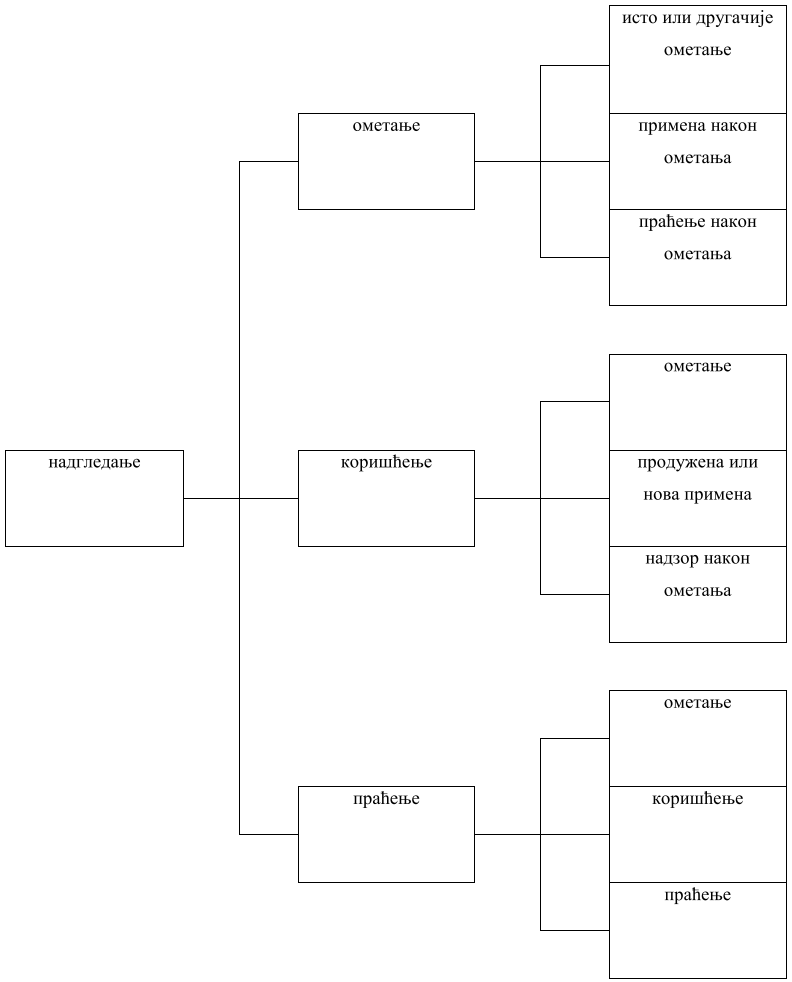
NATO, политичко - војна евроатлантска алијанса је већ дуже време свесна претњи нове форме ратовања – сајбер ратовања, као и осталих претњи које произилазе из сајбер простора. У новембру 2002. године одржан је самит у Прагу, на којем су лидери NATO - а одлучили да ојачају своје способности одбране од сајбер напада. Поменута одлука, подстакла је систематичнији приступ и многе иницијативе и програме за сузбијање тероризма у оквиру NATO - а. Тада су формирана различита NATO тела која су добила надлежности по питању заштите и одбране од сајбер инцидената: а) Агенција NATO - а за комуникације и информационе системе (NCSA - *NATO Communication and Information Systems Services Agency*), сматра се првом линијом одбране од сајбер тероризма, б) NATO INFOSEC Технички Центар (NITC - *NATO INFOSEC Techinical Center*) који је одговоран за компјутерску и комуникацијску сигурност, ц) Оперативни центар (NIAOC - *NATO Information Assurance Operations Centre*) који је надлежан за послове управљања и координацију криптографске опреме која се користи за пружање одговора на сајбер нападе који су усмерени против NATO; д) NATO центар за пружање одговора на компјутерске инциденте (NCIRC - *NATO Computer Incident Response Capability*), чији је основни задатак заштита шифроване комуникације унутар NATO система. NCIRC је главни извор техничке и оперативне стручности и могућности NATO - а у области сајбер одбране, који служи да заштити NATO субјекте (нпр. управу NATO - а) и мисије; служи за решавање претњи којима је угрожена сајбер сигурност NATO информационих система (NATO, 2002).

Слика 8. NATO сајбер одбрана (Fidler, Pregent & Vandurme, 2013 ,7)

На септембарској NATO радионици 2006. године у Израелу први пут је представљен „M.U.D модел“ као вид одговора на сајбер тероризам, који је потом разматран у октобру 2007. године на NATO радионици која је одржана у Анкари, у Турској. Сајнај описује M.U.D као вишестепени модел који подразумева опције: мониторинга, односно надгледање, пасивни надзор, коришћење сметњи у интернет саобраћају и онлајн садржајима како би се уклонили штетни материјали и блокирао им се приступ (Sinai 2011, 23 - 24).

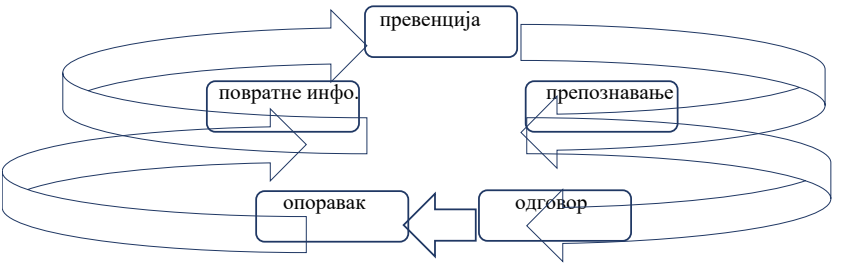
НАТО почиње интензивније да се фокусира на сајбер одбрану, након што је Естонија била жртва координираног сајбер напада 2007. године. Преко три недеље владини и скупштински портали, министарства, новинске куће, интернет провајдери велике банке и мала предузећа у Естонији били су мета DdoS напада. Поменути напади су се поклопили са одлуком владе Естоније која је одлучила да уклони из центра Талина споменик Бронзаном војнику који је био посвећен погинулима у Другом Светском рату. Естонија је себе прогласила за прву жртву међународног сајбер напада. НАТО министри су се 2008. године у Нордвијку договорили о „концепту сајбер одбране“, објављен је Талински приручник и започет је развој НАТО одбрамбене сајбер политике, која је 2010. године постала део „Стратешког концепта“ (Bogdanovski & Petreski, 2016).

Табела 10. Визуелна представа М.У.Д. модела (Weimann, 2015, 190)



НАТО капацитети за одговор на компјутерске инциденте-НЦИРЦ (NCIRC - *NATO Computer Incident Response Capability*) представљају главни НАТО извор техничких и оперативних способности и стручност у сајбер одбрани ради пружања заштитите НАТО ентитета и мисија. НЦИРЦ подразумева различите активности превенције, откривања, реаговања и опоравка система информационих технологија да помогне чланицама НАТО – а у остваривању сајбер безбедности (слика 9).

Слика 9. НЦИРЦ методологија (Fidler, Pregent & Vandurme, 2013, 10)



НАТО је на разним скуповима који су организовани (на пример у Велсу 2014. и Варшави 2016. године) питања сајбер безбедности и сајбер одбране истакао у први план. У периоду 15. до 17. октобра 2019. године одржан је симпозијум NIAS19 - *Nato Information Assurance Symposium* (NIAS19, 2019) како би НАТО чланице размениле своја искуства и најбоље праксе и понудиле иновативна решења за унапређење сајбер сигурности.

НАТО и Европска унија (ЕУ) сарађују кроз технички аранжман о сајбер одбрани, који је потписан у фебруару 2016. У светлу заједничких изазова, НАТО и ЕУ јачају сарадњу у области сајбер одбране, посебно у областима размене информација, обука, истраживању и вежбама. На самиту у Бриселу 2021. године (NATO, 2021) савезници су подржали нову свеобухватну политику сајбер одбране, која подржава кључне задатке НАТО - а и свеукупно одвраћање и одбрану како би се додатно побољшала отпорност Алијансе. НАТО сајбер тероризам види као озбиљну претњу која у будућности може значајно да наруши безбедност и стабилност зато одржава добру сарадњу са међународним организацијама које се такође баве питањима међународне безбедности: УН, ОЕБС и др.

Савет Европе (CoE - *Councile of Europe*) је дао велики допринос у области борбе против сајбер криминала. На предлог Савета Европе основан је 1997. године Комитет експерата за област криминала у сајбер простору (*Committee of Experts on Crime in Cyber - space*) који су били ангажовани на изради „Конвенције о сајбер криминалу“ (*Convention on Cybercrime*). Конвенција је завршена у јуну 2001. године и представља први међународни споразум на тему сајбер криминала. У новембру исте године у Будимпешти је потписана од стране тридесет четири земље које су учествовале у церемонијалном чину, док је шест земаља ратификовало ову Конвенцију (Естонија, Литванија, Мађарска, Румунија, Албанија и Хрватска). Конвенција

садржи: листу злочина које свака држава потписница мора да унесе и криминализује у своје законе, процедуралне механизме и стандарде које свака држава потписница треба да имплементира у оквиру својих закона, обавезује их на међусобну сарадњу и најшире међународне истражне мере и поступања у вези са кривичним делима која се односе на компјутерске системе и податке или за прикупљање доказа у електронском облику који су везани за кривична дела. Ова Конвенција ужива велик међународни ауторитет и отворена је за све, не само за државе чланице Савета Европе. До новембра 2021. године овој конвенцији су приступиле 66. земље. Комитет министара Савета Европе усвојио је 17. новембра 2021. године Други протокол уз Конвенцију о сајбер криминалу о побољшаној сарадњи и обелодањивању електронских доказа (Council of Europe, 2021), проширио је правну регулативу у сајбер простору, пружа бољу заштититу корисника интернета и помоћ у достизању правде за оне који постану жртве злочина.

ОЕБС (OSCE - *Organization for Security and Co - operation in Europe*) је почео интензивније да се бави сајбер безбедношћу након одлуке Савета министара 2004. године да прати различите активности и злоупотребу интернета од стране терориста као што су: финансирање терориста, пропаганда и њихово регрутовање (Bogdanovski & Petreski, 2016, 68). ОЕБС игра важну улогу у јачању сајбер безбедности. ОЕБС - ов Форум за безбедносну сарадњу превасходно је основан с циљем да прати процес наоружавања како би се спречили ризици и обезбедила војна сигурност и стабилност у Европи. ОЕБС поред најосновнијих политичко - војних споразума међу државама чланицама у свој рад све више укључује и разматра питања сајбер безбедности, изазова у сајбер простору и питање претње од сајбер оружја. Одељење ОЕБС - а за транснационалне претње (TNTD - *The Transnational Threats Department*) препознаје сајбер тероризам као значајну претњу и ради на размени знања и искуства у области сајбер безбедности. 22. и 23. јуна 2021. организована је трећа међурегионална Конференција о сајбер безбедности у Бечу на којој је учествовало 280 владиних и невладиних представника (OSCE, 2021). Сврха конференције је била да обезбеди отворену платформу за дијалог између представника државних органа, привредника, стручњака и младих о актуелним темама заштите од сајбер претњи.

Европска Унија такође поклања велику пажњу питању сајбер безбедности. Према подацима Еуростата до 2019. године, удео домаћинстава ЕУ који имају интернет прикључак порастао је на

90%, што је за око 26 % више него у 2009. години. Широкопојасни приступ интернету у 2019. години има 88% домаћинстава што је 33% више него у 2009. години (55%). Проценат особа старосне доби од 16 до 74 година у Европској Унији који су наручили или куповали робу или услуге путем интернета за приватну употребу износи око 60% у 2019. години, 14% више него у 2014. години (Eurostat Statistics, 2020).

Допринос Европске уније у супротстављању сајбер тероризму базира се на Стратегији сајбер безбедности за достизање отвореног и сигурнијег сајбер простора. Стратегија је усвојена 2013. године, након вишегодишње сарадње земаља чланица Европске уније у области безбедности. Основни циљеви стратегије су: јачање сајбер отпорности, значајније смањење сајберкриминалних активности, јачање могућности сајбер одбране развијањем индустријских и технолошких средстава и стварање јединствене европске политике сајбер безбедности која је у складу са досадашњом безбедносном и одбрамбеном политиком ЕУ која се базира на поштовању и промовисању основних принципа и вредности на којима почива Европска унија (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013). Земље ЕУ су донеле и прихватиле „Европску безбедносну агенду" 2015. године (*The European Agenda on Security*) у оквиру које је посебна пажња посвећена борби против сајбер криминала и сајбер тероризма (The European Agenda on Security: Questions & Answers, 2015). Усвајању агенде је претходила Директива о безбедности мрежа и информација којом су се чланице ЕУ обавезале 2013. године, која поред боље сарадње заговара и изградњу капацитета сваке чланице понаособ за спровођење сајбер безбедности. Све чланице ЕУ према одредби Европске комисије усвојиле су да „напад посредством информационих система" буде кажњив као терористички акт, уколико има за циљ „озбиљну измену или уништење политичких, економских или социјалних структура" (Bogdanovski & Petreski, 2016, 64). Европска Унија константно ради на решавању изазова у области сајбер безбедности. У децембру 2020. године ЕУ је усвојила нову Стратегију сајбер сигурности (The EU's Cybersecurity Strategy for the Digital Decade, 2020).

Поред владиних организација, у свету постоје многе агенције и невладине организације које се баве сајбер сигурношћу и одбраном од сајбер претњи, као што су: Тим за реаговање на компјутерске инциденте (CSIRT - *Computer Security Incident Response Team*), *Cybercom group* - нордијска ИТ компанија, невладине организације *Human Rights Watch*и *Amnesty International*, организација APWG - *Unifying the Global Response to Cybercrime* која се бави пружањем

обједињеног глобалног одговора на компјутерски криминал, ISACI - конзорцијум за постизање безбедности на интернету и многе друге. FIRST (*Forum for Incident Response and Security Teams*) је оперативни глобални лидер у суочавању са претњама у сајбер простору. Броји више од 400 чланова којима пружа брз одговор и размену информација, приступ најновијим документима најбоље праксе и размену искуства на конференцијама.

Вајмен наводи три корака за оперативно праћење и надгледање терориста на интернету. Први корак је надгледање терористичких веб страница с циљем праћења тока терористичких размишљања, мотива, пратилаца терориста и њихових активности, планова и потенцијалних циљева напада. Други корак је прикупљање података са вебсајтова. Организације које се боре против тероризма треба да "користе" терористичке вебсајтове да идентификују и лоцирају пропагандисте, модераторе дискусија, интернет провајдере, оперативце и њихове учеснике. Прикупљени подаци се архивирају и математички обрађују зарад идентификације кључних особа или кластера људи унутар мреже и да би се мерила робустност мреже. Трећи корак подразумева ометање терористичких вебстраница и других онлајн платформи на различите начине било негативном кампањом, сајбер нападима - вирусима и црвима или збуњивањем терориста и њихових присталица лажним техничким информацијама (Weimann, 2015, 188 - 190).

СИРТ (SIRT - *Security Incident Response Team*) ради по принципу детектовања сајбер инцидената помоћу индикатора, затим се алармирају / информишу војска, лица и организације са списка (*alert roster*) и одашиље им се порука (*alert message*) - скриптовани опис сајбер инцидента, који пружа довољно информација за адекватан сајбер одговор. Након што се штета у потпуности елиминише, следи поступак опоравка, и пре него што се пређе на свакодневне рутинске дужности, стручњаци СИРТ тима израђују прецизан извештај *after - action review* који садржи информације од првог корака (детектовање сајбер инцидента) до последњег корака (опоравка). Поменути извештај служи као лекција за обуку особља за будуће запослене СИРТ тима (Mattdort & Whitman, 2011, 283).

Индикатори који могу да упућују на вероватни сајбер инцидент су: „1. изненадне неочекиване активности (*Activities at unexpected times*); 2. појава нових налога (*Presence of new accounts*); 3. пријављени напади (*Reported attacks*); 4. обавештења (*Notification from IDS*)" (Mattdort & Whitman, 2011, 278). Матдорт и Витман такође наводе и шест индикатора који дефинитивно потврђују сајбер напад:

„1. употреба неактивних налога (*Use of dormant accounts*); 2. промене приступних налога (*Changes to logs*); 3. присуство хакерских алата (*Presence of hacker tools*); 4. обавештења партнера, сарадника (*Notifications by partner of peer*); 5. обавештења хакера (*Notification by hacker*); 6. употреба необичних протокола (*Use of unusual protocols*)“ (Mattdort & Whitman, 2011, 278 - 279).

Поред Русије, Кине и Француске, САД имају најсофистицираније оперативно - организационе способности одбране од сајбер тероризма. Помак у реализовању сајбер безбедности направљен је 2008. године када је Савезна регулаторна агенција за енергетику (*Federal Electric Regulatory Agency*) прописала мере и правила која важе за све компаније које послују у области енергетике, и санкционисала непоштовање тих правила и процедура новчаном казном од милион долара дневно (Clarke & Knake, 2010, 88). Влада САД - а користи Ајнштајн (*Einstein*) напредни систем за надгледање мрежне комуникације и детекцију напада. Као што наводе Кларк и Кнејк постоје три дела овог система „Ајнштајн 1, Ајнштајн 2 и Ајнштајн 3“ и сваки од њих има засебну функцију. Први део служи за праћење протока саобраћаја, други део служи за откривање упада и малициозних програма, док трећи део има функцију одбране, тако што блокира малициозне програмске пакете са Интернета (Clarke & Knake, 2010, 101 - 102). Безбедност мреже се у САД повећава захваљујући одбрамбеној тријади: „кичма (потпора), заштита мреже снабдевања електричном енергијом и лична заштита (самозаштита)“ (Clarke & Knake, 2010, 131 - 134) која служи не само да стопира различите врсте сајбер напада, него омогућава и јачу контролу активности у сајбер простору. Два кључна проблема сајбер одбране су техничке и политичке природе.

Интернет саобраћај је тешко пратити због великог протока информација. Електронски надзор телекомуникација подразумева електронско прислушкивање телефонских разговора и праћење других начина комуникације, што се коси са поштовањем политике приватности. Електронски надзор комуникација се спроводи превасходно због прикупљања релевантних доказа у судском поступку, за откривање мреже чланова терористичке организације, утврђивање хијерархије и целокупног криминалног деловања. Ову методу могу да примењују једино законски овлашћене особе, уз поштовање одређених начела. Спровођењу ових мера приступа се у случајевима када се истрагом није могло доћи до адекватних доказа, или када примена претходних мера није дала резултат, према тачно наведеном захтеву који садржи „чињенице“, наведене околности

под којима су искоришћене све методе које нису давале адекватан резултат, као и разлоге због којих се сматра да би примена метода тајног прислушкивања дала резултате. Захтев за прислушкивање треба да садржи и временски рок у којем ће се спроводити надзор комуникације који може трајати до тридесет дана, који се спроводи на основу наредбе надлежног судије. Мера надзора може се продужавати на још тридесет дана у неколико наврата, такође уз сагласност надлежног судије" (Weaver, Abramson & Bacigal, 2007, 564). Уколико околности које проистичу из терористичке активности то особито налажу, може се применити и тајни надзор лица чији идентитет није у потпуности утврђен, а које су повезане са најтежим злочинима, као и метод прикривеног иследника. Овај метод се ређе примењује због недовољно јасне правне регулативе и тешкоћа које произилазе из саме реализације планираних послова прикривеног иследника. Већина чланова терористичке организације је неповерљива према новопридошлицама, што додатно отежава продор до врха терористичке организације. Ситуацију прикривеног иследника додатно компликује специфичност околности „у случајевима када прикривени иследник треба да учествује у злочину, за шта му одобрење даје Одбор за вођење тајних истрага у случајевима нужде, како би се прибавиле информације и сазнања које остварују циљ вођења кривичног поступка осумњиченог; уколико би се на тај начин сачувала веродостојност прикривеног иследника или уколико би на тај начин прикривени иследник отклонио од себе смртну опасност или опасност од тежег телесног повређивања" (Јовић, 2001, 181).

Из наведеног можемо да закључимо да је међународна заједница итекако свесна ризика од употребе савремених информационих и комуникационих технологија и да је проблем безбедности сајбер простора актуелна тема која је неретко разматрана. Међутим, велики број докумената и мултилатерална сарадња не гарантују квалитетну превенцију и одбрану уколико донешене одлуке и усвојена документа постоје само као мртво слово на папиру. Односно, потребна је њихова практична примена и ефикасана оперативна.

9. НАЦИОНАЛНЕ МЕРЕ ЗА СУЗБИЈАЊЕ САЈБЕР ТЕРОРИЗМА

Правна регулатива у Србији

Геостратешки положај Србије и минули историјски догађаји: грађански рат и распад некадашње Социјалистичке Федеративне Републике Југославије, НАТО бомбардовање, наметнуте санкције Савезној Републици Југославији и проблеми транзиције знатно су обликовали савремени положај Републике Србије у међународној заједници и утицали на њено целокупно безбедносно стање. Највећу савремену претњу по безбедност Републике Србије представљају сепаратистичке идеје. Проблем самопроглашене републике Косово је један од најзначајнијих фактора дестабилизације и извора терористичких тежњи на овим просторима. Миграције избеглих лица са простора Сирије и Авганистана, као и тензије изазване кризом у Украјини додатно компликују безбедносну ситуацију.

Државни органи Републике Србије који у делокруг својих активности укључују област развоја и примене информационо - комуникационих технологија су:

- Министарство трговине, туризма и телекомуникација према „Закону о министарствима“ („Службени гласник РС“, бр. 128/20) надлежно је за „област телекомуникација, односно електронских комуникација и поштанског саобраћаја; уређење и безбедност у области електронских комуникација и поштанског саобраћаја; инспекцијски надзор; утврђивање стратегије и политике развоја електронских комуникација и поштанског саобраћаја; организовање финансијске и техничке контроле; међународне послове у области електронских комуникација и поштанског саобраћаја; мере за подстицање истраживања и развоја у области електронских комуникација и поштанског саобраћаја; утврђивање предлога плана намене радио - фреквенцијских опсега и доношење плана расподеле радио фреквенција; одлучивање о условима за издавање појединачних дозвола за коришћење радио - фреквенција; утврђивање списка основних услуга електронских комуникација (универзални сервис) које треба да пруже оператори, као и друге послове одређене законом“ („Службени гласник РС“, бр. 128/20). Поред осталих активности Министарство трговине, туризма и телекомуникација „обавља послове државне управе у области информационог друштва који се односе на: предлагање политике и стратегије развоја информационог друштва; припрему закона, других прописа, стандарда и мера у области електронског пословања; мере за подстицање истраживања и развоја у области информационог друштва; припрему закона, других прописа, стандарда и мера у области информационог

друштва и информационо - комуникационих технологија; примену информационо - комуникационих технологија; пружање информационих услуга; развој и функционисање информационо - комуникационе инфраструктуре; развој и унапређење академске, односно образовне и научноистраживачке рачунарске мреже; заштиту података и информациону безбедност; међународне послове у области информационог друштва“ („Службени гласник РС“, бр. 128/20).

- Министарство државне управе и локалне самоуправе у области примене информационо - комуникационих технологија надлежно је за систем државне управе, односно „развој електронске управе; припрему закона, других прописа, стандарда и мера у области електронске управе“ и стручно усавршавање запослених у државним органима према „Закону о министарствима”, члану 11 („Службени гласник РС“, бр. 128/20).

- Министарство грађевинарства саобраћаја и инфраструктуре поред осталих активности „уређење и безбедност техничко - технолошког система саобраћаја“ („Службени гласник РС“, бр. 128/20).

- Министарство одбране обавља поред осталог послове „усклађивање организације веза и информатичких и телекомуникационих система у Републици Србији за потребе одбране“ („Службени гласник РС“, бр. 128/20).

- Канцеларија за информационе технологије и електронску управу обавља послове који се односе на развој и функционисање система електронске управе, њихово пројектовање и усклађивање у органима државне управе и служби Владе. Канцеларија је надлежна за бројне послове међу којима су: пружање подршке за развој, увођење и примену стандарда, одржавање, унапређење и изградњу рачунарске мреже републичких органа. У оквиру активности Канцеларије за информационе технологије и електронску управу формиран је Државни центар за управљање и чување података у Крагујевцу који је према „Закону о електронској управи“: „физичка и виртуелна инфраструктура чија је намена смештање рачунара, сервера, мрежних и безбедносних система неопходних за функционисање електронске управе“ („Службени гласник РС“, бр. 27/18). Портал е Управе је национални веб портал. То је јединствена приступна тачка електронској управи органа, „збирка отворених података која служи за прикупљање, категоризацију и дистрибуцију отворених података у поседу органа и омогућава њихово лакше претраживање и поновну употребу“ према „Закону о електронској

управи“ („Службени гласник РС“, бр. 27/18). Канцеларија такође обавља различите послове за потребе Центра за безбедност ИКТ система републичких органа (ЦЕРТ) који према „Закону о електронској управи“ („Службени гласник РС“, бр. 27/18) примарно обавља „послове који се односе на заштиту од инцидената у оквиру јединствене информационо - комуникационе мреже електронске управе“ („Службени гласник РС“, бр. 27/18).

Поред поменутих и други државни органи и организације су надлежни за развој и имплементацију информационих система (Информациони системи МУП - а, Пореске управе, Управе царина, Управе за трезор, Геодетски информациони систем и др). Влада Републике Србије се залаже за развој паметних мрежа, подстиче иновације и бољу везу између науке, технологије и предузетништва и употребу капацитета нове информационе и комуникационе технологије за истраживање и развој отуда је прописала „Стратегију развоја мрежа нове генерације до 2023. године“ („Службени гласник РС“, бр. 33/18). Све већа примена савремених информационих и комуникационих технологија, као и дигитализација подразумевају и све већу укљученост и других државних органа, као што су: Министарство просвете, Министарство здравља, Министарство правде и др.

Министарство просвете, науке и технолошког развоја Републике Србије поседује сектор за дигитализацију, који је основан у циљу свеобухватне дигитализације у складу са актуелним међународним и националним стандардима. Основне активности овог сектора су: дигитализација података којима Министарство просвете, науке и технолошког развоја располаже, планско увођење и организовање дигитализације услуга и процеса; успостављање, унапређење и управљање постојећим е - сервисима како би се они унапредили за боље функционисање, постигла већа безбедност и контрола доступности података. Због широког дијапазона деловања сектора за дигитализацију у просвети и науци извршена је његова подела на три групе где је свака група посебно надлежна за дигитализацију у: просвети, науци и образовању: „1. група за е - Просвету, 2. група за е - Науку и 3. група за дигитализацију у образовању“ (Министарство просвете, науке и технолошког развоја, 2021). У оквиру „Стратегије научног и технолошког развоја Републике Србије за период од 2021. до 2025. године“ („Службени гласник РС“ бр. 10/21) информационо - комуникационе технологије су једна од четири приоритетних области. Ради остварења боље оптимизације и дигитализације основана су два нова института

(Институт за информационе технологије Крагујевац и Институт Био Сенс, Нови Сад). Успостављена је мрежа научно - технолошких паркова (Ниш, Чачак, Нови Сад, Београд) са тенденцијом даљег ширења. Влада Републике Србије и Европска Унија потписале су споразум којим је договорено да Република Србија буде део програма *Horizon 2020* који подразумева давање грантова за реализацију истраживачких пројеката, што умногоме потпомаже развој и примену нових стандарда и идеја.

Имајући у виду да је сајбер тероризам као и сваки облик тероризма у тесној вези са насиљем, документ који се индиректно односи на сајбер тероризам је „Правилник о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање“ („Службени гласник РС“, бр. 46/19, 104/20). Према поменутом документу поред традиционалних облика насиља и злостављања: физичко, психичко (емоционално) и социјално; дефинисана је и нова форма насиља под називом дигитално насиље. „Дигитално насиље и злостављање је злоупотреба информационих технологија која може да има за последицу повреду друге личности и угрожавање достојанства и остварује се слањем порука електронском поштом, СМС - ом, ММС - ом, путем веб - сајта (*web site*), четовањем, укључивањем у форуме, социјалне мреже и сл.“ („Службени гласник РС“, бр. 46/19, 104/20). Постојање свести о дигиталном насиљу је корак напред у препознавању и разликовању ове врсте насиља од ранијих традиционалних форми насиља, али и препознавању његових различитих врста (појавних облика).

Примена информационих и комуникационих технологија у области трговине и телекомуникација је у надлежности Министарства трговине туризма и телекомуникација које је на основу: „Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању“ („Службени гласник РС“, бр. 94/17) усвојило следеће правилнике и уредбе:

-„Правилник о условима које морају да испуњавају квалификовани електронски сертификати“ („Службени гласник РС“, бр. 34/18 и 81/18)

-„Правилник о условима које мора да испуњава квалификовано средство за креирање електронског потписа односно печата и условина које мора да испуњава именовано тело“ („Службени гласник РС“, бр. 34/18, 3/20, 87/20, 64/21)

-„Правилник о Регистру пружалаца квалификованих услуга од поверења“ („Службени гласник РС“, бр. 31/18)

-„Правилник о Регистру квалификованих средстава за

креирање електронских потписа и електронских печата“ („Службени гласник РС“, бр. 31/18, 64/21)

-„Уредба о условима за пружање квалификованих услуга од поверења“ („Службени гласник РС“, бр. 37/18)

-„Уредба о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости“ („Службени гласник РС“, бр. 60/18)

-„Правилник о Регистру пружалаца услуга електронске идентификације и шема електронске идентификације“ („Службени гласник РС“, бр. 67/18)

У оквиру „Закона о информационој безбедности“ („Службени гласник РС“, бр. 6/16, 94/17, 77/19) усвојене су следеће уредбе:

-„Уредба о ближем садржају акта о безбедности информационо - комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо - комуникационих система од посебног значаја” („Службени гласник РС“, бр. 94/16)

-„Уредба о ближем уређењу мера заштите информационо - комуникационих система од посебног значаја” („Службени гласник РС“, бр. 94/16)

Министарство трговине туризма и телекомуникација такође је усвојило:

-„Уредбу о безбедности и заштити деце при коришћењу информационо - комуникационих технологија“ („Службени гласник РС“, бр. 13/20). Поменута Уредба усвојена је 2016. године и замењена је новом у фебруару 2020. године с циљем да се: “подигне ниво свести и знања о предностима и ризицима коришћења интернета и начинима безбедног коришћења интернета; унапреде дигиталне компетенције деце, односно ученика, родитеља и других законских заступника и наставника и унапреди међуресорна сарадња у области безбедности и заштите деце на интернету („Службени гласник РС“, бр. 13/20).

-„Правилник о избору програма од јавног интереса у области развоја информационог друштва које реализују удружења“ („Службени гласник РС“, бр. 47/13 и бр. 88/16)

-„Правилник о захтевима за уређаје и програмску подршку за законито пресретање електронских комуникација и техничким захтевима за испуњење обавезе задржавања података о електронским комуникацијама“ („Службени гласник РС“, бр. 88/15) према којем „законито пресретање електронских комуникација обухвата откривање садржаја комуникација и надзор података о саобраћају

субјекта надзора у складу са законом; задржани подаци су подаци о електронским комуникацијама које је оператор дужан да задржи у складу са Законом о електронским комуникацијама" („Службени гласник РС", бр. 88/15, Уводне одредбе, члан 2).

На предлог Републичке агенције за електронске комуникације Министарство спољне и унутрашње трговине и телекомуникација усвојило је „Правилник о техничким и другим захтевима при изградњи пратеће инфраструктуре потребне за постављање електронских комуникационих мрежа, припадајућих средстава и електронске комуникационе опреме приликом изградње пословних и стамбених објеката" („Службени гласник РС", бр. 123/12) у којем је дефинисано значење појединих израза као што су: разне врсте апликација, као што су: апликације радиодифузних и комуникационих технологија (*BCT – broadcast and communication technology applications*), апликације информационих и комуникационих технологија (*ICT - information and communications technology applications*), апликације управљања, надзора и комуникације (*CCB - commands, controls and communications in building*), *ICT – information and communications technology* услуге и др.

Област информационог друштва у Републици Србији је регулисана бројним законима, од којих су најзначајнији:

-„Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала" („Службени гласник РС", бр. 61/05 и 104/09) регулише откривање, кривично гоњење и суђење за кривична дела која спадају у област високотехнолошког криминала. Према члану 2: „Високотехнолошки криминал у смислу овог закона представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику" („Службени гласник РС", бр. 61/05 и 104/09).

- „Закон о електронским комуникацијама" („Службени гласник РС", бр. 44/10, 60/13 – УС, 62/14 и 95/18) уређује услове за обављање и развој делатности у области електронских комуникација, регулише доступност услуга уз поштовање домаћих и међународних стандарда и процедура, осигурава безбедност комуникационих мрежа и услуга, као и заштиту података корисника електронских комуникација и др.

- „Закон о информационој безбедности" („Службени гласник РС", бр. 6/16, 94/17, 77/19) регулише мере заштите информационо - комуникационог система (ИКТ систем), уређује међународну сарадњу у области информационе безбедности, превенцију и заштиту

од безбедносних ризика, управљање ризиком, криптобезбедност, криптозаштита, тајност података, криптографски производ, криптоматеријали и др. „Овим законом се уређују мере заштите од безбедносних ризика у информационо - комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо - комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите" („Службени гласник РС", бр. 6/16, 94/17, 77/19, Члан 1).

- „Закон о електронској трговини" („Службени гласник РС", бр. 41/09, 95/13, 52/19) прописује мере којима се уређује пружање услуга информационог друштва, услови које је пружалац услуга дужан да поштује, обавезне информације које је дужан да достави кориснику услуга (потрошачу) и надзорном телу (Инспекторат за услуге информационог друштва), обавезе потрошача, као и захтеве које морају да задовоље комерцијална порука и електронски уговор за достизање пуноважности, привремено и трајно складиштење података и казнене одредбе за прекршаје.

- „Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању" („Службени гласник РС", бр. 94/17, 24/21). Овим законом се уређује електронско пословање и остали елементи неопходни за обављање електронске услуге, као што су: електронска идентификација, дигитализовани документ и електронски потпис, електронски печат, електронски временски жиг, валидација исправности електронског потписа и печата, сертификат за електронски потпис, сертификат за аутентикацију вебсајта и друго. У ставки VII Закона о електронском документу, електронској идентификацији и улугама од поверења у електронском пословању, члан 66 - 71 прописане су новчане казне у распону од 50.000 до 2.000.000 рсд у зависности од прекршаја („Службени гласник РС", бр. 94/17, 24/21).

- „Закон о електронском фактурисању" („Службени гласник РС", бр. 44/21) уређује издавање електронских фактура, њихово слање, пријем и обраду, начин на који се електронске фактуре чувају, одређује њихову садржину и елементе у трансакцијама између субјеката јавног и приватног сектора као и друга питања која су од значаја за електронско фактурисање.

- „Закон о управним споровима" („Службени гласник РС", бр. 111/09) поред тога што регулише предмет управног спора регулише и остале услове везане за предају тужбе у облику електронског документа као што је наведено у члану 20 и поступање

са електронским документима према члану 21. „Начин, техничке услове предаје и утврђивање времена предаје поднесака и доставе аката у облику електронског документа, као и друга питања везана за поступање са електронским документом, ближе се уређују Судским пословником“ („Службени гласник РС“, бр. 111/09).

- „Закон о заштити података о личности“ („Службени гласник РС“, бр. 87/18) члан 1: „Овим законом уређује се право на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебни случајеви обраде” и „право на заштиту физичких лица у вези са обрадом података о личности коју врше надлежни органи у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности, као и слободни проток таквих података.”(„Службени гласник РС“, бр. 87/18).

- „Закон о електронској управи“ („Службени гласник РС“, бр. 27/18) прописује начела за ефикасно и сигурно управљање опремом и системом електронске управе, евиденцију у електронском облику (успостављање и вођење регистара), коришћење и заштиту база података, чување безбедносних копија база података и докумената; прописује правилности њиховог прибављања и уступања, прописује јединствени налог електронске поште, лиценце за успостављање и вођење веб портала, као и његову употребу, забрану дискриминације, прекршајну одговорност и др.

- „Закон о платним услугама“ („Службени гласник РС“, бр. 139/14, 44/18) уређује област платних трансакција, платни рачун, платни налог, платне инструменте, област заштите права и интереса корисника платних услуга (платилаца и прималаца плаћања) и ималаца електронског новца, уређује референтни курс, готов и електронски новац, каматну стопу, услове и начин пружања домаћих и међународних платних трансакција, дозвољено и недозвољено прекорачење рачуна, врсте платних услуга, уређује девизно пословање, платни систем и његов надзор.

- „Закон о оглашавању” („Службени гласник РС“, бр. 6/16, 52/19 – др. закон) уређује област оглашавања у најширем смислу

(тв оглашавање, у штампаним медијима, на отвореним површинама, у електронским медијима), било да је у питању јавно оглашавање или пословно за пласирање одређених производа / услуга, правила и ограничења везана за садржај огласних порука, одговорност преносиоца огласне поруке, прописује забрану подстицања било које врсте дискриминације, угрожавање безбедности и здравља, обмане, прикривено оглашавање и др. Тако у члану 6 који прописује друштвену одговорност стоји: „Оглашавање мора бити засновано на принципу коришћења дозвољених средстава за постизање циља и другим принципима друштвене одговорности. Огласном поруком се не сме изазивати мржња или нетолеранција, злоупотребљавати поверење, однос зависности, лаковерност, недостатак искуства или знања и сујеверје прималаца огласне поруке. Огласна порука не сме да садржи изјаве или визуелно представљање које се може сматрати увредљивим. Огласна порука мора да буде истинита, у складу са законом, добрим пословним обичајима лојалне конкуренције и професионалном етиком" („Службени гласник РС", бр. 6/16, 52/19 – др. закон).

- „Кривични законик" („Службени гласник РС", бр. 85/05, 88/05 - исправка, 107/05 – исправка, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19) забрањује тероризам, односно:

-„диверзија, саботажа, шпијунажа, одавање државне тајне, изазивање националне, расне и верске мржње и нетрпељивости, повреда територијалног суверенитета, удруживање ради противуставне делатности, припремање дела против уставног уређења и безбедности Србије, тешка дела против уставног уређења и безбедности Србије" (члан 312 - члан 321)

- „јавно подстицање на извршење терористичких дела" (члан 391)

- „врбовање и обучавање за вршење терористичких дела" (члан 391 а, 3916)

- „употреба смртоносне направе" (члан 391 в)

- „уништење и оштећење нуклеарног објекта" (члан 391 г)

- „угрожавање лица под међународном заштитом" (члан 392)

- „финансирање тероризма" (члан 393)

- „терористичко удруживање" (члан 393 а)

Србија је у марту 2009. године ратификовала Конвенцију Савета Европе о сајбер криминалу, која је донета 23. новембра 2001. године у Будимпешти. Почев од 1. јануара 2006. године ступио је на снагу „Кривични законик" („Службени гласник РС", бр. 85/05, 88/05- исправка, 107/05- исправка, 72/09, 111/09, 121/12, 104/13,

108/14, 94/16 и 35/19), у којем су прописана „Кривична дела против безбедности рачунарских података“ (глави бр. XXVII, чл. 298. до чл. 304 а) следећа кривична дела:

- оштећење рачунарских података и програма - „Ко неовлашћено избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм, казниће се новчаном казном или затвором до једне године“ (члан 298).

- рачунарска саботажа – „Ко унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар или други уређај за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте, казниће се затвором од шест месеци до пет година“ (члан 299).

- прављење и уношење рачунарских вируса – „Ко направи рачунарски вирус у намери његовог уношења у туђ рачунар или рачунарску мрежу, казниће се новчаном казном или затвором до шест месеци. Ко унесе рачунарски вирус у туђ рачунар или рачунарску мрежу и тиме проузрокује штету, казниће се новчаном казном или затвором до две године“ (члан 300, став 1 и став 2).

- рачунарска превара –„Ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се новчаном казном или затвором до три године“ (члан 301, став 1). Раних 80 - тих година се појавила превара под именом „нигеријска превара“ или „превара 419“ која подразумева кривично дело преваре које се врши помоћу рачунара, тако што пошиљаоц електронске поруке, која је најчешће у *spam* - у, тражи иностран помоћ око трансфера велике количине новца из Нигерије, где је пошиљаоц електронске поруке спреман да учињену услугу новчано надокнади одређеним процентом од пребачене суме (Урошевић, 2009, 2-3). Целокупан процес се чува у строгој тајности. Садржај електронских порука је у суштини исти, без обзира на ситније детаље који могу да се разликују. Преваранти се најчешће служе украденим идентитетима лица која заиста постоје, а нису ни свесна да неко злоупотребљава њихов идентитет за вршење криминалне радње. Најчешће су извршиоци кривичних дела припадници мањих организованих криминалних група, некада делују и самостално,

али тада најчешће нису у могућности да изврше преваре већих размера. Уколико жртва пристане на електронски послату понуду, извршиоци кривичних дела траже жртви да уплати одређени новчани износ на име реализације договореног посла и шаљу јој фалсификована документа и траже нова одлагања уз обећање брзе исплате договореног процента. Када жртва схвати да је преварена, тада је већ касно и уплаћени новац не може никако да поврати назад.

- неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података – „Ко се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података, казниће се новчаном казном или затвором до шест месеци. Ко сними или употреби податак добијен на начин предвиђен у ставу 1. овог члана, казниће се новчаном казном или затвором до две године“ (члан 302, став 1 и 2).

- спречавање и органичавање приступа јавној рачунарској мрежи – „Ко неовлашћено спречава или омета приступ јавној рачунарској мрежи, казниће се новчаном казном или затвором до једне године“ (члан 303)

- неовлашћено коришћење рачунара или рачунарске мреже – „Ко неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист, казниће се новчаном казном или затвором до три месеца“ (члан 304)

- прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података – Према „Кривичном законику Републике Србије” забрањена је производња, употреба, увоз, продаја, дистрибуција и набавка уређаја и рачунарских програма, рачунарске шифре или сличних података који су првенствено пројектовани у сврхе извршења неког кривичног дела затворском казном од шест месеци до три године или новчаном казном (члан 304 а).

- незаконито руковање електронским новцем - Према „Закону о платним услугама” („Службени гласник РС“, бр. 139/14, 44/18), члан 2, тачка 13: „електронски новац означава електронски (укључујући магнетно) похрањену новчану вредност која чини новчано потраживање према издаваоцу тог новца, а издата је након пријема новчаних средстава ради извршавања платних трансакција и прихвата је физичко и / или правно лице које није издавалац тог новца“. Народна банка Србије има овлашћење да посредно или непосредно провери услуге које се наплаћују електронским новцем,

и уколико правно или физичко лице не омогући Народној банци Србије тражене информације и документацију у року, према Закону о платним услугама, члан 182. („Службени гласник РС“, бр. 139/14, 44/18) Народна банка Србије може том лицу да пропише новчану казну од: „100.000 до 500.000 динара за правна лица и од 30.000 до 100.000 динара за одговорна лица у правном лицу; од 30.000 до 100.000 динара за физичка лица“.

Више јавно тужилаштво у Београду је надлежно за кривично гоњење свих кривичних дела која су извршена помоћу високе технологије, према одредбама „Закона о јавном тужилаштву“ („Службени гласник РС“, бр. 116/08, 104/09, 101/10, 78/11 - др. закон, 101/11, 38/12 - одлука УС, 121/12, 101/13, 111/14 - одлука УС, 117/14, 106/15, 63/16 - УС). Посебно тужилаштво за високотехнолошки криминал основано је 2006. године. При Вишем суду у Београду за сва суђења високотехнолошког криминала надлежно је Одељење које је посебно формирано за борбу против поменуте врсте криминала, док је Апелациони суд у Београду надлежан за поступање по правним лековима.

Нормативно уређење употребе ИКТ када су корисници малолетна лица

Малолетна лица представљају значајан део популације који је активно укључен у информационе и комуникационе технологије. Они су корисници различитих услуга које интернет нуди: видео игре, *chat rooms*, *youtube* канали, услуге различитих претраживача, *e – mail* комуникације и друге сличне услуге. Малолетна лица су из најразличитијих разлога (незнања, незрелости и др.) лаке жртве за манипулацију, па су неретко учиниоци терористичких и других криминалних дела. Зато је неопходно ставити под законски оквир активности малолетника на интернету у виртуелном сајбер простору, али је такође нужно и санкционисати дела која су учињена над малолетним лицима уз употребу савремених информационих и комуникационих технологија.

Према „Закону о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица“ („Службени гласник РС“, бр. 85/05) прописано је „искључивање кривичних санкција према деци“ и у зависности од учињеног кривичног дела предлаже се примена васпитног налога. Израђен је „Нацрт закона о изменама и допунама закона о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица“ (2021) којим ће бити знатно побољшан положај малолетника као жртава. Новина је то што ће се све специјализоване евиденције у свим судовима и тужилаштвима да се сливају у централну базу. Према новом Нацрту закона у кривичном поступку ради кривичноправне заштите малолетних лица поступак воде једино судије које су стекле посебна знања из области права детета ради посебне заштите личности малолетног лица.

У оквиру посебног поглавља које је посвећено заштити деце и малолетника „Закон о оглашавању” („Службени гласник РС“, бр. 6/16, 52/19 – др. закон) прописује посебна правила за:

- „заштиту деце и малолетника од неприкладног оглашавања” (члан 21)
- регулисање „огласне поруке намењене деци и малолетницима” (члан 22)
- „злоупотребе неискуства, незнања и лаковерности” (члан 23)
- „заштита здравља и развоја” (члан 24)
- „заштита интегритета” (члан 25)
- „оглашавање у образовним и васпитним установама” (члан 25).

Оваква законска регулатива санкционише и отежава пуштање порука које се циљано односе на популацију малолетних лица у јавност било путем електронских медија или другог начина оглашавања како од стране терористе, тако и од стране било ког лица које не поштује правила која су „Законом о оглашавању" („Службени гласник РС", бр. 6/16, 52/19 – др. закон) прописана.

Током коришћења различитих интернет услуга неретко остављамо велики број личних података. Малолетна лица најчешће то чине када желе да постану чланови различитих *chat* форума и других социјалних мрежа у сајбер простору. Зато је у оквиру „Закона о заштити података о личности" („Службени гласник РС", бр. 87/18) уређена област обраде података о личности за малолетна лица, где је према члану 16. регулисан „пристанак малолетног лица у вези са коришћењем услуга информационог друштва" тако да „малолетно лице које је навршило 15 година може самостално да даје пристанак за обраду података о својој личности", а уколико „није навршило 15 година, пристанак мора дати родитељ који врши родитељско право, односно други законски заступник малолетног лица" („Службени гласник РС", бр. 87/18). На тај начин се малолетна лица штите од злоупотребе података приликом коришћења ИТ комуникација.

На који начин се малолетна лица штите од вршилаца кривичних дела над њима која се изводе применом информационих и комуникационих технологија? „Кривичним закоником" („Службени гласник РС", бр. 85/05, 88/05 - исправка, 107/05 – исправка, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19) су санкционисана кривична дела која су извршена над малолетним лицима уз примену савремених информационих и комуникационих технологија којима се крше полне слободе и врши прибављање за себе или друге, поседовање, приказивање или јавно излагање материјала порнографске садржине. Према члану 185. („Службени гласник РС", бр. 85/05, 88/05- исправка, 107/05 – исправка, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19) забрањује се и законски санционише новчаном казном или затвором искоришћавање малолетног лица уз употребу средстава информационих и комуникационих технологија:

- „за извршење кривичних дела против полне слободе према малолетном лицу" (члан 185 а)
- уколико се „договори са малолетником састанак и појави се на договореном месту ради састанка" (члан 185 б)
- „приступи сликама, аудио - визуелним или другим предметима порнографске садржине насталим искоришћавањем малолетног лица" (члан 185, тачка 5) и др.

Обзиром на савремену технолошку револуцију и све већу укљученост информационих и комуникационих технологија у образовни систем и свакодневни стил живота младих и малолетника, потребно је готово све законске регулативе којима се посредно или непосредно регулише област информационих - технологија и њене безбедности прилагодити малолетним лицима и младима.

10. СТРАТЕГИЈЕ

Упоредо са нормативним развојем и применом поменутих закона у Републици Србији усложњавала се и примена информационо - комуникационих технологија у јавној администрацији и приватном сектору. Како би уредила област информационог друштва Влада Републике Србије је усвојила различите стратегије, уредбе и акционе планове. У наставку монографије је приказано дванаест актуелних и најзначајнијих стратегија које су обликовале уређење информационог друштва у РС:

1. „Стратегија за борбу против прања новца и финансирања тероризма за период 2020 - 2024. године“ („Службени гласник РС“, бр. 14/20)
2. „Национална стратегија за спречавање и борбу против тероризма за период 2017 - 2021. године“ („Службени гласник РС“, бр. 94/17)
3. „Стратегија националне безбедности Републике Србије“ („Службени гласник РС“, 94/19)
4. „Стратегија одбране Републике Србије“ („Службени гласник РС“, бр. 94/19)
5. „Стратегија за борбу против високотехнолошког криминала за период од 2019. до 2023. године“ („Службени гласник РС“, бр. 71/18)
6. „Стратегија развоја вештачке интелигенције у Републици Србији за период 2020 - 2025“ („Службени гласник РС“, број 96/19)
7. „Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године“ („Службени гласник РС“, бр. 86/21)
8. „Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године“ („Службени гласник РС“, бр. 68/10)
9. „Стратегија развоја индустрије информационих технологија за период од 2017. до 2020. године“ („Службени гласник РС“, бр. 95/16) чијим објављивањем је престала да важи претходно донешена „Стратегија развоја и подршке индустрији информационих технологија“ („Службени гласник РС“, бр. 25/13)
10. „Стратегија развоја мрежа нове генерације до 2023. године“ („Службени гласник РС“, бр. 33/18)
11. „Стратегија заштите података о личности“ („Службени гласник РС“, бр. 58/10)
12. „Стратегија развоја дигиталних вештина у РС за период 2020 - 2024“ („Службени гласник РС“, бр. 21/20).

Стратегија за борбу против прања новца и финансирање тероризма

Први значајнији корак Владе Републике Србије у борби против тероризма био је 25. септембар 2008. године када је усвојена прва „Национална стратегија за борбу против прања новца и финансирања тероризма“ са циљем постизања ефикасне свеобухватне борбе против финансирања тероризма и прања новца. Од 2008. до 2021. године усвојени су нови међународни стандарди у области спречавања прања новца и финансирања теоризма ради пружања потпуне заштите финансијског система и привреде од опасности које узрокују прање новца и финансирање тероризма и како би се спречило ширење оружја за масовно уништење. Влада Републике Србије је 21. фебруара 2020. године усвојила нову „Стратегију за борбу против прања новца и финансирања тероризма за период 2020 - 2024.године“ („Службени гласник РС“, бр. 14/20) с циљем јачања интегритета финансијског сектора и ради унапређења безбедности и сигурности.

Прање новца се односи на незаконито прикривање порекла новца или имовине који су стечени на бесправан начин, криминалним активностима кроз три фазе: улагање, раслојавање (прикривање) и интеграција. Финансирање тероризма се одвија у неколико фаза. Прва фаза је прикупљање средстава. Терористи прибављају средства која су стечена вршењем разних кривичних дела као што су трговина дрогом, преваре и слично. Служе се различитим методама као што су изнуде, отмице да прикупе средстава из новчаних извора која су стечена на законити начин, али их терористи противправно присвајају. Такође прибављају средства од донација које добијају од симпатизера који подржавају циљеве терористичких организација. Друга фаза подразумева, чување прикупљених средстава на различите начине. Трећа фаза је пренос средстава ради његовог оперативног коришћења. Пренос се обавља на различите начине од кријумчарења преко државних граница до коришћења разноврсних механизама за прање новца. Последња четврта фаза је употреба финансијских средстава у терористичке сврхе.

Општи циљ поменуте стратегије је: „У потпуности заштитити привреду и финансијски систем државе од опасности које узрокују прање новца и финансирање тероризма и ширења оружја за масовно уништење, чиме се кроз активну сарадњу јавног и приватног сектора и приступ заснован на анализи и процени ризика јачају систем и интегритет институција финансијског и нефинансијског сектора и

доприноси безбедности, сигурности и владавини права“ („Службени гласник РС“, бр. 14/20). Четири посебна циља су изведена из општег:

„1. Смањивати ризике од прања новца, финансирања тероризма и ширења оружја за масовно уништење кроз континуирано унапређење стратешког, законодавног и институционалног оквира, координацију и сарадњу свих учесника у систему борбе против прања новца и финансирања тероризма и међународну сарадњу;

2. Спречити уношење у финансијски и нефинансијски систем имовине за коју се сумња да је стечена кривичним делом, која је намењена финансирању тероризма или ширењу оружја за масовно уништење, односно унапредити откривање такве имовине уколико је већ у систему;

3. Ефикасно и делотворно кажњавати извршиоце кривичног дела прање новца и одузимати незаконито стечену имовину;

4. Уочавати и отклањати претње од финансирања тероризма и кажњавати извршиоце кривичног дела финансирања тероризма“ („Службени гласник РС“, бр. 14/20).

Главни учесници за спровођење поменуте стратегије су: Управа за спречавање прања новца, Републичко јавно тужилаштво, судови, полиција, Војно - безбедносна агенција (ВБА), Војно - обавештајна агенција, Безбедносно - информативна агенција (БИА), Народна банка Србије (НБС), Комисија за хартије од вредности, Сектор тржишне инспекције, Управа царина, Порска управа, Агенција за борбу против корупције, Правосудна академија и Криминалистичко - полицијска академија, Удружење банака Србије и Адвокатска комора Србије.

Национална стратегија за спречавање и борбу против тероризма за период од 2017 - 2021. године

Република Србија је у настојању да очува мир и стабилност на регионалном и глобалном плану потписница многих најзначајнијих међународних докумената из области борбе против тероризма. Да би се на националном плану обезбедила од терористичких претњи и опасности које оне са собом носе, 2017. године је усвојена „Национална стратегија за спречавање и борбу против тероризма за период од 2017 - 2021. године" („Службени гласник РС", бр. 94/17).

Стратегија нуди основне смернице за унапређење постојећих метода и мера борбе против теророзма, и развој нових метода борбе и механизама превенције, „са циљем да успостави пропорцију између обима ангажованих ресурса и степена претње. Ова стратегија има за сврху заштиту Републике Србије од терористичке претње по њене грађане, вредности и интересе, уз истовремено подржавање међународних напора у борби против тероризма" („Службени гласник РС", бр. 94/17).

Стратегијом су предвиђене четири приоритетне области за чије спровођење су предложени следећи циљеви:

- Прва област „Превенција тероризма насилног екстремизма и радикализације који воде у тероризам" („Службени гласник РС", бр. 94/17) спроводи се помоћу пет циљева:

1. „Изграђена безбедносна култура грађана" – подразумева формално и неформално едуковање које ће омогућити подизање свести о претњама и опасностима од тероризма на виши ниво, па самим тиме и његово избегавање, лакше уочавање и алармирање надлежних органа.
2. „Рана идентификација узрока и фактора који погодују ширењу насилног екстремизма и радикализације који воде у тероризам" – омогућава планирање и координацију, па самим тиме и стварање повољнијег амбијента и укључивање свих чинилаца друштва за борбу против тероризма.
3. „Окружење које демотивише регрутовање младих за учешће у терористичким активностима" – омогућава јачање свести код младих и јачање демотивишућих елемената који спречавају младе да се определе за тероризам као облик испољавања незадовољства и деловања против постојећег друштвено - политичког система.
4. „Високотехнолошки системи комуникације и дигиталних мрежа који су отпорни на ширење радикализације и насилног

екстремизма“ – стављање ових система у службу безбедносне политике.

5. „Вештина стратешке комуникације“ – подразумева планski усмерену комуникацију и онемогућавање било какве злонамерне комуникације и интерпретације у служби тероризма и екстремистичких порука („Службени гласник РС“, бр. 94/17).

Друга област, „Заштита, уочавање и отклањање претњи од тероризма и слабости у систему заштите“ односи се на основне смернице за унапређење капацитета, система и механизама безбедности. С поменутим циљем се настоји достићи:

1) „Потпуно разумевање претњи од тероризма у Републици Србији кроз рану идентификацију циљаних група и радикалних метода;

2) Унапређена координација и сарадња између државних органа надлежних за прикупљање обавештајних података;

3) Подигнут ниво оперативних способности полицијских и обавештајно - безбедносних капацитета;

4) Унапређен систем за борбу против финансирања тероризма;

5) Дерадикализација и реинтеграција радикализованих особа;

6) Подигнут ниво заштите критичне инфраструктуре;

7) Унапређена ефикасност механизама интегрисаног управљања границом;

8) Подигнут ниво безбедности у области транспорта, трговине, размене роба и услуга“ („Службени гласник РС“, бр. 94/17)

Трећа област, „Кривично гоњење терориста, уз поштовање људских права, владавине права и демократије“ предложено је да се спроведе помоћу три циља:

1. „Усклађени национални прописи са одговарајућим резолуцијама Савета безбедности Уједињених нација, правним тековинама Европске уније и другим међународним стандардима

2. Унапређен систем откривања, идентификације и кривичног гоњења извршилаца кривичног дела тероризам и кривичних дела повезаних са тероризмом, уз поштовање људских права

3. Ефикасно суђење за кривично дело тероризам и друга кривична дела повезана са тероризмом“ („Службени гласник РС“, бр. 94/17)

Четврта област, „Одговор система у случају терористичког напада“ („Службени гласник РС“, бр. 94/17) предложено је да се спроводи кроз:

1) „Унапређен систем управљања последицама терористичког напада“ и
2) „Смањење последица терористичког напада“ („Службени гласник РС“, бр. 94/17). Стратегијом су предвиђени спровођење, праћење, координација и финансирање у циљу спречавања и борбе против тероризма.

Стратегија националне безбедности Републике Србије

На основу члана 9. став 2. тачка 2) Закона о одбрани („Службени гласник РС", бр. 116/07, 88/09, 88/09 – др. закон, 104/09 – др. закон, 10/15 и 36/18) и члана 8. став 1. Закона о Народној скупштини („Службени гласник РС", бр. 9/10), Народна скупштина је 27. децембра 2019. године донела „Стратегију националне безбедности Републике Србије" („Службени гласник РС", бр. 94/19).

Према Закону одбране „Стратегија националне безбедности Републике Србије је највиши стратешки документ чијом реализацијом се штите национални интереси Републике Србије од изазова, ризика и претњи безбедности у различитим областима друштвеног живота" („Службени гласник РС", бр. 116/07, 88/09, 88/09 - др. закон, 104/09 - др. закон, 10/15 и 36/18). У „Стратегији националне безбедности Републике Србије" („Службени гласник РС", бр. 94/19) указано је на утицај актуелних дешавања у свету и окружењу, као и значај међународне сарадње, наведени су основни ризици, изазови и претње по националну безбедност: сепаратистичка настојања појединих националистичких и верских екстремистичких група, нарочито албанске националне мањине на Косову и Метохији, једнострано проглашена независност Косова, национални и верски екстремизам, тероризам и његова повезаност са другим облицима криминала (организовани, транснационални и прекогранични), нерешен статус и тежак положај избеглих, прогнаних и интерно расељених лица, повећан ризика од високотехнолошког криминала и др.

Тероризам се сматра једним од највећих ризика и претњи за глобалну, регионалну и националну безбедност. У Стратегији је такође наведен ризик од угрожавања безбедности информационих и телекомуникационих система. „Динамика глобалног развоја информационих технологија условиће даље интензивирање активности у сајбер простору чију безбедност ће, превасходно, угрожавати сајбер шпијунажа, напади на критичну инфраструктуру, неовлашћени продори у базе тајних података, као и ширење лажних вести и дезинформација путем друштвених мрежа" („Службени гласник РС", бр. 94/19). Технолошки развој треба усмерити тако да буде у функцији развоја друштва и јачања националне безбедности. Јер, се на тај начин ствара добра основа за убрзан развој одбрамбене индустрије и њену примену.

У поглављу 4 наведено је да је политика унутрашње

безбедности усмерена превасходно на: „очувању суверености независности и територијалне целовитости Републике Србије, очување унутрашње стабилности и безбедности Републике Србије и њених грађана, очување постојања и заштите српског народа где год он живи, као и националних мањина и њиховог културног, верског и историјског идентитета, очување мира и стабилности у региону и свету, Европске интеграције и чланство у Европској Унији, економски развој и укупни просперитет, очување животне средине и ресурса Републике Србије“ („Службени гласник РС“, бр. 94/19)

Очување безбедности Републике Србије је динамичан процес, који захтева стално унапређивање и прилагођавање савременој друштвено - политичкој ситуацији у Републици Србији. Као што је наведено у Стратегији националне безбедности Република Србија ће наставити да доприноси сузбијању претњи од тероризма у свим појавним облицима и да спречава све врсте екстремизма и радикализма како на међународном нивоу кроз сарадњу, тако и на националном нивоу. Такође, Република Србија „настојаће да свој законски оквир и институционални капацитет за борбу против тероризма изгради у складу са стратешким оквиром и стандардима Европске уније“ („Службени гласник РС“, бр. 94/19) како би унапредила сопствене способности и капацитете за прикупљање, анализу, процену, заштиту и достављање података и информација о међународном тероризму и предузела све потребне мере ради спречавања терористичког деловања на свом простору.

Адекватна заштита од сајбер тероризма подразумева организовање стручних тела за координацију ради спречавања и сузбијања сајбер тероризма, по узору на организовање таквих тела у другим земљама. Међународни и национални програми који предлажу и прописују мере безбедности и заштите од сајбер тероризма предлажу благовремено откривање сајбертерористичких претњи кроз: адекватну процену опасности, откривање угрожавајућих терористичких организација, њихових планова, циљева и мотива, технолошких средстава и знања којима теористи располажу, координацију полицијских органа и противтерористичких снага на националном, регионалном и међународном нивоу, благовремено откривање и савладавање потенцијалних нападача у сајбер простору ради ефикасног спречавања извођења сајбер напада и онемогућавања даљих активности нападача, благовремено лишавање слободе, ефикасно вођење истражног поступка, адекватним суђењем и строгим кажњавањем нападача, програме васпитног усмеравања ради одвраћања од сајбер тероризма. Сложеност и специфичност

сајбер тероризма захтева непрекидне напоре, усавршавање мера заштите, истраживање и усаглашавање мера безбедности на међународном нивоу.

Стратегија одбране Републике Србије

Према Закону одбране: „Стратегија одбране Републике Србије је највиши стратешки документ у области одбране којим се дефинишу ставови о безбедносном окружењу, одбрамбеним интересима, мисијама и задацима Војске Србије, структура и функционисање система одбране“ („Службени гласник РС“, бр. 116/07, 88/09, 88/09 - др. закон, 104/09 - др. закон, 10/15 и 36/18).

Војском Србије командује Председник Србије у миру и рату. Док, Влада предлаже Народној Скупштини Републике Србије политику одбране која се спроводи у складу са међународним правом и обавезама. У складу са националним и одбрамбеним интересима Република Србија изграђује потребне капацитете и способности које су неопходне за одбрану од савремених безбедносних претњи.

Народна скупштина Републике Србије донела је „Стратегију одбране Републике Србије“ („Службени гласник РС“, бр. 94/19), која је усмерена на достизање развоја друштва и јачање националне безбедности, заштиту суверености и територијалне целовитости и пружање подршке цивилним властима у супротстављању од претњи којима се нарушава безбедност.

„Елементарне непогоде, техничко - технолошке несреће, као и радиолошка, хемијска и биолошка контаминација настала као последица ратних дејстава и техничко - технолошких несрећа представљају сталну безбедносну претњу за Републику Србију, њено становништво, материјална и културна добра и животну средину. Негативне последице ових појава могу да захвате и угрозе територије суседних држава, а могу се, исто тако, са територија суседних држава проширити на Републику Србију и угрозити њену територију и становништво“ („Службени гласник РС“, бр. 94/19). Стратегијом се предлаже унапређивање односа и сарадња са безбедносним службама других земаља на основу међународних и билатералних уговора и споразума ради постизања колективне безбедности.

Тероризам и сви његови појавни облици препознати су као озбиљна безбедносна претња. „Сепаратистичке тежње, посебно заступљене код појединих националистичких и верских екстремистичких група, као и интересних организација, представљају извор сталног безбедносног ризика и директну претњу територијалној целовитости Републике Србије“ („Службени гласник РС“, бр. 88/09). У зависности од могућности и степена угрожености државе планирају и развијају антитерористичке тимове. „Република Србија организује и развија антитерористичке тимове у саставу

војних оружаних и полицијских снага“ (Пејановић & Бејатовић, 2009, 270). Као што Пејановић указује антитерористички тимови при војним снагама усмерени су на елитне, брзе, организоване и ефикасне војне операције као облик супростављања терористичком деловању (Пејановић, 2003, 87).

Информационе и комуникационе технологије производе двоструки ефекат, истовремено и позитиван и негативан што се може негативно одразити на функционисање одбране. Адекватна заштита и развој ИКТ система одбране су примарни циљеви поменуте стратегије. „Сајбер напади на објекте критичне инфраструктуре, високотехнолошки криминал, угрожавање информационо - комуникационих система, као и ширење лажних вести и дезинформација у оквиру концепта хибридног и информационог ратовања могу се негативно одразити на функционисање елемената система одбране. Због тога је неопходно континуирано развијати технолошку и информациону заштиту елемената система одбране на свим нивоима организовања“ („Службени гласник РС“, бр. 94/19). Такође се предлаже јачање домаће одбрамбене индустрије, технолошка модернизација оружаних снага, развој способности и потенцијала одбрамбене индустрије, научно - технолошки развој, међународни пројекти и ширење тржишта одбрамбене индустрије, као и пласирање домаће војне опреме у Европи и у свету. Специјалне елитне јединице за противтерористичка дејства поуздано могу да делују уколико спроводе сопствена истраживања и сарађују са полицијским антитерористичким јединицама и другим обавештајним органима и службама.

Стратегија за борбу против високотехнолошког криминала за период 2019 - 2023. године

Влада Републике Србије је подстакнута преговорима са Европском Унијом у оквиру „Поглавља 24 – правда, слобода, безбедност“ (Министарство унутрашњих послова, 2015) усвојила „Стратегију за борбу против високотехнолошког криминала за период 2019 - 2023. године“ („Службени гласник РС“, бр. 71/18).

У оквиру поменуте Стратегије као круцијалне претње у области високотехнолошког криминала су препознате:

„1) криминал који зависи од напредних технологија;

2)“онлајн” сексуална експлоатација деце;

3) преваре везане за плаћање;

4)“онлајн” криминална тржишта;

5) преплитање сајбер криминала и тероризма;

6) унакрсни фактори криминала;

7) „онлајн” трговина фалсификованом робом” („Службени гласник РС“, бр. 71/18).

„Стратегија за борбу против високотехнолошког криминала за период 2019 - 2023. године“ („Службени гласник РС“, бр. 71/18) садржи предлоге и препоруке за суочавање са претходно наведеним претњама. Предлаже се детаљнија анализа претњи и сагледавање адекватних иницијатива за пружање онлајн безбедности и одбране, кроз фокусирање на вршиоце сајбер криминала и најчешће идентификована средства која су коришћена за извршење сајбер криминала (тројанци, малвери, добављачи неопходних средстава за извршење DDoS напада и др.), развијање антивируса и других механизама за адекватно и ефикасно реаговање на поменуте претње; истиче се важност координације и сарадње између државних органа надлежних за спровођење закона у области високотехнолошког криминала и приватног сектора који користи услуге савремених информационих и комуникационих технологија, заговара се доступност мера и истраживачких средстава за потребе истраживања, анализе и евидентирања онлајн организованог криминала, предлаже се одржавање заједничке превенције на нивоу целе заједнице, едукација родитеља и деце ради упознавања са претњама од сексуалне експлоатације деце путем интернета и осталих савремених технолошких средстава комуникације, глобална сарадња за дестабилизацију *darknet* - а.

Стратегија развоја вештачке интелигенције у Републици Србији за период 2020 - 2025.

Вештачка интелигенција почела је да се развија неуједначеним темпом пре неколико деценија у области дубоких неуронских мрежа. Очекује се да ће ова технологија да обликује развој свих сегмената функционисања привреде и друштва. Вештачка интелигенција има карактеристике технологије опште намене и може да унапреди ефикасност рада привреде, јавне управе и др. У свету је примећен тренд растуће количине података погодних за машинско учење и већа доступност микропроцесора погодних за нумеричка израчунавања. Многе државе су израдиле стратешки план за развој и примену ове врсте технологије. Република Србија је усвојила 31. децембра 2019. године „Стратегију развоја вештачке интелигенције у Републици Србији за период 2020 - 2025“ („Службени гласник РС“, бр. 96/19) којом су утврђене мере за даљи развој и имплементацију вештачке интелигенције ради постизања економског раста, унапређења јавних услуга и унапређења научних кадрова развојем вештина које су потребне за послове будућности. Поменутом Стратегијом су такође препознати „кључни изазови будућности у погледу регулативе“:

– Потреба за успостављањем више режима ограниченог регулаторног тржишта (*sendboks*) у циљу подстицања иновација;

– Потреба да држава прилагоди прописе који се односе на јавне набавке тако да користи иновативна решења заснована на вештачкој интелигенцији да унапреди ефикасност;

– Недовољна уређеност правног оквира који се тиче власништва над подацима;

– Регулација алгоритамске дискриминације (видети више у: Појединац и друштво)“ („Службени гласник РС“, бр. 96/19).

Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године

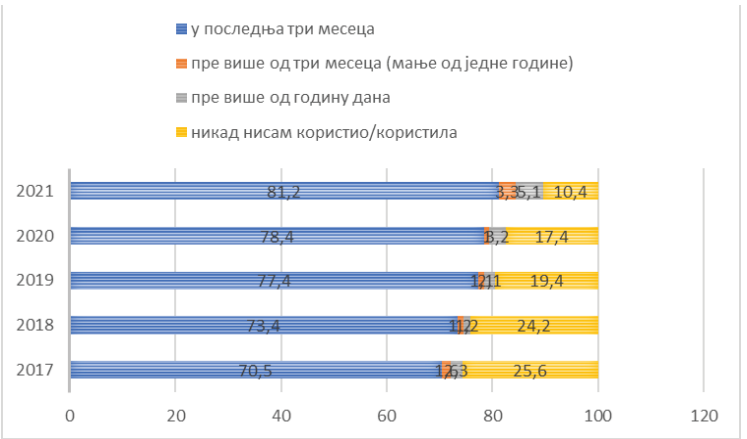
Влада је усвојила „Стратегију развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2025. године“ на основу члана 38. став 1. „Закона о планском систему Републике Србије“ („Службени гласник РС“, бр. 86/21). Први акт Владе Србије којим се уређује област информационог друштва донешен је 2006. године када је усвојена „Стратегија развоја информационог друштва у РС“ („Службени гласник РС“, бр. 87/06) која је престала да буде на снази доношењем нове стратегије 2010. године. Затим је уследила Стратегија из 2017. године која је престала да буде на снази доношењем нове стратегије 2021. године.

То је међусекторска стратегија „којом се утврђују циљеви и мере за развој информационог друштва и информационе безбедности“ („Службени гласник РС“, бр. 86/21). Њоме се стратешки усмерава развој информационог друштва на искористивост потенцијала информационих и комуникационих технологија како у области рада, тако и у свакодневном животу зарад бољег квалитета живота. Један од циљева стратегије је достизање приступа широкопојасном интернету по узору на просек у земаљама Европске уније, што подразумева да цене и услови буду као и у ЕУ.

Слика 10. Широкопојасна интернет конекција у домаћинствима (РЗС, 2021)

Републички завод за статистику (РЗС) годишње спроводи истраживање о употреби информационо-комуникационих технологија у Републици Србији. Према подацима из 2021. године 81,5 % домаћинстава поседује интернет прикључак, док заступљеност рачунара у домаћинствима износи 76,7%. Најзаступљенији тип интернет конекције је фиксна широкопојасна интернет конекција (91,7%), док мобилну широкопојасну интенет конекцију поседује 73,3% домаћинстава. Број корисника рачунара повећао се за 2% у односу на 2020. годину (РЗС, 2021).

Слика 11. Учесталост коришћења интернета (РЗС, 2021)



„Стратегијом развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2025. године“ („Службени гласник РС“, бр. 86/21) обухваћене су све приоритетне области које доприносе развоју информационог друштва:

1. „Електронске комуникације“ – квалитет приступа интернету у Републици Србији још увек није задовољавајући иако је доступност интернета релативно напредовала. Стратегија је усмерена на даљи раст и побољшање квалитета веза и повећање процента домаћинства која имају широкопојасни интернет.
2. „Е - управа, е - здравство и е - правосуђе“ – подразумева унапређење функционалности и сервиса Портала Е - Управа, информационог здравственог система и е - правосуђа. Примена ИКТ и електронских сертификата према „Закону о електронском документу, електронској идентификацији и улугама од поверења у електронском пословању“ („Службени

гласник РС“, бр. 94/17, 52/21) омогућава грађанима да без обавезног физичког присуства обављају одређене послове брже и јефтиније у службама и органима јавне управе, правосуђу и здравственој заштити.

3. „ИКТ у образовању, науци и култури“ – подразумева опремљеност установа, али и примену ИКТ у области науке, образовања и културе. Формирана академска рачунарска мрежа омогућава бржу и лакшу размену знања и искуства, истраживања и иновација што даље поспешује мултидисциплинарну примену технологије. Такође је посебна пажња посвећена дигитализацији у образовању, науци и култури, унапређењу ИКТ инфраструктуре у школама, унапређењу компетенција наставног особља у области ИКТ и запослених у јавној управи, унапређење свести о безбедности деце на интернету.

4. „Електронска трговина (е - трговина)“ - подстицање развоја и ширење дела тржишта применом електронских услуга (електронски рачуни и плаћање и др.) у области трговине. То подразумева одређене измене којима се отклањају нормативне и тржишне препреке чија је основна сврха заштита потрошача и безбедна е - трговина. Усвојен је „Закон о електронској трговини“ („Службени гласник РС“, бр. 41/09, 95/13, 52/19) и формирана је и објављена јавна листа квалификованих услуга од поверења.

5. „Пословни сектор ИКТ“ – Стратегијом се подстиче употреба, производња и извоз ИКТ опреме и ИТ услуга, развијање ИТ сектора *startup* пројектима и подстицањем иновативних компанија, развој људских ресурса и заштита интелектуалне својине софтвера и дигиталних садржаја, подстицање иницијативе малих и средњих предузећа да подигну ИКТ ниво пословања и знања.

6. „Информациона безбедност“ – Са развојем нових технологија и услуга јавља се и све већа потреба за подизањем нивоа информационе безбедности. Ризици информационе безбедности постоје како на страни државе, тако и на страни грађана и привреде. Информациона безбедност „представља скуп мера које омогућавају да подаци којима се рукује путем информационо - комуникационих система буду заштићени од неовлашћеног приступа, неодвојива је од права на заштиту података о личности који представљају велики део података који се чувају у оквиру ИКТ система“ („Службени гласник РС“, бр. 86/21).

Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године

Примена савремених технологија побољшава квалитет живота. Развој електронских комуникација је саставни део свих области друштвеног развоја, док је неоспорна њихова све значајнија употреба у готово свим областима друштвеног, али и државног деловања. Широкопојасни приступ интернету и његова примена у глобалној и националној привреди доприноси повезивању свих делова Републике Србије што поспешује развој руралних и удаљених области и њихово интензивније укључивање у националну привреду. Како би будући ток развоја електронских комуникација, укључујући и телекомуникације био усмерен у складу са релевантним међународним документима и предвиђеном моделу националне мреже електронских комуникација, Влада Републике Србије усвојила је „Стратегију развоја електронских комуникација у Републици Србији од 2010. до 2020. године“ („Службени гласник РС“, бр. 68/10).

„Електронске комуникације подразумевају свако емитовање, пренос или пријем порука (говор, звук, текст, слика или подаци) у виду сигнала, коришћењем жичних, радио, оптичких или других електромагнетских система“ („Службени гласник РС“, бр. 68/10). Сајбер терористи се углавном служе електронским комуникацијама због њихових бројних предности. Зато, иако се поменута „Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године“ („Службени гласник РС“, бр. 68/10) не односи директно на мере одбране и борбе против сајбер тероризма, њоме се уређује област електронских комуникација тако што се ограничава њихово коришћење, и на основу „Закона о електронским комуникацијама“ („Службени гласник РС“, бр. 44/10, 60/13 - одлука УС, 62/14 и 95/18 - др. закон) санкционише злоупотреба услуга електронских комуникација и телекомуникација. Према члану 137 „Закона о електронским комуникацијама“ („Службени гласник РС“, број 68/10) за прекршаје у области електронских комуникација предвиђена је новчана казна правном лицу у износу од 100.000 до 2.000.000 динара у зависности од прекршаја.

„Стратегијом развоја електронских комуникација у Републици Србији од 2010. до 2020. године“ („Службени гласник РС“, бр. 68/10) пројектован је оквир за примену нових технологија у области електронских комуникација како би се развио сектор индустрије у овој области, повећао индекс конкурентности Републике Србије

и пратио развој сервиса према предвиђеном моделу националне мреже електронских комуникација уз поштовање захтева за испуњење одређеног технолошког оквира којим су обухваћене: кабловске и бежичне мреже, конвергенција мрежа и сервиса, радиофренквенцијски спектар, енергетска ефикасност мрежа електронских комуникација, управљање радиофреквенцијским спектром, мреже које служе за емитовање радио и телевизијског програма (кабловска и дигитална телевизија) и размене отворених сервиса по отвореним мрежама електронских комуникација у Републици Србији („Службени гласник РС“, бр. 68/10).

Стратегија развоја индустрије информационих технологија за период од 2017. до 2020. године

Систематска подршка за јачање и развој индустрије информационих технологија у Републици Србији ствара подстицајан амбијент и представља шансу за привредни развој и економски раст наше земље. Отуда је Влада Републике Србије усвојила „Стратегију развоја индустрије информационих технологија за период од 2017. до 2020. године" („Службени гласник РС", бр. 95/16) с циљем да се искористе и унапреде производни и извозни капацитети српске индустрије софтвера, подстакне и подржи развој домаћих ИТ компанија, промовише српска индустрија информационих технологија и унапреди њен положај на светском тржишту. „Према подацима из студије „ИТ индустрија Србије, 2015 – 2017." у периоду од 2006. године српска ИТ индустрија значајно се развила. Данас у ИТ индустрији послује близу 2.000 предузећа (700 више него 2006. године), број запослених дуплиран је са 10.000 (2006) на 20.000, а дуплирани су и пословни приходи на преко 1,5 милијарду евра. Укупан сопствени капитал од 2006. године повећан је са 150 милиона на пола милијарде евра. Годишње се оснива преко 200 ИТ фирми" („Службени гласник РС", бр. 95/16). Из приложених података несумњиво можемо закључити да ИТ индустрија Србије бележи позитиван раст. Привредни субјекти чија област пословања се не односи директно на информационо - технолошку индустрију, такође су препознали савремени тренд развоја и примењују нове технологије у свом пословању, чиме се ствара позитиван амбијент и постиже боља конкурентност Републике Србије у области савремених технологија.

Стратегијом се пружају различите мере подршке у области информационих технологија за развој предузећа и пласирање производа кроз одређене *startup* пројекте, подстицајну пореску политику, модернизацију пословања привредних субјеката у свим привредним гранама, унапређење и јачање људских ресурса (континуирањим праћењем савремених иновација и начинима њихове примене, доквалификацијама и преквалификацијама кадрова) у области информационих технологија, планско развијање боље искористивости постојећих капацитета: технолошких паркова и центара, модернизацију индустрије информационих технологија и њено промовисање, пружањем одговарајућег унапређеног правног оквира у складу са савременим међународним прописима који погодују даљем развоју индустрије информационих технологија у Републици Србији.

Стратегија развоја мрежа нове генерације до 2023. године

Влада Републике Србије усвојила је 3.маја 2018. године „Стратегију развоја мрежа нове генерације до 2023. године" (Службени гланик РС, број 33 / 18) ради остварења одрживог технолошког развоја, остварења боље конкурентске позиције на тржишту кроз иновације, системске промене и инвестиције, продуктивну едукацију и запошљавање кадрова, повећање дигиталне писмености, јачање социјалне инклузије, усаглашавање са правним регулативама Европске Уније.

„Стратегија развоја мрежа нове генерације до 2023. године" („Службени гланик РС", бр. 33/18) предлаже развој „јединственог дигиталног тржишта заснованог на брзом и ултрабрзом интернету и интероперабилним операцијама" („Службени гласник РС", бр. 33/18) његову најширу примену у истраживачкој пракси, пословању, привреди и свакодневним потребама домаћинства ради превазилажења кризе, финансијске и економске на основу три темељна циља која су приказана у Табели 11. Поводом неговања добре комуникације са Европском Унијом и приближавања њеним стандардима и правним регулативама поменута „Стратегија развоја мрежа нове генерације до 2023. године" (Службени гланик РС, број 33 / 18) је у складу са стратегијом „Европа 2020: Стратегија за паметни, одржив инклузивни раст" (Крења, 2011) коју је 2010. године усвојила Европска Унија. Отуда је Република Србија усвојила иницијативу Европске Уније за стварање „јединственог дигиталног тржишта" (Службени гланик РС, број 33 / 18).

Табела 11. Циљеви јединственог дигиталног тржишта („Службени гласник РС“, бр. 33/18).

Јединствено дигитално тржиште		
Бољи приступ дигиталним добрима и сервисима	Окружење у коме дигиталне мреже и сервиси могу да се развијају	Дигитализација као покретач развоја
Правила прекограничне интернет продаје	Телекомуникациона правила	Јачање привреде која се темељи на дигиталним подацима
Побољшање прекограничне доставе пакета	Правила о аудиовизуелним медијима	Приоритети за норме и интероперабилност
Укидање „географског блокирања“	Процена улоге интернет платформи	Изградња јединственог дигиталног тржишта
Реформа европског закона и у ауторским правима	Борба против незаконитих интернет садржаја	
Смањење бирократије повезане са ПДВ-ом	Поступање личним подацима у дигиталним услугама	
	Јавно-приватно партнерство о сајбер сигурности	

Стратегија заштите података о личности

Све до пред крај 2008. године Република Србија је једна од ретких земаља у којој није постојао закон којим се уређује заштита података о личности. Зато је Влада Србије усвојила „Стратегију заштите података о личности“ („Службени гласник РС“, бр. 58/10) на основу „Закона о Влади“, члан 45. став 1 („Службени гласник РС“, бр. 55/05, 71/05 - исправка, 101/07 и 65/08).

Пре него што започне поступак прикупљања и обраде података о личности, руковалац података је дужан да у писменом облику о томе обавести лице на које се односе подаци о правном основу, сврси и начину коришћења података, његовим правима и др. Уколико не постоји основ у прописима, без пристанка лица обрада података о личности није могућа.

„Закон о заштити података о личности уређује и права и заштиту права лица чији се подаци обрађују. У вези са заштитом података о личности, лице чији се подаци обрађују, има следећа права: право на обавештење о обради, право на увид, право на копију и права поводом извршеног увида (под којим се подразумева да лице има право да од руковаоца захтева исправку, допуну, ажурирање, брисање података као и прекид и привремену обуставу обраде. Поступак остваривања ових права детаљно је уређен Законом“ („Службени гласник РС“, бр. 58/10, IV глава, став 2).

Да би се подаци о личности обрађивали на законит начин, неопходна је примена информационих технологија заштићених таквим мерама обезбеђења које омогућавају овлашћеном руковаоцу података да у било ком тренутку има приступ подацима, као што су: датум када су подаци обрађивани, мењани или коришћени од стране кога и по којој основи. Отуда савремене технологије имају значајну улогу у заштити података од злоупотребе. Приступ подацима није неограничен. Он се спроводи једино уз дозволу, односно правни основ за приступ подацима „на основу изричитих овлашћења за вођење одређених управних, судских или других поступака“ („Службени гласник РС“, бр. 58/10, IV глава, став 2)

„Стратегија заштите података о личности“ („Службени гласник РС“, бр. 58/10) индиректно представља један вид борбе против сајбер тероризма јер ставља под законски оквир „прикупљање, држање, обраду и коришћење података о личности“ којим се забрањује дискриминација у области података о личности и штите подаци сваког лица без обзира на: пол, расу, језик, држављанство, националну припадност, вероисповест, политичко уверење, социјални статус и

остала лична својства.

Међутим, како ранији „Закон о заштити података о личности“ („Службени гласник РС“, бр. 97/08, 104/09 - др. закон, 68/12-УС и 107/12) из 2008. године није садржао одговарајуће „прописе којима се уређује питање обраде података о личности које је веома заступљено у тим областима, као што су нпр. маркетинг, видео надзор, употреба биометријских података и др.“, и обзиром да правни оквир којим се уређује област заштите података о личности који датира из 2008. године није био усклађен са многим законима, подзаконским актима и прописима, Народна скупштина је усвојила нови „Закон о заштити података о личности“ („Службени гласник РС“, бр. 87/18) који је ступио на снагу 21. новембра 2018. године. Предвиђено је до 2020. године његово усклађивање са осталим законима и прописима у Републици Србији.

Новим „Законом о заштити података о личности“ („Службени гласник РС“, бр. 87/18) из 2018. године су обухваћени и посебни случајеви обраде података о личности, Члан 88 - 94:

„1) обрада и слободе изражавања и информисања;

2) обрада и слободан приступ информација од јавног значаја;

3) обрада јединственог матичног броја грађана;

4) обрада у области рада и запошљавања;

5) у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања, или у статистичке сврхе;

6) обрада од стране цркве и верских заједница;

7) обрада података о личности у хуманитарне сврхе од стране органа власти” („Службени гласник РС“, бр. 87/18).

За непоштовање права у овој области предвиђене су казнене мере. Сертификовано стручно тело за праћење и надзор је Повереник за информације од јавног значаја и заштиту података о личности, који је према члану 4, став бр. 22: „независан и самостални орган власти установљен на основу закона, који је надлежан за надзор над спровођењем овог закона и обављање других послова прописаних законом“ („Службени гласник РС“, бр. 87/18).

Стратегија развоја дигиталних вештина

Влада Републике Србије усвојила је 6. марта 2020. године „Стратегију развоја дигиталних вештина у РС за период 2020 - 2024“ („Службени гласник РС“, бр. 21/20) која представља „национални стратешки програм Владе којим се на целовит начин уређује развој дигиталних вештина становништва са циљем коришћења потенцијала савремених информационо - комуникационих технологија у правцу подизања квалитета живота свих грађана, веће запослености, ефикасности рада и економског раста друштва. Под дигиталним вештинама се подразумева поседовање одговарајућих знања, вештина и понашања у складу са потребама појединца и друштва у условима савременог брзог развоја ИКТ у 21. веку“ („Службени гласник РС“, бр. 21/20). Поменута Стратегија проистекла је из потребе да што већи број грађана поседује знања, вештине и способности које су потребне за употребу дигиталних уређаја (*desktop* рачунари, лаптопови, паметни телефони и слични уређаји) у циљу успешног проналажења, анализе, процене, стварања и преноса најразноврснијих информација у дигиталном формату.

Готово све јединице Дирекције полиције Министарства унутрашњих послова посредно обављају послове у вези са сузбијањем тероризма. Полиција као овлашћени државни орган за борбу против криминала иде у сусрет савременим облицима криминалних активности и има пред собом задатак суочавање са изазовима и претњама високотехнолошког криминала. Према „Закону о полицији“ („Службени гласник РС“, бр. 6/16, 24/18, 87/18), члану 11, тачка 5, Министарство унутрашњих послова Србије поред осталих послова надлежно је да: „обавља послове заштите и спасавања људи, материјалних и културних добара и животне средине од елементарних непогода, техничко - технолошких несрећа, удеса и катастрофа, последица тероризма, ратних и других већих несрећа“ („Службени гласник РС“, бр. 6/16, 24/18, 87/18). Припадници Управе криминалистичке полиције, пре свега Службе за борбу против тероризма и екстремизма су специјализовани за борбу против тероризма и екстремизма, подршку и међународну сарадњу у овој области.

Ефикасна борба против сајбер тероризма на националном нивоу захтева добру кооперативност свих органа унутрашњих послова и по вертикалној и по хоризонталној основи, али и добру полицијску сарадњу на регионалном и међународном нивоу. Поред тога неопходни су и стручна обученост кадрова, мобилност службе,

финансијско планирање и улагање у техничке и људске капацитете. Сајбер тероризам као криминални акт може да проузрукује веома тешке последице и по својој нехуманости превазилази бројне друге криминалне акте. Тим пре је потреба полиције за још чвршћом борбом против сајбер тероризма већа, зарад очувања реда и стабилности, живота и имовине недужних грађана од претњи сајбер тероризма.

Полиција и безбедносне службе за поступање у ситуацијама опасности од претњи кривичних дела тероризма и других сличних дела насиља, ангажују посебно организоване полицијске јединице за интервенцију у ванредним ситуацијама, које чине посебно обучена лица за вршење одређених полицијских задатака. Министарство унутрашњих послова Србије поседује Специјалну антитерористичку јединицу (САЈ).

Полицијски органи током криминалистичке обраде у циљу откривања и разјашњења кривичног дела и његових учинилаца спроводе разне криминалисатичко – тактичке радње и процедуре за прикупљање доказа. Оперативни рад подразумева примену адекватних криминалистичких метода с циљем супростављања криминалитету, како превентино тако и репресивно. Док, избор и примена метода зависе од садржаја учињеног кривичног дела, у овом случају дела сајбер тероризма. Оперативни рад има свој правни основ и одвија се уз поштовање законских и одговарајућих подзаконских прописа.

Шта подразумева оперативни рад, односно оперативна делатност? „Оперативна делатност почиње самоиницијативном делатношћу органа унутрашњих послова када: постоје основи сумње да је учињено кривично дело за које се гони по службеној дужности, а нема видљиве последице (кријумчарење, прикривање) и када је последица криминалне делатности манифестована јавно (убиства, крађа). Оперативна делатност може ићи: од потенцијалног или познатог учинилаца и од кривичног дела ка непознатом учиниоцу (по НН)“ (Водинелић, 1984, 53). Постоји више облика и фаза реализације оперативне делатности у зависности од своје садржине, времена предузимања начина реализације и резултата.

Два кључна проблема сајбер одбране су техничке и политичке природе. Полиција спороводи истражне радње једино када су за то испуњени законски услови, односно правни основ. Када се ради о најтежим кривичним делима против Уставног уређења и безбедности земље са елементом иностраности и високим степеном друштвене опасности, полиција користи посебне оперативне методе и средства на основу посебног прописа Министарства унутрашњих

послова Републике Србије који је предвиђен за такве ситуације. Служба државне безбедности (БИА) има значајну улогу у очувању Уставом утврђеног поретка. БИА као и полиција примењује истоветна или слична средства, методе и радње за прибављање, процену и проверавање информација о антиуставној делатности. Једина разлика је у делокругу рада, јер се бави делима која се у основи тичу политичког криминалитета и која углавном имају заједничких тачака са кривичним делима општег криминалитета, али их разликују мотиви извршења. Сврха оперативне делатности је благовремено откривање намера и циљева који теже да угрозе уставно уређење и безбедност земље и друге виталне државне интересе. Дакле, оперативна делатност се спроводи пре извршења кривичног дела, али и након што је оно извршено када се спроводи истражни поступак и прикупљање материјалних доказа у складу са криминалистичким правилима и процесним одредбама да би они били употребиви на суду. Међутим, „информације које прикупља обавештајно безбедносна служба применом оперативно техничких средстава и метода не представљају било какав доказ, али могу представљати основу за примену основних метода криминалистичке методике којима се обезбеђују ваљани докази у односу на конкретно кривично дело и учиниоца“ (Матијевић, 2002, 37). Обзиром да је сајбер тероризам специфично криминално дело потребно је прикупити што више доказа и информација о учињеном делу и његовом починиоцу. Јер, интернет саобраћај је тешко пратити због великог протока информација. Електронски надзор телекомуникација подразумева електронско прислушкивање телефонских разговора и праћење других начина комуникације, што се коси са поштовањем политике приватности.

Електронски надзор комуникација се спроводи превасходно због прикупљања релевантних доказа у судском поступку, за откривање мреже чланова терористичке организације, утврђивање хијерархије и целокупног криминалног деловања. Ову методу могу да примењују једино законски овлашћене особе, уз поштовање одређених начела. Спровођењу ових мера приступа се у случајевима када се истрагом није могло доћи до адекватних доказа, или када примена претходних мера није дала резултат, па се према тачно наведеном захтеву који садржи „чињенице, наведене околности под којима су искоришћене све методе које нису давале адекватан резултат, као и разлоге због којих се сматра да би примена метода тајног прислушкивања дала резултате. Захтев за прислушкивање треба да садржи и временски рок у којем ће се спроводити

надзор комуникације који може трајати до тридесет дана, који се спроводи на основу наредбе надлежног судије. Мера надзора може се продужавати на још тридесет дана у неколико наврата, такође уз сагласност надлежног судије“ (Weaver, Abramson & Bacigal, 2007, 564). Уколико околности које проистичу из терористичке активности то особито налажу, може се применити и тајни надзор лица чији идентитет није у потпуности утврђен, а која су повезана са најтежим злочинима, као и метод прикривеног иследника. Овај метод се ређе примењује због недовољно јасне правне регулативе и тешкоћа које произилазе из саме реализације планираних послова прикривеног иследника. Већина чланова терористичке организације је неповерљива према новопридошлицама, што додатно отежава продор до врха терористичке организације.

Тимски и синхронизовани рад и сарадња уз примену адекватних научних метода и достигнућа како природних и техничких наука, тако и друштвених (политикологије, социологије и психологије) су неопходни у расветљавању и доказивању сајбер тероризма. Држава је битан субјект у супростављању злоупотребе сајбер простора. Стратегијски приступ у супростављању сајбер тероризму омогућава адекватну превенцију и репресију, уз примену технолошких, правних, политичких, економских, социјалних и других мера које делују учинковито на борбу против сајбер тероризма.

Ефикасно супростављање претњама сајбер тероризма подразумева неколико фаза. Најпре је потребно да држава са свим надлежним органима и субјектима отклони услове који погодују настајању, развоју и спровођењу дела сајбер тероризма. Следећа фаза се односи на оперативну делатност, идентификацију претњи и предузимање техничких и криминалистичких радњи и мера са циљем откривања и разјашњавања конкретног кривичног дела. Ова фаза подразумева откривање учинилаца и обезбеђивање доказа за даље поступање. Рачунарско претраживање података је уведено 2006. године у наше процесно законодавство изменама и допунама „Законика о кривичном поступку“ („Службени гласник РС“, бр. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14 и 35/19, 27/21, 62/21) којим су прописани услови и начин спровођења рачунарског претраживања података. Претрагу тражених података спроводи овлашћен државни орган према опису података које је потребно рачунарски претражити и обрадити, у траженом обиму и времену трајања доказне радње. „Рачунарско претраживање података може трајати највише три месеца, а због неопходности даљег прикупљања доказа може се изузетно продужити још највише два пута у трајању од по три

месеца. Спровођење рачунарског претраживања података се прекида чим престану разлози за његову примену“ („Службени гласник РС“, бр. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14 и 35/19, 27/21, 62/21). Електронски докази се најчешће прибављају помоћу уређаја као што су: рачунарски системи, системи видео надзора, таблет - уређаји, дигитални апарати, уређаји за складиштење података (хард - дискови и SDD дискови, USB уређаји, меморијске картице, оптички компакт дискови и др.) и други. Поменути докази се такође прикупљају и уз помоћ обавештајних служби. На који начин обавештајне службе долазе до података? „Обавештајне службе долазе до података преко низа специфичних метода и поступака чија је заједничка карактеристика елеменат тајности у свим фазама и поступцима обавештајног рада. У својим активностима примењује скуп метода, радњи и поступака на основу којих обавештајна служба остварује своју функцију. Неке од тих метода су:

- метод тајног прикупљања података о терористима
- метод прикривеног прикупљања података
- метод легалног прикупљања података
- метод обавештајне делатности
-метод не обавештајне делатности обавештајних служби“ (Савић у: Пејановић & Бејатовић, 2009, 279 - 270).

Последња, завршна фаза подразумева прогон учинилаца и пресуду што је у надлежности тужилаштва и суда. Важни предуслови за ефикасно супростављање сајбер тероризму су стално праћење развоја науке и технологије, примена савремених изума и њихово прилагођавање постојећим расположивим криминалистичким методама.

Јавна тужилаштва као органи гоњења и судови као органи правосуђа имају значајну улогу у откривању и разјашњењу испољених облика сајбер тероризма. Табела 12. Приказује појединачни и збирни статистички приказ примљених кривичних пријава и извештаја у Посебном тужилаштву за високотехнолошки криминал у периоду од 2006. до 2016. године. Улога јавног тужилаца у фази криминалистичке обраде је нарочито важна. Посебно одељење за борбу против високотехнолошког криминала формирано је 2006. године при Вишем јавном тужилаштву у Београду према члану 5. „Закона о организацији и надлежности дрзавних органа за борбу против високотехнолоског криминала“ („Службени гласник РС“, бр. 61/05 и 104/09).

Табела 12. Појединачни и збирни статистички приказ примљених кривичних пријава и извештаја у Посебном тужилаштву за високотехнолошки криминал у периоду од 2006. до 2016. године (Стаменковић, Живановић, Пауновић & Стевановић, 2017, 12)

Година	Уписник КТ	Уписник КТР	Уписник КТН	Укупно
2006	19	/	/	19
2007	75	68	11	154
2008	110	60	14	184
2009	91	114	42	247
2010	116	443	13	572
2011	130	502	28	660
2012	114	609	65	788
2013	160	558	243	961
2014	294	770	352	1416
2015	198	1306	570	2074
2016	240	1237	580	2058
Укупно	1547	5667	1918	9132

Веома је тешко водити борбу против сајбер тероризма, јер надлежни субјекти морају да открију и разјасне тешко доказиве везе између учињеног сајбер напада и нападача. То потврђује тамна бројка и велики број неосуђених извршитеља сајбер напада. Како примећује Гудмен „жртве могу озбиљно да сумњају у способност полиције да се бави инцидентима компјутерског криминала ефикасно, правовремено и на поуздан начин“ (Goodman, 2001, 13), јер за спровођење закона у области сајбер безбедности често недостаје одговарајуће знање да би се држао корак са сајбер терористима (Gabrys, 2002).

Писарић наводи изазове са којим се суочава полиција у Србији поводом откривања дела високотехнолошког криминала:

- „неусклађеност правне регулативе са савременим облицима извршења кривичних дела;
- недовољна техничка опремљеност и оспособљеност полицијских службеника везана за откривање извршилаца у онлајн окружењу;
- недостатак операционалних обука које би омогућиле да полицијски службеници који се баве спречавањем високотехнолошког криминала буду довољно обучени и технички опремљени за вршење ових задатака;
- потешкоће у откривању извршилаца кривичних дела који користе лажне идентитете у онлајн окружењу, посебно када се у обзир узме чињеница да је у великом броју случајева

међународна полицијска сарадња лоша, а да у некима чак и не постоји;

- потешкоће у откривању тачне локације извршења кривичног дела, пошто се ова кривична дела врше са многих места широм света, а у великом броју случајева извршиоци кривичних дела користе мреже са јавним приступом“ (Писарић, 2016, 54).

Због тога је важно адекватно ангажовање свих надлежних субјеката, почев од ИТ администратора, корисника мреже све до надлежних субјеката у супротстављању сајбер тероризма још у фази постојања индиција, односно када се јављају прва упозорења и сметње на мрежи. Сарадња са другим државама на сузбијању сајбер тероризма је веома значајна, нарочито због проналажења и изручења терориста у складу са правилима међународне кривичноправне помоћи уз ангажовање Интерпола – међународне организације криминалистичке полиције „уз услов да се то односи само на оне терористичке акте који имају међународне имликације тј. да ангажовање интерпола подразумева борбу само против тероризма који има елементе иностраности“ (Бошковић & Јовичић, 2002, 59). Дакле, Интерпол је такође ангажован на спречавању и сузбијању свих облика сајбер тероризма. У септембру 2014. године, у Сингапуру је основан IGCI (*INTERPOL Global Complex for Innovation*), посебна организациона јединица Интерпола чији је основни циљ борба против компјутерског криминала, иновације и развој у области супротстављања рачунарском криминалитету. Тимови водећих ИТ стручњака из целог света данонoћно су ангажовани на превенцији рачунарског криминалитета, сарађују са националним полицијским службама, пружају им помоћ у вештачењу и истрагама, обавештавају их о могућим криминалним претњама.

Министарство унутрашњих послова Републике Србије сарађује са Европолом. Између Републике Србије и Европске полицијске организације потписан је 18. септембра 2008. године споразум, који је регулисан „Законом о потврђивању Споразума о оперативној и стратешкој сарадњи између Републике Србије и Европске полицијске канцеларије“ („Службени гласник РС“ – Међународни уговори, бр. 5/14). Основна сврха Споразума према члану 1. је унапређење сарадње „у спречавању и борби против организованог криминала, тероризма и других облика међународног криминала у областима криминала“ („Службени гласник РС“ – Међународни уговори, бр. 5/14). Еуропол посебну пажњу посвећује борби против сајбер криминала и од 2013. године формиран је посебно специјализован центар *European Cybercrime Centre (EC3)*.

Дужи временски период су рачунари и рачунски програми у употреби у нашој земљи. Рачунарски, односно високотехнолошки криминалитет, није новина на просторима Републике Србије. Према подацима Посебног одељења за високотехнолошки криминал Вишег јавног тужилаштва у Београду у периоду 2006. до 2013. године кривична дела ове врсте сваке године бележе раст (Стаменковић, Живановић, Пауновић & Стевановић, 2017, 12). Актуелна безбедносна ситуација захтева посвећеност и пуну пажњу као никада раније јер се инциденти и ризици повезани са сајбер нападима повећавају (Choo, 2011).

ЗАКЉУЧНА РАЗМАТРАЊА

Сагледавање савременог друштвено - политичког контекста упућује нас на чињеницу да сајбер тероризам представља континуирану претњу и изазов за националну и међународну безбедност. Јер, убрзан развој и растућа примена технологије, поред тога што несумњиво пружају бројне олакшице у свакодневном животу, такође остављају простора за разне злоупотребе и нове форме криминала и тероризма (сајбер тероризам) којима се служе одређене организације или појединци. Услед таквих околности сајбер злоупотребе представљају актуелне претње, а сајбер тероризам једну од најактуелних претњи у савременом друштву која прети да угрози виталне вредности поједине државе или међународни друштвени поредак. Намеће се потреба да се шира друштвена јавност боље упозна са овим друштвеним изазовом за чије разматрање је неопходан мултидисциплинаран приступ, док је за сузбијање сајбер тероризма неопходна свеобухватна реакција комплетног безбедносног сектора на националном и глобалном нивоу. Имајући у виду комплексност сајбер тероризма као безбедносног феномена, значајно је увидети да су последице његовог деловања на државу и друштво у целини веома изражене и да могу бити потенцијално веома разорне како у политичкој, социјеталној, тако и економској и безбедносној сфери.

Развој и примена информационе и комуникационе технологије значајно су изменили свакодневни живот људи, као и функционисање основних друштвених структура чији рад значајно зависи од технологије, што поменуте структуре чини рањивим на нове врсте претњи из сајбер простора. Технолошки напредак је мултипликатор друштвеног развоја, али подразумева и одређене ризике. На глобалном нивоу нису од старта препознате претње од сајбер тероризма и сајбер криминала, стога технолошки развој, његову експанзију и доступност високотехнолошких изума по комерцијалним ценама на слободном тржишту није пратила адекватна реформа безбедносног система, што је омогућило терористима да користе предности и рањивости савремене технологије у различите сврхе. Отуда се безбедност информационих и комуникационих технологија намеће као једно од најзначајнијих питања данашњице, док истовремено сајбер безбедност постаје један од најзначајнијих елемената савремене безбедности у друштву.

Процеси (глобализација, научно - технолошка револуција, пандемија, миграције, климатска и енергетска криза, економска криза) који обликују садашњост подстичу ширење терористичких

аспирација путем интернета. Глобализација због своје контрадикторности, пораста богаства и стандарда са једне стране уз истовремени пораст социјалне тензије и сиромаштва са друге стране представља неисцрпан извор за регрутовање нових чланова терористичких и других криминалних организација. Све већи број организованих криминалних група користи терористичке тактике.

Глобализација је омогућила тешње зближавање, повезаност између организованог криминала и тероризма који су попримили као никада раније глобалну димензију. Неретко је тероризам спонзорисан од стране појединих држава, што додатно компликује ситуацију на макро нивоу друштвене стварности. На индивидуалном плану научно - технолошка револуција изнедрила је нове врсте друштвених форми, као што су виртуелне заједнице и сајбер култура. Друштвене мреже постале су значајан елемент у одржавању социјалних веза и комуникације са другима, нарочито за време пандемије када су ограничени услови путовања и кретања. Сајбер простор постаје арена сусрета онлајн идентитета, информација, виртуелних заједница, сајбер културе, криминалних активности, па чак и сајбер ратовања. Иако последице из онлајн окружења значајно утичу на дешавања у реалном (физичком) простору, поменуте сајбер активности не могу да замене чулну пуноћу, што може да има негативне психолошке и бихејвиоралне последице. Тако с једне стране настају негативни ефекти на личном (индивидуалном) нивоу, као што су: криза идентитета, алијенација (отуђење), вандализам, насиље, зависност од ИКТ и др. Глобални проблеми с друге стране, као што су: миграције, климатске промене, енергетска криза, економска криза и сиромаштво само додатно распирују тензије. Поменуте тензије се са глобалног нивоа преливају на регионални, а потом и национални ниво. Не смемо изузети значај који појединац (индивидуа) има као друштвено - политички актер. Савремене информационе и комуникационе технологије пружају могућност свакоме без обзира на порекло, родну и класну припадност, године старости, економски, политички и културни статус да приступи глобалној онлајн заједници, размењује информације и „утиче“ на глобална дешавања.

Садашњу ситуацију одликује криза, која представља погодно тло за развој сајбер терористичких аспирација и других злоупотреба на интернету. Услед настојања да се што ефикасније заштити, кривично гони и санкционише дела тероризма, Србија је ратификовала бројне конвенције и усвојила је многа међународна документа која се баве борбом против сајбер тероризма, али и тероризмом у општем смислу.

Тероризам је неретко актуелна тема у многим политичким и научним расправама. Међународна заједница улаже велике напоре да пронађе решење за проблеме тероризма и све његове појавне облике. То потврђује велики број састанака и конференција на поменуту тему, резолуција и усвојених докумената који су обликовали безбедносне политике на међународном, регионалном и националном нивоу.

Република Србија има развијен и модеран антитерористички национални систем, чији су институционални капацитети један од подсистема унутар националног система Републике Србије. Национални систем за супростављање тероризму постоји од када постоји и тероризам на подручју наше земље, карактеришу га динамичност и константно усвршавање и реорганизовање с циљем превенције и што ефикаснијег суочавања са делима тероризма. Влада Републике Србије је препознала претње које произилазе из сајбер простора и нормативно - правно их регулисала. Дакле, Србија је несумњиво показала своју посвећност у супростављању сајбер тероризму. Ефикасно супростављање сајбер тероризму захтева: 1. континуирано праћење његовог развоја, 2. идентификацију свих његових појавних облика, 3. избор адекватних превентивних и репресивних метода, 4. организован тимски и стручан рад, 5. размену искуства, информација и најбољих пракси на међународном, регионалном нивоу, 6. међусобну сарадњу државних органа (полицијских, правосудних и других) који су задужени за откривање, надзор и контролу на националном нивоу, 7. укључивање приватног сектора у супростављање сајбер тероризму, 8. сарадњу државног (јавног сектора) са организацијама које послују и раде у ИТ индустрији (приватни сектор), 9. боља информисаност и едукација грађана о постојећим претњама, 10. систематичност, планирање и улагања, 11. примена научних и практичних метода, адекватно коришћење технолошких достигнућа, 12. мултидисциплинарност. Република Србија је усвојила неколико стратегијских докумената који су непосредно или посредно посвећени проблему сајбер тероризам и који постављају нове антитерористичке темеље на основу сопствених и иностраних искустава. Међутим, иако Република Србија има свеобухватан стратегијско - политички приступ заштите, превенције и кривичног сузбијања дела тероризма неопходна је „стална будност“ континуирани развој, иновације, односно примена претходно поменутих дванаест препорука за ефикасно сузбијање сајбер тероризма.

СПИСАК ТАБЕЛА И СЛИКА

Табеле

Слике

ИНДЕКС ПОЈМОВА

ЛИТЕРАТУРА

Научни и стручни текстови, монографије и зборници радова

Abadinsky у: Шкулић, М. (2003). Организовани криминалитет. Појам и кривично процесни аспекти, Београд: Досије.

Abadinsky, H. (1994). *Organized Crime*, Chicago: Nelson- Hall Publishers.

Abrahamson, P. (1995). Social Exclusion in Europe: Old Wine in New Bottles? *Družboslovne razprave* 11(19–20), 119–136.

Abrams, M., Podell H., Jajodia S. (1995). *Information Security: An Integrated Collection of Essays*, Los Alamitos, CA USA: Computer Society Press, 117.

Akhgar, B., Staniforth A. & Bosco F. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*, USA: Elsevier Inc.

Albrow, M. (1996). *The Global Age: State and Society Beyond Modernity*. Cambridge: Polity Press.

Alqahtani, S. H. (2016). Latest Trends and Future Directions of Cyber Security Information Systems. *Journal of Information Engineering and Applications* 6 (11), 9-14.

Appadurai, A. (2000). Grassroots Globalization and the Research Imagination. *Public Culture* 12 (1), 1-19 .

Arnett, J.J. (2002). The psychology of globalization. *American Psychologist*, Vol. 57, 774-783.

Ashley, K. B. (2003). *Anatomy of cyber terrorism: Is America vulnerable?* USA: Air University, Maxwell AFB, AL.

Auwema, N.M. (2015). *The Discourse of Cyberterrorism:Exceptional measures call for the framing of exceptional times*, Thesis MSc Political Science.

Bamberg, M. (2011). Who am I? Narration and its contribution to self and identity. *Theory and Psychology* 21(1), 3-24.

Baruch, Y. (2000). Teleworking: Benefits and Pitfalls as Perceived by Professionals and Managers. *New Technology, Work and Employment*, Vol. 15, 34–49.

Bauman, Z. (1998). *Globalization: the human consequences*. New York, Columbia University Press.

Beaulac, S. (2004). The Westphalian model in defining international law: challenging the myth. *Australian Journal of Legal History* Vol. 7, 181–213.

Beggs, C & Butler, M. (2004). *Developing New Strategies to Combat Cyber-Terrorism*, Idea Group Publishing.

Belenky, A. & Ansari, N. (2003). IP Traceback with Deterministic Packet Marking. *IEEE Communications Letters,* Vol. 7, No. 4.

Bianchi, A. (2011). Terrorism and Armed Conflict: Insights from a Law & Literature Perspective. *Leiden Journal of International Law* 24 (1), 1–21.

Bishop, M. (1995). *A taxonomy of UNIX system and network vulnerabilities*. Technical report CSE 95/10. University of California at Davis: Department of Computer Science.

Bobbitt, P. (2008). *Terror and Consent: The Wars for the Twenty-First Century*. New York: Anchor Books.

Boebert, W. E. (2010). A Survey of Challenges in Attribution. *Proceedings of a workshop on Deterring CyberAttacks*, *Informing Strategies and Developing Options for U.S. Policy*, Washington DC: National Academy of Sciences.

Bollen, J., Mao H. & Zeng, X. (2011). Twitter mood predicts the stock market. *Journal of Computational Science* 2 (1), 1–8.

Boon, S. & Sinclair, C. (2009). A world I don't inhabit: disquiet and identity in Second Life and Facebook. *Educational Media International* 46 (2), 99–110.

Bossler, A.M. & Holt, T.J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management* 35 (1), 165-181.

Brenner, S. W. (2007). At Light Speed, *The Journal of Criminal Law and Criminology*, Vol. 97, No. 2, 379-475.

Britz, M. T. (2013). *Computer Forensics and Cyber Crime – An Introduction*, Prentice Hal, 3th edition.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime, *Policing: An International Journal of Police Strategies and Management* 2, 408-433.

Bryant R. & Stephens, P. (2014). Policing Digital Crime: the International and Organisational Context. In: Bryant R.& Bryant S. (eds.)(2014). *Policing Digital Crime* (111-123). Surrey: Ashgate Publishing Limited.

Burrows, M. & Engelke P. (2020). *What World POST-COVID-19? Three Scenarios*, Atlantic Council: Scowcroft Center for Strategy and Security.

Carr J. (2010). *Inside Cyber Warfare*, Sebastopol: Reilly Media.

Carter, D., Schwartz, N.& Norris, F. (2008, 6. oktobar). *Financial crises spread in Europe*, New York Times.

Chak, K. & Leung, L. (2004) Shyness and locus of control as predictors of internet addiction and internet use. *CyberPsychology & Behavior* 5, 559-570.

Chandan, K. S. (1935). *Le terrorisme devant la Societe des Nations*, Paris.

Cheng, Y. Y. (2010). *Social psychology of globalization: Joint activation of cultures and reactions to foreign cultural influence*. University of Illinois at Urbana-Champaign: PhD Dissertation.

Chiu, C.Y., Gries, P., Torelli, C. J. & Cheng, S. Y.Y. (2011). Toward a social psychology of globalization. *Journal of Social Issues* 67, 663–676.

Clarke R. & Knake R. (2010). *Cyber War – The next treat to National Security and What to do about it*, Harper Collins Publisher.

Cohen, F. (1997). Information system attacks: a preliminary classification scheme. *Computer & Security* 16 (1), 29-46.

Collin, B. (1997).The Future of Cyberterrorism, *Crime and Justice International* 13(2),15-18.

Condorelli, L. & Naqvi, Y. (2004). The War Against Terrorism and Jus in Bello: Are the Geneva Conventions Out of" Date? In: Bianchi A. & Naqvi Y. (eds.) (2004) *Enforcing International Law Norms Against Terrorism* (25-37). Oxford ; Portland, Or. : Hart.

Correia, M. & Bowling, C. (1999). Veering toward digital disorder: computer-related crime and law enforcement preparedness. *Police Quarterly* 2 (2), 225-244.

Cottim, A. (2010). Cibercrime, cyberterrorism and jurisdiction: an analysisof article 22 of the COE convention of cybercrime. *European Journal of Legal Studies* 2 (3), European University Institute: San Dominico de Fiesole, Italy.

Cronin A.C. (2009). Behind the Curve, Globalization and International Terrorism. In: Howard, D. R., Sawyer, L.R & Bajema, E.N. (eds.), *Terrorism and Counter Terrorism, Readings and Interpretations* (30-58). Boston: Higher education.

Davis, T. J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component, *Policing: An International Journal of Police Strategies & Management* 35 (2), 272-284.

Deardorff, A. & Stern, R. (2001). What you should know about globalization and the world trade organization? *Review of International Economics*, 403-427.

Della Porta D. (2012). Communication in movement: Social movements as agents of participatory democracy. In: Loader B. & Mercea D. (eds) *Social Media and Democracy: Innovations in Participatory*

Politics (39–55). London: Routledge.
Denning, D. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy. In: Arquilla, J. & Ronfeldt, D. (eds.) (2001) *Networks and Netwars. The Future of Terror, Crime, and Militancy* (239-288). RAND Corporation.
Denning, D. (2014). Framework and Principles for Active Cyber Defense. *Computers & Security*, Vol. 40, 108-113.
Dogrul, M., Aslan A. & Celik E. (2011). *Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*, Turkey: Turkish Air War College Istranbul.
Dollar, D. & Kraay, A. (2001). *Trade, Growth and Poverty*. Washington: The World Bank, Development Research Group.
Dreher, A., Gassebner M. & Siemers, L. H. (2010). Does Terrorism Threaten Human Rights? *The Journal of Law & Economics* 53 (1), 88.
Duggan, P. (2015). Harnessing cyber-technology's human potential, *Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School*, Vol. 28, Iss. 4, p. 15.
Dunn-Cavelty, M. (2008). *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age.* New York: Routledge, Print.
Everett, A. (2004). On cyberfeminisms and cyberwomanism: High-tech mediations of feminism's discontents. *Signs: Journal of Women in Culture and Society* 30(1), 1278–1285.
Farwell, J.P. & Rohozinski, R. (2012). The New Reality of Cyber War,*Survival* 54 (4), 107–120.
Ferreira, F. (1999). *Inequality and Economic Performance*. Washington: World Bank.
Fidler, P. D, Pregent, R & Vandurme, A. (2013). Nato, Cyber Defense, and International Law, *ST. John's Journal of International & Law* 4 (1), 1-25.
Flaxner S. B. (1987). *The Random Hause Dictionary of the English language*, New York: Random House.
Frances, S. (2004). Development and security, *Conflict, Security and Development* 4(3), 261-288.
Friedman, T. L. (1999). *The Lexus and the Olive Tree*, US: Farrar, Straus and Giroux.
Fu, H.-Y., & Chiu, C. -Y. (2007). Local culture's responses to globalization: Exemplary persons and their attendant values. *Journal of Cross-Cultural Psychology*, Vol. 38, 636–653.
Geer, E. Daniel Jr. (2006). The Physics of Digital Law: Searching for Counterintuitive Analogies. In: Balkin, J. M., Grimmelmann J.,

Katz E., Kozlovski N.,Wagman S., Zarsky T., (Eds.), *Cybercrime*: *Digital Cops in a Networked Environment* (13-36). New York University Press.

Gilpin R. (2001). *Global Political Economy: Understanding the International Economic Order*, Princeton University Press.

Giraldo, J. & Trinkunas, H. (2010). *Terrorism Financing and State Responses: A Comparative Perspective*. Redwood: Stanford University Press.

Goodman, M. (2001). *Making computer crime count*. FBI Law Enforcement Bulletin, 70 (8), 10-17.

Goodman, S. E. (2007). Cyberterrorism and Security Measures. In: National Academy of Sciences, R. Narasimha, A. Kumar, S. P. Cohen & R. Guenther (Eds.), *Science and Technology to CounterTerrorism. The Proceedingsof an Indo – U.S Workshop* (43-54), Washington DC: The National Academy Press.

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology* 2 (1), 13–20.

Grabosky, P. (2007). *Electronic Crime*, New Jersey: Pearson Prentice Hall.

Gray, J. (1998). *False Dawn. The Delusions of Global Capitalism*, New York Press.

Greitzer F.L. & Ferrymann T.A. (2013). Methods and metrics for evaluating analytic insider treat tools. In: *Proccedings of the 2013 IEE security and privacy workshops (SPW'13)*, (90-97). California, USA: IEE.

Hafner, K. (1998). Where Wizards Stay Up Late: The Origins of the Internet, New York: Simon & Schuster.

Hagan, E. F. (2010). *Crime Types and Criminals*. Thousand Oaks, California: SAGE Publications.

Halfond, W., Viegas, J, Orso, A. (2006). A Classification of SQL Injection Attacks and Countermeasures, *IEEE International Symposium on Secure Software Engineering*, The Institute of Electrical and Electronics Engineers.

Hapa, J. and Fairclough, G. (2017). „A Model to Facilitate Discussions about Cyber Attacks". In: M. Taddeo, L. Glorioso (eds.), *Ethics and Policies for Cyber Operations*. Philosophical Studies Series 124, Springer International Publishing Switzerland, 169-185.

Harmon, C.C. (2000). *Terorrism today*, London; Portland, OR: Frank Cass.

Hathaway, A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue W., Spiegel, J. (2012). The Law of Cyber-Attack. *California Law*

Review 100 (4), 817-885.
Hengsbach, F. (1997). Ein neuer Gesellschaftsvertrag in Zeiten der Globalisierung. In: Fricke, W. (Ed.), *Jahrbuch Arbeit und Technik* (182–195), Dietz: Bonn.
Holm, H., Ekstedt, M &Andersson, D. (2012). Empirical analysis of system-level vulnerability metrics through actual attacks, *Transactions on Dependable and Secure Computing* 9 (6), 825–837.
Iasiello, E. (2013). *Cyber Attack: A Dull Tool to Shape Foreign Policy*, Tallinn: NATO CCD COE Publications.
Janczewski L. & Colarik, A. (2008). *Cyber Warfare and Cyber Terrorism*, Hersey (USA): IGI Global.
Jones, A. L. & Howard- Hassmann, R. E. (2005). Under Strain: Human Rights and International Law in the Post 9/11 Era, *Journal of Human Rights*, Vol. 4, 61–71.
Kacerguis, M. & Adams, G. (1979). Erickson stage resolution: The relationship between identity and intimacy. *Journal of Youth and Adolescence* 9(2), 117-126.
Kahn R. & Kellner, D. (2004). New media and internet activism: From the Battle of Seattle to blogging. *New Media and Society* 6(1), 87–94.
Kandias, M., Stavrou V, Božović N., Mitrou L., Gritzalis, D. (2013). Predicting the insider threat via social media: the YouTube case, In: *Proccedings of the 12th ACM Workshop on privacy in the electronic society* (261-266), Berlin: ACM Press.
Katz, C. (2004). *Growing up global: economic restructuring and children's everyday lives*. Minneapolis, MN: University of Minnesota Press.
Kaul, I. (1994). *Human security: The need for a new security council. Roundtable on Global Change. Change: Social Conflict or Harmony?* United Nations Development Programme (UNDP), Stockholm, Sweden. Participant Paper no. 32 (22–24 July).
Kegley, C. W. Jr. (2003). *The New Global Terrorism: Characteristics, Cause, Control*, New Jersey: Prentice Hall.
Keith, J, Bejtlich, R. & Rose, C. (2008). *Real Digital Forensics*, New Jersey: AddisonWesley.
Khamis, S. (2015). Gendering the Arab Spring: Arab women journalists/ activists, cyber-feminism and the socio-political revolution. In: Carter C, Steiner L and McLaughlin L (Eds.) *The Routledge Companion to Media and Gender* (565–575), London: Routledge.
Kizza J. (2009). *Guide to Computer Network Security*, London: Springer.
Lechner, J. F. & Boli, J. (2003). *The Globalization Reader*. Maiden: Mass.
Lemkin, R. (1933). Faut il un nouveau délit de droit gens nomme

terrorisme, *Revue de droit penal et criminologie, Belge*, no. 13, 900–901.

Li, H., Squire, L. & Zou, H. (1998). Explaining International and Intertemporal Variations in Income Inequality. *The Economic Journal* Vol. 108, 26-43.

Li, Q. (2005). Does democracy promote or reduce transnational terrorist incidents? *Journal of Conflict Resolution* 49 (2), p. 278 - 97.

Liem, A., C. Wang, Y. Wariyanti, C.A. Latkin & B.J. Hall (2020). The neglected health of international migrant workers in the COVID-19 epidemic. *The Lancet Psychiatry* 7 (4). doi: 10.1016/S2215-0366(20)30076-6

Luknar, I. (2018). Terrorism and human rights. In: M Gjurovski (Ed.), *Security System Reforms as Precondition for Euro-Atlantic Integrations. Vol. 2. International scientific conference Ohrid* (p. 94-99). Skopje: Faculty of security.

Luknar, I. (2020a). Cyber Terrorism Threat and the Pandemic. In: Cane T. Mojanoski (Ed. in chief), *The Euro-Atlantic values in the Balkan countries*, Vol. 3 (p. 29-38). Bitola: University "St. Kliment Ohridski", Skopje: Faculty of Security.

Luknar, I. (2020b). Cybercrime – Emerging Issue. In: S. Jaćimovski (ed.), *Archibald Reiss Days. Vol. 10. International scientific conference* (621-628). Beograd: Kriminalističko-policijski univerzitet.

Luknar, I. (2021). „Social implications of the Internet in new reality due to COVID-19", *Српска политичка мисао*, Вол. 72, Бр. 2, 225-235.

Luknar, I. (2022b). Social control theory and cibercrime issue. *Национални интерес*, Бр.1, (прихваћено за објављивање).

Lundberg, M. & Squire, L. (2000). *The Simultaneous Evolution of Growth and Inequality*. World Bank Working Paper.

Lutz M. J. & Brenda J. L. (2004). *Global Terrorism*, Routledge.

Mahoney, J. (2000). Path Dependence in Historical Sociology. *Theory and Society*, 29(4), 507-548.

Manap., N.A., & Tehrani, P. M. (2012). Cyber Terrorism: Issues in Its Interpretation and Enforcement. *International Journal of Information and Electronics Engineering*, 2(3), 409-413.

Matijašević-Obradović, J. (2014). The Significance and modalities of internet abuse as the primary global communicat. computer networks in cyberspace. *Megatrend revija* 11(1), 279-298.

Mattdort, J. H. & Whitman, E.M. (2011). *Roadmap to Information Security*, USA, Boston: Course Technology.

Merton, R.K. (1957). *Social theory and social structure*, Glencoe, Ill. : Free Press.

Miller, C., Matusitz, J., O'Hair, D., & Eckstein, J. (2008). The complexity of terrorism: Groups, semiotics, and the media. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and retorical perspectives*. Cresskill, NJ: Hampton Press.

Mittelman, H. J. (2000). *The Globalization Syndrome: Transformation and Resistance*, Princeton University Press.

Moore, D. & Rid, T. (2016). Cryptopolitik and the Darknet, *Global Politics and Strategy*, Vol.58, No.1, 7-38.

Morris, M. W., Mok, A. & Mor, S. (2011). Cultural identity threat: The role of cultural identifications in moderating closure responses to foreign cultural inflow. *Journal of Social Issues*, Vol. 67, 760–773.

Munkhdorj, B. & Yuji S. (2017). Cyber attack prediction using social data analysis, *Journal of High Speed Networks* 23 (2), 109–135.

Murthy, D. (2012). Towards a Sociological Understanding of Social Media: Theorizing Twitter, *Sociology* 46(6), 1059 –1073.

Nagar, R, Lawson, V, Mc Dowell & Hanson, S. (2002). Locating globalization: feminist (re)readings of the subjects and spaces of globalization. *Economic Geography*, 78 (3), 257–284.

Neeraj (2001). *Globalisation or Recolonisation*, ELGAR: Pune.

Nguyen, R. (2013). „Jus Ad Bellum" in the Age of Cyber Warfare, *California Law Review* 101 (4), 1079-1129.

Nicholas N. (2007). *The Black Swon – The Impact of the Highly Improbable*, New York : Random House.

Ning, H., Liu, H., Ma, J., Yang, T. L. & Huang, R. (2016). Cybermatics: Cyber-physical-social-thinking hyperspace based science and technology. *Future Generation Computer Systems* Vol. 56, 504-522.

Norasakkunkit, V. & Uchida, Y. (2011). Psychological consequences of postindustrial anomie on self and motivation among Japanese youth. *Journal of Social Issues* Vol. 67, 774–786.

Norris, P. (2011). *Democratic Deficit. Critical Citizens Revisited*. Cambridge: Cambridge University Press.

O'Harrow, R. Jr. (2005). *No Place to Hide*, New York: Free Press.

Olsen, M. (1969). Two Categories of Political Alienation. *Social Forces* Vol. 47, 288-299.

Orman, H. (2003). The Morris Worm: A Fifteen-Year Perspective, *IEEE Security & Privacy* 1 (5), 35-43.

Palazzi, E. (1965). *Dizionario della lingua italiana*, Milano: Garzanti.

Paletz, L. D. & Schmid P. A. (1992). *Terrorism and the Media*, Sage Publications: Newbury Park.

Pauwels, T. (2014). *Populism in Western Europe: Comparing Belgium,*

Germany and the Netherlands. London: Routledge.
Payne B. K., & Walton, C. D. (2002). Deterrence in the Post-Cold War World. In: John Baylis, James Wirtz, Eliot Cohen, and Gray Colin (Eds.), *Strategy in the Contemporary World, An Introduction to Strategic Studies*, Oxford: Oxford University Press.
Piazza, J.A. & Walsh, J.I. (2010). Terrorism and Human Rights: Editors' Introduction. *Political Science and Politics* 43 (3), 407-409.
Piketty, T. (2015). *Kapital u dvadesetprvom veku*, Sarajevo: Buybook.
Pipyros K., Thraskias C., Mitrou L., Gritzalis D., Apostolopoulos T. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, *Computers & Security* Vol. 74, 371-383.
Robertson, R. (1992). *Globalization: Social theory and global culture*. London: Sage Publications Ltd.
Sassen, S. (2002). Towards a sociology of information technology. *Current Sociology* 50(3), 365–385.
Savona, E.U., Adamoli, S., Di Nicola A. & Zoffi, P. (1998). *Organized Crime Around the World*, No. 31, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI).
Schjolberg, S. (2014). *The History of Cybercrime: 1976-2014*, Koln.
Schmid, A. (1996). The links between transnational organized crime and terrorist crimes. *Transnational Organized Crime* 2(4), 40-82.
Schmid, A., Jongman A. (2005). *Political Terrorism*. Piscataway, NJ: Transaction Publishers.
Schmitt, N. M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press.
Schuster, J. (2013). Invisible feminists? Social media and young women's political participation. *Political Science* 65(1), 8–24.
Selley, L. (2003). Organized Crime, Terrorism and Cybercrime. In: Alan Bryden, Philipp Fluri (eds.) *Security Sector Reform: Institutions, Society and Good Governance* (303-312). Nomos Verlagsgesellschaft: Baden-Baden.
Sennett, R. (1998). *The Corrosion of Character. The Personal Consequences of Work in the New Capitalism*. W. W. Norton & Company, New York/London.
Shelley, L. I. & Melzer, S., A. (2008). The Nexus of Organized Crime and Terrorism: Two Case Studies in Cigarette Smuggling, *International Journal of Comparative and Applied Criminal Justice* 32 (1), 1-21.

Shinder, L. D. (2002). *Scene of the Cybercrime: Computer Forensics*

Handbook. USA; Rockland, MA: Syngress Publishing Inc.
Sieber, U. (1994). *Information Technology Crime – National Legislations and International Initiatives*, Köln: Carl Heymanns Verlag.
Silvey, R. (2009). Development and geography: anxious times, anemic geographies and migration, *Progress in Human Geography*, 33(4), 507–515.
Sinai, J. (2011). Terrorism on the Internet and Effective Countermeasures, *The Intelligencer: Journal of U.S. Intelligence Studies* Vol. 18, 21–24.
Sklair, L. (2013). *Globalization. Capitalism and its Alternatives*. Oxford University Press.
Sofaer, A. D. (2010). *The Best Defense? Legitimacy and Preventive Force*, Stanford, CA: Hoover Institution Press.
Solange G.H. (2009). *Cybersecurity Guide for Developing Countries*, Geneva: International Telecommunication Unione.
Sommestad, T. (2012). *A framework and theory for cyber security assessments*. Doctoral dissertation, Stockholm, Sweden: KTH, Royal Institute of Technology.
Stallings, W. & Brown L. (2015). *Computer security : principles and practice*, Harlow : Pearson Education Limited.
Stavrou V, Kandias, M., Karoulas G., Gritzalis, D. (2014). Business process modeling for insider threat monitoring and handling. In: *Proccedings of the 11th international conference on trust, privacy &security in digital business* (119-131). Germany: Springer.
Stoll, C. (2005). *The Cuckoo's Egg*, New York: Gallery Books.
Stytz, M. (2006). Cyberwarfare Distributed Training, *Military Technology* (MILTECH) Vol. 11, 95-96.
Talbot, J. & Welsh D. (2006). *Complexity and Cryptography: an introduction*, Cambridge: Cambridge University Press.
Tavani H. T. (2003). *Ethics and Technology: Ethical Issues in an Age of Information and Communications Technology*, Hoboken, John Wiley & Sons Inc.
Todd, E. (2003). *After the Empire: The Breakdown of the American Order,* New York: Columbia University Press.
Tomlinson, John (1999): *Globalization and Culture*, Cambridge: Polity Press.
Tong, Y. -Y., Hui, P. P. -Z., Kwan, L. & Peng, S. (2011). National feelings or rational dealings? The role of procedural priming on the perceptions of cross-border acquisitions. *Journal of Social Issues* 67, 743–759.
Tonhauser, M. & Ristvej, J. (2019). Disruptive acts in cyberspace, steps

to improve cyber resilience at National Level, *Transportation Research Procedia* 40, 1591–1596. https://doi.org/10.1016/j.trpro.2019.07.220

Townsend, P. (1979). *Poverty in the United Kingdom*. Harmondsworth: Penguin Books.

Townsend, P. (1987). Deprivation. *Journal of Social Policy,* 16(2), 125–146.

Trager F. R & Zagorcheva, P. D. (2005-2006). Deterring Terrorism, *International Security* 30 (3), 87-123.

Tsakloglou, P. & Papadopoulos, F. (2002). Aggregate Level and Determining Factors of Social Exclusion u Twelve European Countries, *Journal of European Social Policy* 12(3), 211–225.

United Nations Environment Programme (2021). *Emissions Gap Report 2021: The Heat Is On – A World of Climate Promises Not Yet Delivered*. Nairobi.

Vandemoortele, J. (2002). *Are we really reducing global poverty*. New York: UNDP.

Vernotte, A., Dadeau, F., Lebeau, F., Legeard, B., Peureux, F. & Piat, F. (2014). Efficient Detection of Multi-step Cross-Site Scripting Vulnerabilities, *10th International Conference on Information Security Systems*, Indija: ICISS 2014.

Vidanage, H. R. (2006). *Apparition of the predator*. The Lanka Academic, 6 (281), p. 3.

Wagner, R. Abraham (2005). Terrorism and the Internet: Use and Abuse. In: *Fighting Terror in Cyberspace, Terrorism and the internet*; (Eds.) Mark Last, Abraham Kandel, World Scientific.

Wagner-Pacifici, R. & Hall, M. (2012). Resolution of Social Conflict. *Annual Review of Sociology* Vol. 38, 181-199.

Walsh E. L. (1997). *Firewall : the Iran-contra conspiracy and cover-up*, New York: W. W. Norton & Company.

Walsh, J. I. (2007). Do States Play Signaling Games? *Cooperation and Conflict: Journal of the Nordic International Studies Association* 42 (4), 441.

Weaver, L.R., Abramson, W.L. & Bacigal, R. (2007). *Criminal Procedure, cases, Problem and Exercises*, USA: Gale Cengage.

Weimann, G. (2006). *Terror on the Internet: Tne New Arena, The New Challenges*, Washington: United States Institute of Peace Press.

Weimann, G. (2015). *Terrorism in Cyberspace. The Next Generation*, New York: Columbia University Press.

Weinstock N. N. (2000). Cyberspace self-Governance, *California Law*

Review Vol. 88.
Wenger, E., McDermott, R., & Snyder, W. M. (2002). *Cultivating communities of practice*. Boston: Harvard Business School Press.
Williams, K. (2008). Using Tittle's control balance theory to understand computer crime and deviance, *International Review of Law Computers & Technology* 22 (1-2), 145-155.
Wong, P. T (2011). *Active cyber defense: enhancing national cyber defense*, Calhoun: The NPS Institutional.
Yang, D. Y-J., Chen, X., Cheng, S. Y. Y., Kwan, L., Tam, K. -P., & Yeh, K. -H.(2011). The lay psychology of globalization and its social impact. *Journal of Social Issues* Vol. 67, 677–695.
Yeates, N. (2001). *Globalization and Social Policy*, London: SAGE Publications.
Yergin, D. & Stanislaw, J. (2002). *The Commanding Heights: The Battle for the World Economy*, New York: Simon & Schuster.
Yılmaz, E. N. & Gönen S. (2018). Attack detection/ prevention system against cyber attack in industrial control systems, *Computers & Security* Vol. 77, 98.
Бабић, В. (2009). *Компјутерски криминал*, Сарајево: Рабиц.
Басан, М., Кофман, В. & Жоа, Д. (2005). „Десет теза за социолошку теорију урбане динамике". У: Вујовић, С. & Петровић М. (прир.) (2005). *Урбана социологија* (229-238). Београд: Завод за уџбенике и наставна средства.
Бауман, З.(2003). „Туристи и вагабунди". У: Вулетић, В. (ур.) (2003). *Глобализација – мит или стварност* (251-273). Београд: Завод за уџбенике и наставна средства.
Бек, У. (2001). *Ризично друштво: у сусрет новој модрени*. Београд: Филип Вишњић.
Бериша, Х. & Баришић, (2016). Безбедносни изазови - Кибернетски простор и информационо ратовање. У: С. Петровић (ур.). *Злоупотреба информационих технологија и заштита*, Београд: ИТ вештак.
Божиловић, Н. (2004). *Рок култура*. Ниш: Студенстски културни центар.
Бошковић, М. (1998). *Организовани криминалитет*, Београд: Полицијска академија.
Бошковић. М. & Јовичић, Д. (2002). *Криминалистика методика*. ВШУП: Бања Лука.
Бурдије, П. (1999). *Сигнална светла: прилози за отпор неолибералној инвазији*. Београд: Завод за уџбенике и наставна средства.
Виденовић, И. (2015). *Речник социјалног рада*, Београд: Удружење

стручних радника социјалне заштите Србије.
Волерстин, И. (2003). „Глобализација или период транзиције? Поглед на дугорочно кретање светског система“. У: В. Вулетић (прир.), *Глобализација – мит или стварност* (92-111), Београд: Завод за уџбенике и наставна средства.
Вујаклија, М. (1975). *Лексикон страних речи и израза*, Београд: Просвета.
Вулетић, В. (2006). *Глобализација-актуелне дебате*, Београд: Библиотека Полис.
Вулетић, Д. (2011). *Одбрана од претњи у сајбер простору*, Београд: Институт за стратегијска истраживања.
Вулетић, Д. (2017). Употреба сајбер простора у контексту хибридног ратовања, *Војно дело,* вол. 69, бр.7, 308-325.
Гаћиновић, Р. (1998). *Савремени тероризам*, Београд: Графомарк.
Гаћиновић, Р. (2011). Тероризам – Изазов науке и политике. У: Шикман, М., Амиџић Г. (ур.) *Супростављање тероризму-Међународни стандарди и правна регулатива*. Бања Лука: Висока школа унутрашњих послова.
Герц, К. (1998). *Тумачење култура*, Београд : Чигоја штампа.
Giddens, A. (2005). *Odbjegli svijet – kako globalizacija oblikuje naše živote?* Zagreb: Klub studenata sociologije Diskrepancija i Naklada Jesenski i Turk.
Гиденс, Е. (1998) *Последице модерности*, Београд: Филип Вишњић.
Гиденс, Е. (2003). *Социологија*, Београд: Економски факултет.
Горц, А. (1982). *Због пролетаријату*, Београд: Радничка штампа.
Дамњановић, И. (2009). Постоји ли сајбертероризам, *Политичка ревија* 8 (19) 1, 237-253.
Ђокић, З. & Живановић, С. (2005). „Компјутерски криминал као обиљежје прогресивног криминалитета“. У: Д. Радовановић (ур.), *Казнено законодавство - прогресивна или регресивна рјешења* (305-318), Београд: Институт за криминолошка и социолошка истраживања.
Ериксон, Е. (2008). *Идентитет и животни циклус*. Београд: Завод за уџбенике.
Жоа, Д. & Шулер, М. (2005). „Неједнакости, територије и покретљивости: обновљена перспектива урбане социологије“. У: С., Вујовић & Петровић М. (прир.), *Урбана социологија* (248-262). Београд: Завод за уџбенике и наставна средства.
Јазић, А. (2010). Терористичка пропаганда и улога медија, *Међународни проблеми*, Вол. 62, Бр.1, 113-135.
Јовашевић, Д. (2011). *Лексикон кривичног права*. Београд: Службени

гласник.

Јовић, В. (2001). Прикриверни иследник, Београд: Сезам.

Јонев, К. & Бериша, Х. (2016). Опасност од кибертероризма. У: С. Петровић (ур.). *Злоупотреба информационих технологија и заштита- ЗИТЕХ16*, Београд: ИТ вештак

Кастелс, М. (2000). Информацијско доба : економија, друштво и култура. Књ. 1, *Успон умреженог друштва*. Загреб : Голден маркетинг.

Кастелс, М. (2002). *Моћ идентитета*. Загреб: Голден Маркетинг.

Комлен Николић Л, Гвозденовић Р., Радуловић, С., Милосављевић, А., Јерковић, Р, Живковић, В. Живановић, С, Рељановић, М, Алексић, И. (2010). *Сузбијање високотехнолошког криминала*, Београд: Удружење јавних тужилаца и заменика јавних тужилаца Србије.

Куљански Р. С. (2010). РСА алгоритам и његова практична примена. *Војнотехнички гласник: стручни и научни часопис Југословенске народне армије* 58 (3), 65-77.

Лукнар, И. (2022а). „Прошлост као инструмент геополитике“. У: З. Милошевић (ур.), *Историја као инструмент геополитике* (141-161). Београд: Институт за политичке студије.

Љајић, С., Мета, М. & Младеновић, Ж. (2016). Глобализација економски и психолошки аспекти, *Економски сигнали: пословни магазин* 11 (1), 39-62.

Мандер, Џ. (2003). „Правила корпорацијског понашања“. У: Џ. Мандер и Е. Голдсмит, Т. Живић, М. Марковић, И. Чорбић (Прир.). *Глобализација – аргументи против*, Београд: Clio.

Марић, Р. (1998). Поткултурни стил као поље симболичке акције. *Социологија* 40(2), 159-190.

Мијалковић, С. & Бошковић, Г. (2009). Прање новца и финансирање тероризма. У: Матијевић, М. (ур.). *Корупција и прање новца – узроци, откривање, превенција* (293–302). Сарајево: Интернационална асоцијација криминалиста.

Милашиновић, Р. & Мијалковић, С. (2011). Тероризам као савремена безбедносна претња. У: Шикман, М., Амиџић Г. (ур.) *Супростављање тероризму- Међународни стандарди и правна регулатива*. Бања Лука: Висока школа унутрашњих послова.

Милић, А. (2001). *Социологија породице: критика и изазови*, Београд: Чигоја штампа.

Мимица А. & Богдановић М. (2007). *Социолошки речник*, Београд: Завод за уџбенике.

Павлићевић, П. (2017). Тероризам и организовани криминал: анализа и процена ризика. *Национална безбедност* 4 (6), 34–56.

Пејановић, Љ. & Бејатовић, М. (2009). *Авиотероризам*, Нови Сад: АБМ економик.

Пејановић, Љ. (2003). *Тероризам и противтерористичка дејства у ваздушном саобраћају*, Београд: ВИЗ-ЈАТ.

Петровић, Д. (1998). Организовани криминалитет између визије и реалности. У: Д. Стојановић (ур.) *Србија и европско право* III (30-48), Крагујевац: Правни факултет Универзитета: Институт за правне и друштвене науке.

Петровић, Р.С. & Стојановић Р. М. (2016). Информациона технологија у функцији криминала беле-крагне. У: С. Петровић (ур.). *Злоупотреба информационих технологија и заштита*, Београд: ИТ вештак, 13-26.

Петровић, С. (2000). Кибер-тероризам, реалност или фикција? *Безбедност* 42 (5/6), 643-675.

Савић, А. & Стајић Љ. (2006). *Основи цивилне безбедности*, Нови Сад: Факултет за правне и пословне студије.

Симеуновић, Д. (1989). *Политичко насиље*, Београд: Радничка штампа.

Симеуновић, Д. (1993). *Насиље. Енциклопедија политичке културе*, Београд: Савремена администрација.

Симеуновић, Д. (2009). *Тероризам: општи део*, Београд: Правни факултет Универзитета у Београду.

Скакавац, З. (2010). Тероризам - савремени феноменолошки облици испољавања и карактеристике. У: М, Креча (ур.). Међународни научни скуп Тероризам и људске слободе, Вол. ИХ. (331-345), Београд: Удружење за међународно кривично право.

Смит, Д. А. (1998). *Национални идентитет*, Београд: Библиотека XX век.

Сорос, Џ. (2003). *О глобализацији*, Београд: Самиздат Б92.

Стиглиц, Ј. Е. (2013). Слободан пад. Америка, слободна тржишта и слом светске привреде, Нови Сад: Академска књига.

Стојнов, Д. (1999). Личност: испитивање порекла, значења и разлике од сродних појмова, *Психологија* 32(1-2), 45-64.

Субошић, Д. & Васиљевић (Лукнар) И. (2017). „Мигрантска криза као изазов за очување националног идентитета чланица Европске уније“. *Војно дело*, вол. 69, бр. 2, 78-89.

Тасић, В. & Бауер И. (2003). *Речник компјутерских термина*, Београд: Микро књига.

Томашевски, К. (1983). *Изазов тероризма*, Београд: НИРО Младост.

Урошевић, В. (2009). „Нигеријска превара“ у Републици Србији, *Безбедност* Вол.3, 1-12

Хантингтон, С. (2000). *Сукоб цивилизација*, Подгорица: ЦИД

Хелд, Д. (2003). Дебате о глобализацији. У: В. Вулетић (ур.), *Глобализација – мит или стварност* (48-60). Београд: Завод за уџбенике и наставна средства.

Шикман, М. (2011). Тероризам као криминални феномен – криминолошко, криминалистичко, кривичноправно гледиште. У: М. Шикман, Г. Амиџић (ур.)., *Супротстављање тероризму – међународни стандарди и правна регулатива* (43-63). Бања Лука: Висока школа унутрашњих послова.

Шкулић, М. (2003). *Организовани криминалитет. Појам и кривично процесни аспекти*, Београд: Досије.

Шкулић, М. (2014). Однос организованог криминалитет у кривичноправном смислу и саучесништва, *Наука, безбедност, полиција: часопис Полицијске академије* 19 (3), 1-26.

Документи (законска акта, одлуке, акциони планови, уредбе, правилници, стратешки документи, агенде)

APEC (2021). *TEL Strategic Action Plan 2021-2025*. Retrieved from: https://www.apec.org/groups/som-steering-committee-on-economic-and-technical-cooperation/working-groups/telecommunications-and-information (28.11.2021)

CER-Proposal for a Directive on the resilience of critical entities (2020). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN (28.11.2021)

Council of Europe (2021). *Second Additional Protocol to the Cybercrime Convention adopted by the Committee of Ministers of the Council of Europe*. Retrieved from: https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe (28.11.2021)

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013). Retrieved from: https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en (28.11.2021)

Enisa (2018, 7 November). *EU cybersecurity organisations agree on 2019 roadmap*. Retrieved from: https://www.enisa.europa.eu/news/enisa-news/eu-cybersecurity-organisations-agree-on-2019-roadmap (12.12.2018)

European Commission (2021). *Communication from the Commission to the European Parliament and the Council on the Second Progress Report on the implementation of the EU Security Union Strategy*, Brussels. Retrieved from: https://ec.europa.eu/info/system/files/com2021_440_en.pdf (28.11.2021)

Migration Data Portal (2021). *Total number of international migrants at mid-year 2020*. Retrieved from: https://www.migrationdataportal.org/international-data?i=stock_abs_&t=2020 (27.11.2021)

NATO (2002, 21-22 November). *Prague Summit*. Retrieved from: https://www.nato.int/docu/comm/2002/0211-prague/ (21.3.2017)

NATO (2021). *Brussels Summit Communique*. Retrieved from: https://www.nato.int/cps/en/natohq/news_185000.htm (27.11.2021)

NIAS19 (2019, 15-17 October). Cyber Security Simposium. Retrieved from: https://securitydelta.nl/events/event/2157-nato-information-assurance-symposium-nias-2019-2019-10-15 (18.2.2022)

NIS2 (2021). *The NIS2 Directive: A high common level of cybersecurity in the EU*. Retrieved from:https://www.europarl.europa.

eu/thinktank/en/document.html?reference=EPRS_BRI(2021)689333 (27.11.2021)

OSCE (2021). *The 3rd Inter-Regional Conference on Cyber/ ICT Security.* Retrieve from: https://www.osce.org/secretariat/490955 (28.11.2021)

Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/1148 (2020). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN (28.11.2021)

The EU's Cybersecurity Strategy for the Digital Decade (2020). Retrieved from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade- (28.11.2021)

The European Agenda on Security: Questions & Answers (2015). Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_4867 (28.11.2021)

UN Global Counter - Terrorism Strategy, 2006. Retrieved from: https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy (12.2.2017)

Закон о електронским комуникацијама, „Службени гласник РС", бр. 44/10, 60/13, 62/14, 95/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2010/44/1/reg (14.10.2017)

Закон о електронској трговини, „Службени гласник РС", бр. 41/09, 95/13, 52/19. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2009/41/4/reg (31.8.2019)

Закон о електронској управи, „Службени гласник РС", бр. 27/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/27/4/reg (14.3.2019)

Закон о електронском документу, електронској идентификацији и улугама од поверења у електронском пословању, „Службени гласник РС", бр. 94/17. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2017/94/4/reg (15.11.2021)

Закон о електронском фактурисању, „Службени гласник РС", бр. 44/21. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2021/44/3/reg (22.11.2021)

Закон о заштити података о личности, „Службени гласник РС", бр. 87/18. Преузето с https://www.paragraf.rs/propisi/zakon-o-zastiti-podataka-o-licnosti.html (8.2.2019)

Закон о информационој безбедности, „Службени гласник

РС“, бр. 6/16, 94/17, 77/19. Преузето с https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html (26.11.2021)

Закон о јавном тужилаштву, „Службени гласник РС“, бр. 116/08, 104/09, 101/10, 78/11 - др. закон, 101/11, 38/12 - одлука УС, 121/12, 101/13, 111/14 - одлука УС, 117/14, 106/15, 63/16-УС. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2008/116/4/reg (30.10.2017)

Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица, „Службени гласник РС“, бр. 85/05. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/85/7/reg (31.1.2017)

Закон о министарствима, „Службени гласник РС“, бр. 128/20. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2020/128/1 (27.11.2021)

Закон о оглашавању, „Службени гласник РС“, бр. 6/16, 52/19 – др. закон. Преузето с https://www.paragraf.rs/propisi/zakon_o_oglasavanju.html (30.8.2019)

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, „Службени гласник РС“, бр. 61/05 и 104/09. Преузето с: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/61/7/reg (7.10.2017)

Закон о платним услугама, „Службени гласник РС“, бр. 139/14, 44/18. Преузето с https://www.paragraf.rs/propisi/zakon_o_platnim_uslugama.html7 (15.2.2019)

Закон о управним споровима, „Службени гласник РС“, бр. 111/09. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2009/111/6 (28.4.2017)

Кривични законик, „Службени гласник РС“, бр. 85/05, 88/05 - исправка, 107/05 – исправка, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/85/6/reg (15.9.2019)

Министарство просвете, науке и технолошког развоја (2021). Информатор о раду Министарства просвете, науке и технолошког развоја. Преузето с https://www.mpn.gov.rs/informator-o-radu/ (27.11.2021)

Национална стратегија за спречавање и борбу против тероризма за период 2017-2021. године, „Службени гласник РС“, бр. 94/17. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/94/1/reg (30.12.2017)

Правилник о захтевима за уређаје и програмску подршку за законито пресретање електронских комуникација и техничким

захтевима за испуњење обавезе задржавања података о електронским комуникацијама, „Службени гласник РС“, бр. 88/15. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2015/88/1/reg (18.12.2017)

Правилник о избору програма од јавног интереса у области развоја информационог друштва које реализују удружења, „Службени гласник РС“, бр. 47/13 и бр. 88/16. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2013/47/3/reg (21.12.2018)

Правилник о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање, „Службени гласник РС”, бр. 46/19, 104/20. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2019/46/7/reg (27.11.2021)

Правилник о Регистру квалификованих средстава за креирање електронских потписа и електронских печата, „Службени гласник РС“, бр. 31/18, 64/21. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/31/7/reg (16.11.2021)

Правилник о Регистру пружалаца квалификованих услуга од поверења, „Службени гласник РС“, бр. 31/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/31/8/reg (1.12.2018)

Правилник о Регистру пружалаца услуга електронске идентификације и шема електронске идентификације, „Службени гласник РС“, бр. 67/18. Преузето с http://pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/67/1/reg (7.12.2018)

Правилник о техничким и другим захтевима при изградњи пратеће инфраструктуре потребне за постављање електронских комуникационих мрежа, припадајућих средстава и електронске комуникационе опреме приликом изградње пословних и стамбених објеката, „Службени гласник РС“, бр. 123/12. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2012/123/4/reg (7.2.2018)

Правилник о условима које мора да испуњава квалификовано средство за креирање електронског потписа односно печата и условима које мора да испуњава именовано тело, „Службени гласник РС“, бр. 34/18, 3/20, 87/20, 64/21. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/34/4/reg (21.11.2021)

Правилник о условима које морају да испуњавају квалификовани електронски сертификати, „Службени гласник РС“, бр. 34/18 и 81/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/ministarstva/pravilnik/2018/34/3/reg (21.1.2019)

РЗС (2021). Годишње истраживање о употреби информационо-комуникационих технологија. Преузето с https://www.stat.gov.rs/sr-latn/vesti/20211022-godisnje-istrazivanje-o-ikt/?a=27&s=0 (5.5.2022)

Стратегија за борбу против високотехнолошког криминала за период 2019-2023. године, „Службени гласник РС“, бр. 71/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg (19.11.2021)

Стратегија за борбу против прања новца и финансирања тероризма за период 2020-2024. године, „Службени гласник РС“, бр. 14/20. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2020/14/1/reg (27.11.2021)

Стратегија заштите података о личности, „Службени гласник РС“, бр. 58/10. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2010/58/1 (17.10.2019)

Стратегија научног и технолошког развоја Републике Србије за период од 2021. до 2025. године, „Службени гласник РС“, бр. 10/21. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/10/1/reg (27.11.2021)

Стратегија националне безбедности Републике Србије, „Службени гласник РС“, бр. 94/19. Преузето с: https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/strategija/2019/94/2 (10.11.2021)

Стратегија одбране Републике Србије, „Службени гласник РС“, бр. 94/19. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/strategija/2019/94/1 (25.11.2021)

Стратегија развоја вештачке интелигенције у Републици Србији за период 2020-2025, „Службени гласник РС“, бр. 96/19. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2019/96/1/reg (27.11.2021)

Стратегија развоја дигиталних вештина у РС за период 2020-2024, „Службени гласник РС“, бр. 21/20. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2020/21/2/reg/ (18.10.2021)

Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године, „Службени гласник РС“, бр. 68/10. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/

reg/viewAct/df3fb65a-6acc-4e90-bd0f-f69066f6e0aa (19.11.2017)

Стратегија развоја индустрије информационих технологија за период од 2017. до 2020. године, „Службени гласник РС“, бр. 95/16. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2016/95/1/reg (12.1.2017)

Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године, „Службени гласник РС“, бр. 86/21. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/86/1/reg (12.11.2021)

Стратегија развоја мрежа нове генерације до 2023. године, „Службени гласник РС“, бр. 33/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/33/1 (3.4.2019)

Уредба о безбедности и заштити деце при коришћењу информационо-комуникационих технологија, „Службени гласник РС“, бр. 13/20. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2020/13/4/reg (27.11.2021)

Уредба о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, „Службени гласник РС“, бр. 94/16. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/1/reg (12.1.2017)

Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, „Службени гласник РС“, бр. 94/16. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2016/94/2/reg (21.5.2017)

Уредба о ближем уређењу услова које морају да испуне шеме електронске идентификације за одређене нивое поузданости, „Службени гласник РС“, бр. 60/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2018/60/1/reg (12.12.2018)

Уредба о условима за пружање квалификованих услуга од поверења, „Службени гласник РС“, бр. 37/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2018/37/2/reg (1.11.2018)

Интернет извори

Blic (2022, 6. Jun). Svet-Blic online. Retrieved from: https://www.blic.rs/vesti/svet (6.6.2022)

Bogdanovski, M. & Petreski, D. (2016). Cyber Terrorism – Global Security Threat, *International Scientific Defence*, *Security and Peace Journal*. Retrieved from: https://www.academia.edu/11151330/CYBER_TERRORISM_GLOBAL_SECURITY_THREAT (15.2.2017)

Clay, W. (2007). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress, Congressional Research Service. Retrieved from: https://fas.org/sgp/crs/terror/RL32114.pdf (17.3.2017)

Council of Europe (2005). *Organised crime situation report 2005. Focus on the threat of economic crime*, Octopus Programme. Retrieved from: https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Report2005E.pdf (16.4.2017)

Davis, A. (2002, 1 February). The Afghan files: Al-Qaeda Documents from Kabul. *Jane's Intelligence Review*. Preuzeto s https://www.janes.com/security/janes-intelligence-review (7.2.2017)

Deutsch, J. (1996, 25 June). Statement before the US Senate Governmental Affairs. 1996 Conressional Hearings Intelligence and Security. Retrieved from: https://fas.org/irp/congress/1996_hr/s960625d.htm (23.9.2017)

Dewar, R. S. (2014). The Triptych of Cyber Security: A Classification of Active Cyber Defence. In: P. Brangetto, M. Maybaum, J. Stinissen (Eds.). *6th International Conference on Cyber Conflict* Retrieved from: https://www.academia.edu/6412868/_The_Triptych_of_Cyber_Security_A_Classification_of_Active_Cyber_Defence (8.4.2017)

Eurostat Statistics (2020). *Digital economy and society statistics - households and individuals*. Retrieved from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals (25.11.2021)

Fallico, M. (2013, 24 October). *Cyber terrorism*. Computer Crimes. Retrieved from: https://www.coursehero.com/file/8455402/Cyber-Terrorism-Essay/ (9.8.2018)

Farnsworth, T. (2011, June). China and Russia Submit Cyber Proposal, *Arms Control Association*. Retrieved from: https://www.armscontrol.org/act/2011-11/china-russia-submit-cyber-proposal (28.11.2018)

Fischer E. A. (2005, 22 February). *CRS Report for Congress, Creating a National Framework for Cybersecurity: An Analysis of Issues*

and Options, Congressional Research Service. The Library of Congress. Retrieved from: https://fas.org/sgp/crs/natsec/RL32777.pdf (25.4.2018)

Gercke, M. (2012, September). *Understanding cybercrime: phenomena, challenges and legal response,* Cibercrime: ITU. Retrieved from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (19.6.2017)

Glazer, Ilsa M. (Spring 2006). Armies of the Young: Child Soldiers in War and Terrorism (review). [Online] *Anthropological Quarterly*, 79 (2), 373-384. DOI:10.1353/anq.2006.0021. Retrieved from: https://muse.jhu.edu/ [Project Muse Database] (4.9.2017)

Healey, J. (2012). *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council. Retrieved from: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/ (28.11.2017)

Hutchins, E. M., Cloppert, M. J., Amin R. M. (2011). Intelligence - driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. In: *Proceedings of the 6th annual international conference on information warfare and security*, Washington DC. Retrieved from: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (28.11.2017)

Iasiello, E. (2012). *Identifying Cyber-Attackers to Require High-Tech Sleuthing Skills*, National Defense Industrial Association. Retrieved from: http://www.academia.edu/3680849/Identifying_Cyber-Attackers_to_Require_High-Tech_Sleuthing_Skills_Iasiello (30.11. 2017)

Iasiello, E. (2018, 1st Quarter). Is Cyber Deterrence an Illusory Course of Action? *ASPJ Africa & Francophonie* 9 (1), 35-51. Retrieved from: https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue-1/2018_1_e.pdf (21.11.2020)

IEA (2021). Global Energy Review 2021. CO2 emissions. Retrieved from: https://www.iea.org/reports/global-energy-review-2021/co2-emissions (25.4.2022)

ITU Plenipotentiary Conference (2021). Retrieved from: https://www.itu.int/en/events/Pages/default.aspx (27.11.2021)

Jalil, S. A. (2003, June). *Countering Cyber Terrorism Effectively: Are We Ready To Rumble?* Giac Security Essentials Certification (GSAC): Global Information Assurance Certification Paper. Retrieved from: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 (19.11.2017)

Klein, J.J (2018). Deterring and Dissuading Cyberterrorism, *ASPJ Africa & Francophonie* 9 (1), 21-34. Retrieved from: https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue-1/2018_1_e.pdf (21.11.2020)

Knopf, W. J. (2013, 11 June). Use with Caution: The Value and Limits of Deterrence Against Asymmetric Threats, *World Politics Review*. Retrieved from: http://www.worldpoliticsreview.com/articles/13006/use-with-cautionthe-value-and-limits-of-deterrence-against-asymmetric-threats (18.7.2017)

Lachow, I. (2013, February). *Active Cyber Defense. A Framework for Policymakers*, Policy Brief: Center for a New American Security. Retrieved from: https://s3.amazonaws.com/files.cnas.org/documents/CNAS_ActiveCyberDefense_Lachow_0.pdf?mtime=20160906080446 (11.11.2017)

Lee, M., R. (2015). *Activecyber defense cycle: Asset identification and network security monitoring***.** Retrieved from: https://www.oilandgaseng.com/articles/active-cyber-defense-cycle-asset-identification-and-network-security-monitoring/ (28.11.2021)

Lewis, A. J. (2002, December). *Assessing the Risks of Cyber Washington DC, Terrorism, Cyber War and Other Cyber Threats*. Washington DC: Center for Strategic and International Studies. Retrieved from: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (10.1.2018)

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corp. Retrieved from: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (8.9.2017)

Mandt, E & Lee, R. (2016). *Leveraging Threat Intelligence in an Active Defense*. [Power Point Presentation]. Retrieved from: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492180823.pdf (23.9.2017)

Menn, J. (2013, May 18). *Cyber attacks against banks more severe than most realize*. Reuters. Retrieved from: https://www.reuters.com/article/us-cyber-summit-banks/cyber-attacks-against-banks-more-severe-than-most-realize-idUSBRE94G0ZP20130518 (5.8.2017)

Mohsin, Saima; Khan, Shaan. (March 14, 2013). *Police: Kids young as 8 used as bombers in Pakistan*. CNN [Online] Retrieved from: https://edition.cnn.com/2013/03/14/world/asia/pakistan-child-bombers/index.html (15.3.2013)

Mulvenon, C. J. & Rattray, J. G. (2012). *Addressing Cyber Instability: Executive Summary*, Cyber Conflict Studies Association. Retrieved from: http://static1.1.sqspcdn.com/static/f/956646/19193589/1341880349257/

CCSA+-+Addressing+Cyber (5.10.2015)

Murray, Rebecca (2010, October 29). *Scarred by Sri Lanka's war with Tamil Tigers, female exfighters build new lives*. The Christian Science Monitor. Retrieved from: http://www.csmonitor.com/World/Asia-South-Central/2010/1029/Scarred-by-Sri-Lanka-s-war-with-Tamil-Tigers-female-ex-fighters-build-new-lives (17.4.2017)

Puttonen, R. & Romiti, F. (2020). The Linkages between Organized Crime and Terrorism, *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2019.1678871. Retrieved from: https://www.tandfonline.com/doi/full/10.1080/1057610X.2019.1678871 (7.12.2021)

Rauscher, K. (2013, 27 November). *It's Time to Write the Rules of Cyberwar*, IEEE Spectrum. Retrieved from: https://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar (24.2.2017)

Rollins, J. & Wilson, C. (2007, 22 January). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, CRS Report for Congress. Retrieved from: https://fas.org/sgp/crs/terror/RL33123.pdf (19.1.2018)

Saint-Claire, Steve (2011). *Overview and Analysis on Cyber Terrorism*, Retrieved from: http://www.oalib.com/paper/2690062#.W4Pa9V4zbIU (7.1.2017)

Scaparrotti, M. C (2014). Information Operations, *Joint Publication* 3-13. Retrieved from: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (18.1.2018)

Schmitt, M. N. (1999). Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework, *Columbia Journal of Transnational Law* Vol. 37, 885- 937. Retrived from: http://www.dtic.mil/dtic/tr/fulltext/u2/a471993.pdf (14.3.2017)

Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington D.C.: The National Academies Press, 151-178. Retrieved from: http://wpressutexas.net/cs378h/images/f/fe/DeterringCyberAttacksWorkshop2010.pdf (19.3.2017)

Schneier, Bruce (2003, 16 December). *Blaster and the Great Blackout*, SALON. Schneier on Security. Retrieved from: https://www.schneier.com/essays/archives/2003/12/blaster_and_the_grea.html (23.11.2017)

Smith, Tony (2001, 31 October). Hacker Jailed for Revenge Sewage Attacks. Job rejection caused a bit of a stink, *The Register. Biting the hand that feeds IT*. Retrived from: https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ (11.10.2017)

Sproles, J. & Byars, W. (1998). *Statistics on Cyber-terrorism. Computer Ethics Course at ETSU*. Retrieved from: http://csciwww.etsu.edu/gotterbarn/stdntppr/stats.htm (14.3.2017)

Stalings, Wiliam (2011). *Cryptography and Network Security Principles and Practices*. Prentice Hall. Retrieved July 3, 2017 from: https://wanguolin.github.io/assets/cryptography_and_network_security.pdf (11.7.2020)

Swanson, J. (2012, 25 July). *Looking into the minds of killers*. Special to CNN [Online] Retrieved from: https://edition.cnn.com/2012/07/24/opinion/swanson-colorado-shooting/index.html (21.4.2017)

Tajdi, Džo (2021, 12 May). "Amerika i hakerski napad na Kolonijal: kako su sajbernapadači zaustvili naftovod", *BBC News*. Retrieved from: https://www.bbc.com/serbian/lat/svet-57070222 (9.10.2021)

Tikk, E., Kaska, K. & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*. Cooperative Cyber Defence Centre of Excellence. Retrieved from: https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/ (6.8.2018)

United Nations (2008). *International Instruments related to the Prevention and Suppression of International Terrorism*. Retrieved from: https://www.unodc.org/documents/terrorism/Publications/Int_Instruments_Prevention_and_Suppression_Int_Terrorism/Publication_-_English_-_08-25503_text.pdf (7.8.2018)

United Nations (2021). *Counter-Terrorism Week*. Retrieved from: https://www.un.org/counterterrorism/2021-counter-terrorism-week (27.11.2021)

Warren Axelrod, C. (2002, 27 February). *Security Against Cyber Terrorism.* Pershing Division of Donaldson, Lufkin & Jenrette Securities Corp 2002. Preuzeto s: http://www.sia.com/iuc2002/pdf/axelrod.pdf (6.7.2003)

Wasielewski, Philip G. (2007, 1st Quarter). Defining the War on Terror. [Online] *Joint Force Quarterly*, Issue 44, 13-18. Retrieved from: http://www.ndu.edu/press/lib/pdf/jfq-44/JFQ-44.pdf (26.2.2017)

Weigant, C. (2013, 28 October). *We Need a Geneva Convention on Cyber Warfare*, Huffington Post: The Blog. Retrieved from: https://www.huffpost.com/entry/we-need-a-geneva-conventi_b_4171853?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnJzLw&guce_referrer_sig=AQAAADlD2CIt4Wur3r4w3YYrl7IbJF3srq7aYRael71ZRPvqmhTirTeehGDNDs4yp8xFDJRKSC5hWSY-8VveoXq_7lK1Wy_oXLPqxGGuVf_tMWBFKMHg_hgcZTuiERtSHXTnD3iwKDbUk5AJkNnhutGDnfgO0zSD6QF (6.12.2017)

Weimann, G. (2004, March). *How Modern Terrorism Uses The Internet*. Special Report Washington, DC: United States Institute of Peace. Retrieved from: https://www.usip.org/sites/default/files/sr116.pdf (24.12.2018)

Weimann, G. (2008, December). How Terrorists Use the Internet to Target Children. *InSite*: *The Official Newsletter of SITE Intelligence Group* 1(8), 14–16. Retrieved from: http://sitemultimedia.org/docs/inSITE_December_2008.pdf (15.10.2017)

Wilke, A. Clifford. (1999, 5 March). *Infrastructure Threats from Cyber-Terrorists*. Retrieved from: https://www.occ.gov/news-issuances/bulletins/1999/bulletin-1999-9.pdf (8.6.2018)

Wilson, C. (2003, 17 October). *Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress. Retrieved from: https://fas.org/irp/crs/RL32114.pdf (27.7.2018)

WSIS forum (2021). ICTs for Inclusive, Resilient and Sustainable Societies and Economies. Retrieved from: https://www.itu.int/net4/wsis/forum/2021/ (28.11.2021)

Yagli, S. & Dal, S. (2014). Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures, *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering* 8 (4). Retrieved from: https://pdfs.semanticscholar.org/959c/817cd8d725a3e37feb3b251b18a1c951e1cf.pdf (22.7.2021)

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

327.88::323.28
343.3::004
341.41/.46

ЛУКНАР, Ивана, 1984-
Сајбер тероризам : мере за сузбијање и превенција / Ивана Лукнар. - Београд : Институт за политичке студије, 2022 (Житиште : Ситопринт). - 245 стр. : илустр. ; 21 cm

Тираж 100. - Регистар. - Библиографија: стр. 218-245.

ISBN 978-86-7419-360-0

а) Тероризам -- Превенција б) Рачунарска технологија -- Злоупотреба -- Спречавање

COBISS.SR-ID 70101513

Књига систематизује научно-стручну грађу о актуелном проблему и указује на неопходне елементе за сузбијање и превенцију сајбер тероризма; представља добру основу за упознавање са истраживаним феноменом и подстиче његова даља истраживања.

Проф. др Ивана Дамњановић

Стваралац дела је понудила низ иновативних закључака изложених прегледним и јасним научним стилом на поједностављен начин, језиком лако разумљивим читаоцима без обзира на њихово претходно познавање истраживане теме.

Академик Драган Симеуновић

ISBN 978-86-7419-360-0