УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

# Компјутерски тероризам

(мастер рад)


МЕНТОР:

Проф. др Дарко Димовски

СТУДЕНТ:

Марија Клејић

Број индекса: М023/25-УП


Ниш, 2026.

# САДРЖАЈ

# УВОД

Сајбер нападачи различитих профила су у више наврата показали да имају способност да угрозе рад читавих система. Поставља се питање да ли су терористи такође у стању да изазову такве последице. Интернет и рачунарске мреже представљају снажан ресурс на који се савремено друштво у великој мери ослања. Имајући у виду да се државна инфраструктура, као што су саобраћајни системи, електроенергетске мреже, финансијске трансакције и војни одбрамбени механизми, све више заснива на рачунарским мрежама, јавља се страх да би компјутерски напад терористе могао озбиљно да наруши функционисање нападнутог система, па чак и да доведе до угрожавања људских живота. Компјутерски, односно сајбер (cyber) тероризам представља противзаконити активност и односи се на унапред планиране, политички мотивисане нападе на податке, компјутерске системе и програме, са намером да се, пре свега, изазову страх и осећај несигурности код жртава. Како се одвија у сајбер простору, подразумева се да је терористички чин планиран, изведен или координисан уз помоћ рачунара и рачунарских мрежа. Сајбер тероризам, попут свих осталих облика тероризма, има своју политичку, идеолошку, верску и социјалну димензију. Угрожавање критичне националне инфраструктуре је један од потенцијално најопаснијих видова сајбер тероризма.

Поштујући основне научне принципе објективности, општости и систематичности и имајући у виду специфичност предмета истраживања у раду су примењени методи дескрипције, анализе и синтезе, а научни метод коришћен приликом прикупљања података је претежно метод анализе садржаја, у оквиру којег су анализирани научни извори (уџбеници, научни радови, докторске дисертације и сл.). Такође су у раду анализирани прописи који се могу довести у везу са предметом истраживања, као и мањи број електронских извора података. Осим поменутих, у раду су у мањем обиму коришћене и статистичка метода, компаративна метода, као и метод просте дедукције.

Предмет истраживања првог поглавља мастер рада под називом „појам и карактеристике тероризма“ ће бити: историјски развој тероризма, дефинисање појма тероризма, феномен тероризма као друштвене појаве, карактеристике тероризма као злочина и карактеристике самих терористичких аката.

Предмет истраживања другог поглавља мастер рада под називом „појам и карактеристике компјутерског криминалитета“ биће: појам и одлике компјутерског криминалитета, кривична дела против безбедности рачунарских података (оштећење рачунарских података и програма, рачунарска саботажа, прављење и уношење рачунарских вируса, рачунарска превара, неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, спречавање и ограничавање приступа јавној рачунарској мрежи, неовлашћено коришћење рачунара или рачунарске мреже, прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података), затим кривична дела чији је компјутерски криминал елемент бића кривичног дела (приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију, искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу, неовлашћено искоришћавање ауторског дела или предмета сродног права), затим обим, динамика и појавни облици извршења кривичних дела компјутерског криминала у Републици Србији и узроци, услови и поводи извршења компјутерског криминалитета у Републици Србији.

Предмет истраживања трећег поглавља мастер рада под називом „компјутерски тероризам“ биће: појам компјутерског тероризма, разлика компјутерског тероризма од сајбер напада, специфичности компјутерског тероризма у односи на конвенционални тероризам, облици деловања сајбер терористa (у које спадају: регрутовање чланова, комуникација, бављење организованим криминалом, могућност вођења асиметричног сукоба и ширење пропаганде), затим значај друштвених мрежа за деловање сајбер терористa и покушаји борбе против компјутерског тероризма на глобалном плану.

# 1. ПОЈАМ И КАРАКТЕРИСТИКЕ ТЕРОРИЗМА

## 1.1. Историјски развој тероризма

Међу првим актима тероризма убраја се убиство Хипарха, озлоглашеног тиранина Атине, (514 год. п.н.е.) у име републике, а призма савременог тероризма је обликована у периоду буржоаске револуције, када се стварао нови економски, политички и идеолошки профил живота. Од првих цивилизација до данашњег времена су међу основним субјектима међународне заједнице и унутар појединачних држава, несугласице решаване насилним путем, без обзира што се до решења могло доћи и рационалним и демократским облицима комуникације. Последњих неколико векова, често се посезало за терористичким облицима насиља у решавању сукоба у свету. Као феномен је тероризам настао још у давним временима и био пратилац целокупне људске историје.

Према Цицероновом схватању, Римљани су тираноубиство доживљавали као најузвишенији подвиг, нарочито у случајевима када је убица био у блиским односима са тиранином. Управо због тога су изузетно ценили Брутову храброст, сматрајући да их је она избавила од самовоље Јулија Цезара. Поједини теоретичари истичу да се појава тероризма може везати за настанак класног друштва, односно државе као институције која служи заштити интереса владајуће класе. Насупрот томе, други аутори корене тероризма проналазе на Блиском истоку, у настанку верско-политичке секте у античком Јерусалиму. Роберт Фрајдлендер сматра да су групни тероризам као средство политичке борбе прве примениле исламске оружане групе, које се уједно сматрају и првим организованим терористичким формацијама, познатим под називом „Assassins“.[1]

Тероризам, као појава, није савременог порекла, али претња коју данас носи са собом и шири интензивнија је него икада раније. Он и даље користи структурно смртоносно насиље како би застрашио људе и произвео систематску доминацију и подређеност, али се истовремено јавља и као средство екстремног, насилног отпора према структурама доминације и експлоатације. У савременом добу тероризам је постао инструмент којим се безрезервно настоји остварење политичких циљева, док

[1] Д. Симеуновић, *Тероризам, општи део*, Правни факултет, Београд, 2009, стр. 104-105.

управо ниво насиља и бруталности којима се ти циљеви спроводе даје тероризму посебну специфичност и сврстава га међу изразито упечатљиве друштвено-политичке феномене.

## 1.2. Дефинисање појма тероризма

Реч „тероризам“ потиче из латинске речи „terror, terroris“, што значи страх, ужас, политичко застрашивање и страховладу, а термин тероризма подразумева насиље, страховладу, владање путем застрашивања, политичку борба путем индивидуалног терора и сл. Поред тога, под тероризмом се подразумева и одређена доктрина, као и начин борбе за постизање конкретних циљева кроз систематичну примену насиља. Француски књижевник Жил Ромен (Jules Romains) истиче да тероризам може служити као метод владавине, док Ел Фатах (El Fattah) подсећа да се у античком периоду тероризам користио у борби против тираније и тирана и да, према Ксенофонту, тираноубице нису биле кажњаване, већ су, напротив, биле слављене.[2]

Када се дефинише тероризам, треба кренути од термина „terror“, који у политичком смислу значи акте насиља који се врше у циљу засташивања народа, сламања отпора и одржања власти тоталитарног режима. „Teror“ значи страх, ужас, страховладу и политичко насиље, а због неких заједничких елемент долази до мешања појмова „teror“ и тероризам. „Teror“ је власт која је чврсто организована у којој је страх саставни елемент свакодневнице, а тероризам је акт насиља из политичких и идеолошких побуда у циљу застрашивања и сламања отпора у намери постизања идеолошких и политичких циљева.

## 1.3. Феномен тероризма као друштвене појаве

Схватити на адекватан начин схватити суштину и карактеристике савременог тероризма без разумевања ширих културних, социјалних, економских и политичких оквира у којима се реализује није могуће. Предмет истраживања је веома комплексан,

[2] Д. Живаљевић, А. Југовић, Тероризам као безбедносни проблем и друштвена девијација*, Журнал за криминалистику и право бр. 1, vol. 2014,* стр. 86.

тако да постоје различита схватања приликом успостављања консензуса међу теоретичарима који се њиме баве.

Савремени тероризам све више поприма интернационални карактер, јер се командовање и контрола терористичких организација, процеси регрутовања и обуке, извођење активности, као и циљне групе, могу налазити у различитим државама. Једна од кључних одлика тероризма у 21. веку јесте његова сложеност, будући да представља спој бројних аспеката људског искуства, укључујући области као што су политика, психологија, филозофија, војне стратегије и историја.[3]

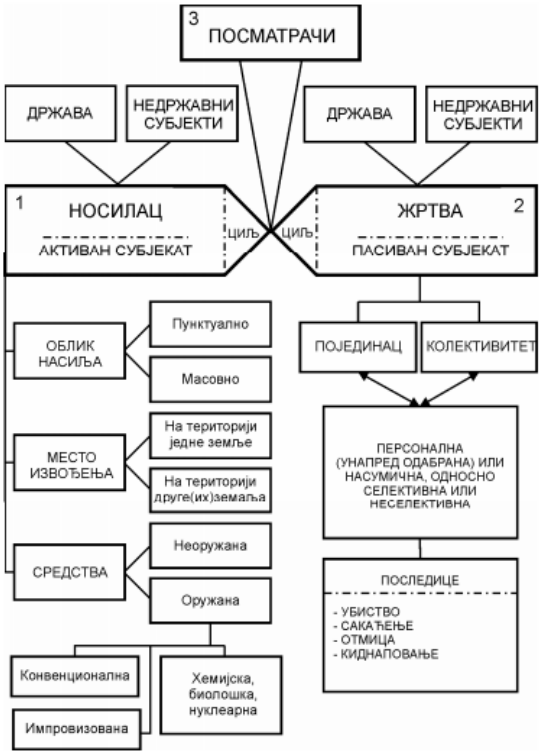
Основна карактеристика већине истраживања тероризма огледа се у недостатку јединствене, универзалне дефиниције, јер је реч о изузетно хетерогеном и тешко одредивом феномену, што је последица сложених и различитих разлога. Због тога је неопходно успоставити јасан концептуални и методолошки оквир који би омогућио што свеобухватније сагледавање природе и суштине тероризма.

Алекс Шмит (Alex Schmidt), један од најзначајнијих светских истраживача тероризма и насиља, још почетком осамдесетих година прошлог века настојао је да формулише академску дефиницију тероризма засновану на консензусу. Анализирајући 109 академских дефиниција, дошао је до закључка да је насиље, односно примена силе, најзаступљенији елемент, са уделом од чак 83,5%, испред појмова као што су страх, претња, психолошки ефекти, циљ, стратегија, метод борбе, непоштовање прихваћених правила, присила, публицитет и других елемената који се појављују у дефиницијама тероризма.

Због својих социјалних узрока и последица, тероризам поседује и обележја друштвене девијације, јер угрожава кључне друштвене вредности попут људског живота, слободе, имовине и политичког система одређене државе. Он је обележен застрашујућим физичким и психолошким методама политичке борбе, којима се на систематичан начин настоје остварити различити политички и друштвени циљеви. Напори усмерени на сузбијање радикализације требало би да буду прилагођени конкретним околностима, уз ослањање на продубљена сазнања о карактеристикама

[3] М. Крстић, Улога обавештајног фактора у борби против тероризма, *Цивитас бр. 6. vol 2016*, стр. 95.

појединца или групе којима су намењени, као и да буду предмет континуиране процене.[4]



Илустрација 1. Сложеност терористичког процеса[5]

Стога, због глобализма, криза која је у прошлости била локалног карактера, као што су унутрашњи ратови, сиромаштво, незапосленост, друштвена нестабилност и низак ниво образовања, сада су претворени у међународне безбедносне ризике. Дакле, слабости у овим областима представљају могућности за екстремисте да шире своје ставове, регрутују чланове и присталице и шире свој рат против држава на нова бојна поља. Ипак, у мери у којој се проактивне могућности за за контролу опасности од тероризма нису показале ефикасне и продуктивне, неопходан је један нови приступ и надоградња знања о томе како појединци узимају учешће у тероризму у процесу познатом као радикализација.[6] Заједничке карактеристике насилног и других облика екстремизма представљају прелазак на мотивациони дисбаланс и способност одржавања екстремних средстава као доминантних потреба.

[4] М. Крстић, Улога обавештајног фактора у борби против тероризма, *Цивитас бр. 6. vol 2016*, стр. 98-99.
[5] М. Дробац, *Тероризам – цивилизацијска пошаст, Култура полиса*, стр. 681.
[6] М. Крстић, Улога обавештајног фактора у борби против тероризма, *Цивитас бр. 6. vol 2016*, стр. 123.

Карактеристике насилног екстремизма се тичу специфичних мотива који опредељују појединца ка употреби насиља као екстремног средства за задовољење тих потреба. Путеви насилног екстремизма и радикализације су бројни, а могу их подстаћи дуготрајни проблеми у друштву док у неким случајевима то могу бити неки актуелни догађаји. Разумевање процеса радикализације пружа научну основу за спровођење дерадикализације, разматрајући импликације овог модела и анализирајући прелиминарне доказе о ефикасности компоненти за спровођење програма рехабилитације. Процеси радикализације и дерадикализације се могу посматрати кроз један пирамидални модел, који разликује три фазе: осетљивост на радикалну идеологију, затим фазу кроз коју појединац постаје члан радикалне групе и на крају, спремност особе да делује у име идеологије групе, односно планирањем напада.[7]

## 1.4. Карактеристике тероризма као злочина

Тероризам је као злочин скуп индивидуалних негативних друштвених појава, с обзиром на распрострањеност у простору и времену, којом се крше неке норме и угрожавају вредности. У почетку су те вредности биле националног карактера, а данас су све више заштићене међународним правом.[8] Сам појам тероризма конструисан је ради описивања систематског изазивања страха и анксиозности са циљем контроле и усмеравања цивилног становништва, при чему он у свом начину деловања следи сопствене принципе, модалитете и облике комуникације са окружењем, као и са онима којима су терористичке поруке упућене. Тероризам се може окарактерисати као безумно, бесциљно и ирационално насиље, односно насиље усмерено против лица која не учествују у оружаним сукобима, а све у сврху остваривања одређених идеолошких, верских или политичких циљева. Као друштвена и политичка појава, али и као процес и систем, тероризам се испољава на различите начине, директно или индиректно, непосредно или посредно, у оквиру друштвене и политичке стварности, што подразумева да мора бити јасно препознатљив и специфичан у односу на друге друштвене и политичке феномене.[9] Важан елемент сваке појаве, било да је реч о

[7] М. Крстић, Улога обавештајног фактора у борби против тероризма, *Цивитас бр. 6. vol 2016*, стр. 125.

[8] М. Симовић, М. Шикман, Тероризам – злочин VS норма, *Криминалистичке теме бр. 1-2, vol. 2017,* стр. 74.

[9] М. Крстић, Улога обавештајног фактора у борби против тероризма, *Цивитас бр. 6. vol 2016*, стр. 97.

друштвеним, политичким појавама или појави тероризма, јесте чињеница да све оне поседују одређену структуру, унутрашње односе и везе, функције, трајање у времену и начин просторног ширења. Сви ти елементи заједно представљају неопходан услов постојања било које појаве, па самим тим и тероризма. Са друге стране, у друштвеним и политичким наукама тероризам се најчешће посматра и дефинише као политичка појава, јер настаје у конкретним политичким околностима, у оквиру одређеног политичког система, са циљем остваривања специфичних политичких интереса и намера. Да би остварила своје потребе, циљеве и интересе, свака организована група спроводи одређену политику, што се огледа у постојању руководства, хијерархијских односа надређених и подређених, као и у чињеници да се чланови групе придржавају утврђених правила ради постизања заједничког циља. Према Веберу, за појам групе није пресудно да ли је реч о заједници или друштву, већ је довољно да постоји вођа, попут главе породице, као и управни апарат, који обезбеђује да поједини чланови делују у правцу очувања поретка групе, односно да постоје лица спремна да у одређеним ситуацијама реагују, што представља гаранцију стабилности тог поретка.

Када се говори о политичким групама, под тим појмом се у основи подразумевају групе људи чији је примарни циљ освајање, задржавање и очување политичке власти, утицаја и моћи, ради управљања општим и посебним друштвеним пословима у оквиру одређеног друштва, заједнице или државе, било на целокупној територији или на њеном делу. У том смислу, политичке групе се организују, формирају сопствене структуре и спроводе бројне активности. Њих карактерише постојање одређеног апарата, јасна подела надлежности, хијерархијски односи, као и примена различитих облика насиља, физичког и психичког, принуде, силе, терора и застрашивања. Политичке групе делују са позиција легитимности и легалности, ослањајући се на традицију, емоционално-афективно прихватање нових узора, вредносно-рационална уверења, позивање на историјска и природна права, било на основу договора или путем наметања и покоравања.[10]

Важан фактор друштвених сукоба јесу политички сукоби, који произилазе из самог појма друштва и друштвених конфликата. Употребом синтагме политички сукоби указује се на њихову везаност за посебну област – сферу политике, политичких процеса и односа, односно управљања општим друштвеним и политичким интересима.

[10] Н. Станковић, *Тероризам и финансирање тероризма,* Европски универзитет, Брчко, 2014, стр. 6-7.

У том смислу, неспорно је да су они повезани са политичком моћи, политичким интересима и политичком влашћу, као и са борбама за њихово освајање или очување у постојећим друштвеним и политичким околностима. Суштина тероризма огледа се у инструментализацији насиља, чији ефекат резонанце проширује круг лица обухваћених страхом и осећајем несигурности за себе, породицу и друге. Користећи криминалне групе за поједине активности, екстремисти на основу остварених успеха предузимају даље кораке усмерене ка изазивању побуне или организују оружани устанак ради отцепљења дела територије од матичне државе и слично. Појединачни терористички акти обухватају широк спектар екстремних активности, те се у такве облике екстремизма и тероризма могу убројати атентати и отмице, саботаже, као и убацивање наоружаних група.[11]

## 1.5. Карактеристике самих терористичких аката

Као акт насиља, тероризам има одређене карактеристике. Пре терористичког напада терористи системски и темељно проучавају навике, обичаје и психологију људи на подручју на коме планирају извршити терористички акт. Код терориста се наглашено валоризира одлучност у реализацији терористичког акта.[12] Терористичке операције су офанзивне и динамичне активности терориста које се састоје од припремања и извођења терористичког напада према унапред одабраној мети напада, а усмерене су на остваривање пројектованих терористичких циљева.

По свом карактеру терористичке операције су увек офанзивне, с обзиром да терористи настоје да избегну оне ситуације које их доводе у дефанзивни положај. На тај начин постиже се ефекат изненађења терористичког напада, а са друге стране, терористи избегавају директну конфронтацију са службама безбедности.[13]

[11] М. Дробац, *Тероризам – цивилизацијска пошаст*, Култура полиса, Београд, стр. 679.

[12] П. Мишевић, *Утјецај тероризма на приљев иноземних директних инветиција – докторска дисертација,* Економски факултет, Ријека, 2016, стр. 30.

[13] Д. Живаљевић, А. Југовић, Тероризам као безбедносни проблем и друштвена девијација*, Журнал за криминалистику и право бр. 1, vol. 2014,* стр. 92.

# 2. ПОЈАМ И КАРАКТЕРИСТИКЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

## 2.1. Појам и одлике компјутерског криминалитета

У нашем закону је прописан посебан кривични поступак за дела компјутерски криминала, у која сврстава кривична дела против безбедности рачунарских података, али и кривична дела против интелектуалне својине, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику, уколико је реч о одређеним, квалификованим облицима извршења к.д. о којима ће више бити речи у наредном делу рада.

Компјутерски криминалитет је једна од најмлађих врста криминалитета, а назива се још и сајбер, односно компјутерски криминалитет, а своје порекло има у међународном праву, а посебно у Ковенцији Савета Европе о сајберкриминалу, која му је дала и назив. Чине га специфична кривична дела против безбедности рачунарских података из главе двадесет седме Кривичног законика Републике Србије (у даљем делу рада КЗ РС), која се начелно деле на кривична дела повреде рачунарских података и кривична дела злоупотребе рачунарских програма. Откривање ових дела, њихово доказивање и процесуирање поверено је посебним полицијским, тужилачким и судским органима, са концентрованом надлежношћу.[14]

Наиме, за поступање у предметима кривичних дела на основу Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[15] надлежно је Више јавно тужилаштво у Београду за територију Републике Србије. У Вишем јавном тужилаштву у Београду образовано је посебно одељење за борбу против високотехнолошког криминала тј. Посебно тужилаштво. Радом Посебног тужилаштва руководи Посебни тужилац за високотехнолошки криминал.

[14] М. Милошевић, *Кривично право,* Факултет за образовање дипломираних правника и дипломираних економиста за руководеће кадрове, Нови Сад, 2013, стр. 108.

[15] Чл. 4 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *„Сл. гласник РС“, бр. 61/2005, 104/2009 10/2023 и 10/2023 - др. закон*

Компјутерски криминалитет је криминалитет који се састоји од кривичних дела чије је средство извршења, или објекат напада компјутер, компјутерски систем, или мрежа. Постоји више дефиниција компјутерског криминалитета, а заједнички елементи готово сваке од њих су: компјутер као средство компјутерског напада или компјутер, компјутерски систем или компјутерска мрежа као циљ криминалног напада. Неопходно знање из области информационих технологија је неопходна вештина у највећем броју случајева како би се извршилац могао бавити овом врстом криминалитета.[16]

Рачунар је електронски уређај који служи за аутоматску обраду и размену података, док се рачунарским системом сматра сваки појединачни уређај или скуп међусобно повезаних, односно зависних уређаја, од којих један или више, на основу унапред дефинисаног програма, врши аутоматску обраду података. С обзиром на то да предмет високотехнолошког криминала могу бити и крађе, потребно је нагласити да се покретном ствари сматрају и рачунарски подаци, као и рачунарски програми. Рачунарски податак представља свако приказивање чињеница, информација или појмова у облику погодном за обраду у оквиру рачунарског система, укључујући и одговарајући програм на основу којег рачунарски систем извршава своје функције.

Рачунарска мрежа представља скуп међусобно повезаних рачунара или рачунарских система који међусобно комуницирају и размењују податке. Рачунарским програмом се сматра уређен скуп наредби који омогућава управљање радом рачунара и извршавање одређених задатака помоћу њега. Рачунарски вирус је програм или други скуп наредби унет у рачунар или рачунарску мрежу, дизајниран да сам себе умножава и утиче на друге програме или податке у систему, додајући свој код једном или више рачунарских података или програма.[17]

[16] С. Николска, Израда и употреба лажних платежних картица као масовни облик компјутерског криминала у Републици Македонији, у: ур. М. Шикман, *Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал*, ВШУП, Бања Лука, 2012, стр. 109.

[17] Чл. 112 КЗ РС

## 2.2. Кривична дела против безбедности рачунарских података

Као што је већ речено, већину дела к.д. компјутерског криминалитета чине к.д. против безбедности рачунарских података, садржаних у глави двадесет седмој од члана 298 до члана 304 КЗ РС. Ова к.д. обухватају:[18]

- оштећење рачунарских података и програма,
- рачунарска саботажа,
- прављење и уношење рачунарских вируса,
- рачунарска превара,
- неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података,
- спречавање и органичавање приступа јавној рачунарској мрежи,
- неовлашћено коришћење рачунара или рачунарске мреже,
- прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података

### 2.2.1. Оштећење рачунарских података и програма

Радња извршења основног облика дела је неовлашћено брисање, измена, оштећење, прикривање или на други начин чињење неупотребљивим рачунарског податка или програма. Прописана санкција за овај вид извршења је алтернативно одређена у виду новчане казне или казне затвора до једне године.

Тежи облик дела постоји уколико је радњом извршења проузрокована штета у износу који прелази четристопедесет хиљада динара и у том случају је прописана санкција казна затвора од три месеца до три године. Други тежи облик дела постоји уколико је радњом извршења проузрокована штета у износу који прелази милион и

[18] Чл. 298-304. КЗ РС

петсто хиљада динара и у том случају је прописана санкција казна затвора од три месеца до пет година.

Такође је и предвиђена мера безбедности одузимања предмета – уређаја и средстава којима је учињено кривично дело (рачунара).[19]

### 2.2.2. Рачунарска саботажа

Радња извршења дела је одређена алтернативно као уношење, брисање, промена, оштећење, прикривање или учињавањем неупотребљивим на било који други начин рачунарског податка или програма или уништавање или оштећење рачунара или другог уређаја за електронску обраду и пренос података.

Ова радња извршења мора бити извршена са намером да се онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте. Прописана санкција за ово к.д. је казна затвора од шест месеци до пет година.[20]

### 2.2.3. Прављење и уношење рачунарских вируса

Радња извршења основног дела је стварање рачунарског вируса са циљем његовог уношења у туђ рачунар или рачунарску мрежу. Прописана санкција за овај вид извршења је алтернативно одређена као новчана казна или казна затвора до шест месеци.

Тежи облик дела постоји уколико се уношењем рачунарског вируса у туђ рачунар или рачунарску мрежу проузрокује штета и у том случају је прописана алтернативно новчана казна или казна затвора до две године.

Предвиђена је и мера одузимања предмета – уређаја и средстава којима је извршено к.д. (рачунар).[21]

[19] Чл. 298 КЗ РС
[20] Чл. 299 КЗ РС
[21] Чл. 300 КЗ РС

### 2.2.4. Рачунарска превара

Радња извршења основног облика дела је уношење нетачног податка, пропуштање уношења тачног податка или прикривање или лажно приказивање на други начин податка и у намери утицања на резултат електронске обраде и преноса података са циљем противправног прибављања себи или другоме противправне имовинске користи или наношења материјалне штете. Прописана санкција за овај вид извршења је новчана казна или казна затвора до три године.

Тежи облик дела постоји уколико је радњом извршења прибављена имовинска корист чији износ прелази четристопедесет хиљада динара и у том случају је прописана санкција, казна затвора од једне до осам година.

Други тежи облик дела постоји уколико је радњом извршења прибављена имовинска корист чији износ прелази милион и петсто хиљада динара и у том случају је прописана казна затвора од две до десет година.

Лакши облик дела постоји уколико је радња извршења извршена само у намери да се друго лице оштети и у том случају је алтернативно прописана санкција новчана казна или казна затвора до шест месеци.[22]

### 2.2.5. Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података

Радња извршења дела је неовлашћено приступање електронској обради података, кршењем мера заштите или неовлашћено укључивање у рачунар или рачунарску мрежу. Прописана санкција за овај вид извршења је новчана казна или казна затвора до шест месеци.

Тежи облик дела постоји уколико  лице сними или употреби податак добијен на начин предвиђен радњом извршења и у том случају је прописана санкција новчана казна или казна затвора до две године.

[22] Чл. 301 КЗ РС

Други тежи облик дела постоји уколико радњом извршења дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице и у том случају је прописана санкција казна затвора до три године.[23]

### 2.2.6. Спречавање и ограничавање приступа јавној рачунарској мрежи

Радња извршења се састоји у неовлашћеном спречавању или ометању приступа јавној рачунарској мрежи и прописана санкција за овај вид извршења је новчана казна или казна затвора до једне године.

Тежи облик дела постоји уколико је радња извршења учињена од стране службеног лица у вршењу службене делатности и у том случају је прописана санкција казна затвора до три године.[24]

### 2.2.7. Неовлашћено коришћење рачунара или рачунарске мреже

Радња извршења се састоји у неовлашћеном коришћењу рачунарске услуге или рачунарске мреже са намером да се себи или другом прибави противправна имовинска корист. За овај вид извршења је прописана санкција новчана казна или казна затвора до три месеца.

Кривично гоњење за ово дело предузима се по приватној тужби.[25]

### 2.2.8. Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података

Радња извршења је производња, продаја, набавља ради употребе, увожење, дистрибуција или стављања на располагање на други начин уређаја и рачунарских

[23] Чл. 302 КЗ РС
[24] Чл. 303 КЗ РС
[25] Чл. 304 КЗ РС

програма пројектованих првенствено у сврхе извршења кривичног дела против безбедности рачунарских података, или рачунарске шифре или сличне податке путем којих се може приступити рачунарском систему као целини или неком његовом делу са намером да буде употребљен у извршењу неког од кривичних дела против безбедности рачунарских података. Прописана казна за ово дело је казна затвора од шест месеци до три године.

Лакши облик дела прописан је за поседовање наведених средстава и прописана казна за овај вид извршења је новчана казна или казна затвора до једне године. Предвиђена је и мера одузимања предмета којима је извршено кривично дело.[26]

## 2.3. Кривична дела чији је компјутерски криминал елемент бића кривичног дела

Предмет истраживања овог дела рада биће к.д. која спадају у домен високотехнолошког криминала, али не улазе у к.д. против безбедности рачунарских података. Наиме, високотехнолошки криминал је погодан начин извршења не само ове групе к.д., већ и к.д. против полне слободе и ауторских права у одређеним случајевима одређеним околностима,[27] као што је то већ речено.

### 2.3.1. Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију

К.д. приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију може ући у домен високотехнолошког криминала, имајући у виду да је радња извршења продавање, приказивање или учињавање доступним малолетном лицу текстова, слика, аудио-визуелних или других предмета порнографске садржине или порнографске представе (за шта ће запрећена новчана казна, односно казна затвора до шест месеци), као и искоришћавање малолетника за производњу слика, аудио-визуелних или других

[26] Чл. 304а КЗ РС

[27] М. Милошевић, *Кривично право,* Факултет за образовање дипломираних правника и дипломираних економиста за руководеће кадрове, Нови Сад, 2013, стр. 108.

предмета порнографске садржине или за порнографску представу (за шта је запрећена казна затвора од шест месеци до пет година. односно уколико је дело извршено према детету, од шест месеци до три године, а за дело из става 2. од једне до осам година).

Кажњиво је и електронским путем излагање и чињење доступним слике, аудио-визуелне или друге предмете порнографске садржине настале искоришћавањем малолетног лица и у том случају је предвиђена казна затвора од три месеца до три године. Посебан облик је када се помоћу средстава информационих технологија свесно приступи сликама, аудио-визуелним или другим предметима порнографске садржине насталим искоришћавањем малолетног лица и у овом случају је предвиђена новчана, односно казна затвора до шест месеци. Предвиђено је и обавезно одузимање предмета којим су дела извршена, односно електронског уређаја у конкретном случају (рачунара).[28]

### 2.3.2. Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу

Исти члан, ставом б  нормира да је к.д. искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу дело којим се учинилац, користећи рачунарску мрежу или комуникацију другим техничким средствима договори са малолетником састанак и појави се на договореном месту ради састанка. У том случају се извршилац кажњава кумулативно, затвором од шест месеци до пет година и новчаном казном.

Тежи облик дела постоји уколико је радња извршења уперена према детету и у том случају је прописана санкција казна затвора од једне до осам година. [29]

[28] Чл. 185 КЗ РС

[29] Чл. 185б КЗ РС

### 2.3.3. Неовлашћено искоришћавање ауторског дела или предмета сродног права

Такође је инкриминисана и радња извршења к.д. неовлашћено искоришћавање ауторског дела или сродног права, а део који се односи на високотехнолошки криминал, тиче се неовлашћеног објављивања, снимања, умножавања, или на други начин јавног саопштавања рачунарског програма или базе података. Прописана санкција за ово дело је затвор до три године. Инкриминисано је и само држање рачунарског програма или базе података. Рачунарски програм, односно база података је у овом случају објекат извршења к.д.[30]

## 2.4. Обим, динамика и појавни облици извршења кривичних дела компјутерског криминала у Републици Србији

У следећој табели се може видети удео к.д. против рачунарских података у Републици Србији за период 2009-2018, у односу на укупни криминалитет.

Табела 1. Поређење броја пријављених к.д. против рачунарских података и укупног броја к.д. у Републици Србији за период 2009-2018[31]

| | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|---|---|---|
| **РЕПУБЛИКА СРБИЈА** | **100026** | **74279** | **88207** | **92879** | **91411** | **92600** | **108759** | **96237** | **90348** | **92874** |
| Кривична дела против живота и тела | 4912 | 3381 | 3908 | 3923 | 3734 | 3268 | 3818 | 3451 | 3278 | 3084 |
| Кривична дела против слобода и права човека и грађанина | 1501 | 1786 | 2470 | 2676 | 2850 | 2975 | 3874 | 4046 | 4052 | 4264 |
| Кривична дела против изборних права | 29 | 22 | 37 | 34 | 33 | 23 | 8 | 30 | 17 | 36 |
| Кривична дела против права по основу рада | 279 | 165 | 176 | 145 | 157 | 177 | 212 | 193 | 202 | 220 |
| Кривична дела против части и угледа | 85 | 115 | 58 | 53 | 39 | 47 | 53 | 41 | 37 | 65 |
| Кривична дела против полне слободе | 448 | 387 | 414 | 372 | 320 | 252 | 352 | 367 | 338 | 435 |
| Кривична дела против брака и породице | 5617 | 4657 | 5868 | 6182 | 6268 | 5914 | 7891 | 10190 | 10561 | 10729 |
| Кривична дела против интелектуалне својине | 294 | 161 | 154 | 167 | 178 | 115 | 98 | 85 | 57 | 81 |
| Кривична дела против имовине | 47343 | 31618 | 39742 | 45291 | 45899 | 50303 | 58741 | 44000 | 40443 | 40595 |
| Кривична дела против привреде | 3131 | 2479 | 2957 | 3221 | 3397 | 3347 | 3526 | 3333 | 2939 | 2767 |
| Кривична дела против здравља људи | 4490 | 4052 | 3409 | 3603 | 3464 | 3161 | 3731 | 3687 | 4574 | 5546 |
| Кривична дела против животне средине | 2081 | 1568 | 1789 | 1841 | 1996 | 2148 | 2205 | 2507 | 2187 | 2550 |
| Кривична дела против опште сигурности људи и имовине | 1354 | 807 | 1128 | 1305 | 1210 | 1264 | 1284 | 1220 | 1135 | 1285 |
| Кривична дела против безбедности јавног саобраћаја | 8140 | 5265 | 6447 | 7186 | 7773 | 7439 | 7856 | 7805 | 7724 | 8437 |
| Кривична дела против рачунарских података | 45 | 20 | 22 | 15 | 28 | 9 | 14 | 16 | 20 | 11 |
| Кривична дела против уставног уређења и безбедности | 87 | 87 | 51 | 89 | 39 | 38 | 31 | 62 | 13 | 28 |
| Кривична дела против државних органа | 1414 | 758 | 1894 | 4045 | 3914 | 2938 | 3713 | 3702 | 2659 | 2474 |
| Кривична дела против правосуђа | 993 | 793 | 898 | 946 | 821 | 865 | 1114 | 1039 | 994 | 974 |
| Кривична дела против јавног реда и мира и | | | | | | | | | | |

[30] Чл. 199. Чл.

[31] Републички завод за статистику, https://publikacije.stat.gov.rs/G2019/Pdf/G20195653.pdf, Приступљено: 01.12.2025. у 11:00h

Такође се може видети обим ових дела у временском периоду од девет година. Јасно се може уочити да од око 100.000 к.д. која се пријаве годишње, само 9-45 буду к.д. против безбедности рачунарских података, па је логичан закључак да велики део ових к.д. остане непријављен.[32] Такође се не може уочити тенденција раста ове групе кривичних дела, што је такође нелогично, имајући у виду технолошки напредак и повећање броја уређаја који могу бити како објеката напада, тако и објекти заштите ових к.д.

У следећој табели се може видети удео пријављених к.д. искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу у к.д. против полне слободе у Републици Србији за 2018 и јасно се може закључити да само 2 од укупно 435 к.д. против полне слободе припадају овој групи к.д. И овде се претпоставља да је реч о великој тамној бројци криминалитета, односно да се ова дела не пријављују.

Табела 2. Удео пријављених к.д. искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу у к.д. против полне слободе у Републици Србији за 2018[33]

| **КД против полне слободе** | **435** | **385** | **14** | **132** | **29** | **20** | **1** | **6** | **76** | **1** |
|---|---|---|---|---|---|---|---|---|---|---|
| Силовање | 76 | 71 | 3 | 23 | 1 | 3 | - | - | 19 | - |
| Обљуба над немоћним лицем | 7 | 7 | - | 1 | - | - | - | - | 1 | - |
| Обљуба са дететом | 34 | 32 | - | 7 | - | 4 | - | - | 3 | - |
| Обљуба злоупотребом положаја | 1 | 1 | - | - | - | - | - | - | - | - |
| Недозвољене полне радње | 165 | 143 | 3 | 53 | 11 | 9 | 1 | 1 | 31 | - |
| Полно узнемиравање | 105 | 87 | 2 | 39 | 15 | 2 | - | 5 | 17 | 1 |
| Посредовање у вршењу проституције | 13 | 12 | 3 | 2 | 1 | - | - | - | 1 | - |
| Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу | 2 | 2 | - | - | - | - | - | - | - | - |

У следећој табели се може видети анализа к.д. против безбедности рачунарских података у Републици Србији за 2018. Од познатих 11 учинилаца највише је за к.д. оштећење рачунарских података (7), а постоје дела која нису ни једном пријављена, попут неовлашћеног приступа заштићеном рачунару, рачунарској мрежи и електронској обради података.

Табела 3. Анализа к.д. против безбедности рачунарских података у Републици Србији за 2018.[34]

[32] Тамна бројка криминалитета је разлика између стварног броја извршених кривичних дела и пријављених кривичних дела

[33] Републички завод за статистику, https://publikacije.stat.gov.rs/G2019/Pdf/G20195653.pdf, Приступљено: 02.12.2025. у 19:00h

[34] Републички завод за статистику, https://publikacije.stat.gov.rs/G2019/Pdf/G20195653.pdf, Приступљено: 03.12.2025. у 13:00h

| | Укупно | Познати учиниоци | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | укупно познати | жене | одбачена кривична пријава | | | | | | прекинута истрага |
| | | | | свега | одлагање кривичног гоњења због испуњења одређених обавеза | дело није кривично дело | застарелост | трајно искључено гоњење | не постоје основи сумње, нецелисходност кривичног гоњења | |
| **КД против безбедности рачунарских података** | **11** | **7** | **1** | **3** | **3** | **-** | **-** | **-** | **-** | **-** |
| Оштећење рачунарских података и програма | 3 | 2 | 1 | 2 | 2 | - | - | - | - | - |
| Рачунарска превара | 2 | 2 | - | - | - | - | - | - | - | - |
| Неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података | 4 | 2 | - | - | - | - | - | - | - | - |
| Неовлашћено коришћење рачунара или рачунарске мреже | 2 | 1 | - | 1 | 1 | - | - | - | - | - |

## 2.5. Узроци, услови и поводи извршења компјутерског криминалитета у Републици Србији

Основни разлози који узрокују извршење ових дела су могућност брзе зараде, где се учиниоци воде лукративним побудама и приступају извршењу ових дела, као и доступност неопходне технологије и алата (средстава извршења) великом броју људи, а не само стручњацима за информатику. За непосредно извршавање криминалних активности професионалци могу ангажовати велики број неквалификованих појединаца

Такође обиму извршења ових дела погодује повећање броја корисника интернета у неразвијеним регионима света, као и велики број потенцијалних богатих жртава у развијеним регионима, који је углавном непроменљив. На обим ове врсте к.д. утиче и све већа аутоматизација нових алата и интернета.

Даљи развој нелегалних онлајн тржишта, употреба сигурних сервера и све сложенијих система заштите сопствених ресурса од стране криминалних структура, сукоби између великих организованих група високотехнолошког криминала (ВТК), раст броја напада заснованих на социјалном инжењерингу, електронски напади на критичну инфраструктуру као што су снабдевање, саобраћај и услуге преноса података, као и хаковање уређаја повезаних на интернет, представљају само нека од предвиђања која се односе на будући развој високотехнолошког криминала.[35]

[35] А. Ђукић, Организовани високотехнолошки криминал, појам, развој и карактеристике, *Војно дело бр. 3, вол. 2018,* стр. 128-156.

# 3. КОМПЈУТЕРСКИ ТЕРОРИЗАМ

## 3.1. Појам компјутерског тероризма

Термин сајбер тероризам се у све већој мери користи у савременом друштву како би се означили различити облици противправног деловања, као што су крађа података и хаковање, планирање терористичких активности, изазивање насиља или напади на информационе системе, односно рачунарске мреже. Према званичној дефиницији коју су формулисали стручњаци Центра за заштиту националне инфраструктуре Сједињених Америчких Држава (National Infrastructure Protection Center – NIPC), сајбер тероризам се одређује као криминално дело извршено путем рачунара, које за последицу има насиље, смрт и/или разарање, при чему се ствара осећај терора са циљем да се влада примора на промену своје политике.[36]

Појам сајбер тероризма обухвата политички мотивисане нападе на информационе системе, рачунарске програме и податке. Специфичност сајбер тероризма произлази из места напада (кибернетички простор), употребљених средстава напада (информациона технологија) и циљева напада (информациони системи, рачунарски програми и подаци), док су мотиви деловања једнаки онима код класичног тероризма (утицај на државу и/или међународну организацију, изазивање застрашености грађанства, хаоса итд.).[37]

Више аутора је настојало да прецизно одреде појам сајбер тероризма. Марк Полит (Marc Pollitt) истиче да сајбер тероризам представља унапред планиран, политички мотивисан напад на информације, рачунарске системе, програме и податке, који изазива страх и насиље код цивилних мета. Позната стручњакиња за сајбер тероризам, Дороти Денинг (Dorothy Denning), дефинише га као недозвољени напад или претњу нападом на рачунаре, рачунарске мреже или сачуване податке с циљем да се заплаши влада или њени грађани ради остваривања политичких или других циљева. Џејмс Луис (James Lewis) из Центра за стратегијске и међународне студије (Center for Strategic and International Studies) и експерт за сајбер тероризам Маркус Хендршот

[36] Д. Вулетић, *Одбрана од претњи у сајбер простору,* Институт за стратегијска истраживања, Београд, 2011, стр. 27.

[37] Р. Соколовић Р, *Електронски надзор комуникација у борби против тероризма и људска права и слободе грађана – докторска дисертација*, Правни факултет, Ниш, 2010, стр. 52.

(Marcus Hendershot) дефинишу сајбер тероризам као употребу рачунарских мрежа и алата за прекид рада критичних националних инфраструктура или за приморавање и застрашивање владе и грађана. Поред тога, одређени стручњаци за информациону безбедност сматрају да напади на рачунаре и мреже могу бити класификовани као сајбер тероризам ако су њихови ефекти довољно деструктивни или пореметилачки да изазову страх сличан оном који производи физички акт тероризма.[38]

Сајбер тероризам представља посебан облик тероризма у којем се савремене информационо-комуникационе технологије користе било као средство, било као мета напада, ради остваривања политичких циљева. У оквир сајбер тероризма убрајају се незаконити напади и претње нападом на рачунаре, рачунарске мреже и податке који се у њима чувају, с циљем застрашивања или принуде владе или њених грађана ради остваривања политичких или друштвених циљева. Домаћа литература о сајбер тероризму је оскудна, а термин се први пут појављује крајем двадесетог века. Дебра Шиндер (Deborah Schneider) у својим дефиницијама посебно истиче разорност последица оваквих напада. Напади на рачунаре и рачунарске мреже могу се сматрати сајбер тероризмом ако су њихови ефекти довољно деструктивни да изазову страх сличан оном који производи физички терористички акт.[39]

Сајбер тероризам представља приближавање сајбер простора и тероризма и односи се на незаконите нападе и претње напада на рачунаре, мреже, а подаци који се налазе у њему, тежећи да застраше или присиле владу или своје људе у циљу политичких или друштвених промена. Даље, да би се напад квалификовао као сајбер тероризам, требало би да доведе до насиља против лица или имовине, или бар да изазове довољно штете или страха.

Као и конвенционални тероризам, сајбер тероризам настоји да промени мишљење циљане публике, међутим, у односу на њега, он може да користи различите начине деловања у ту сврху. Главни мотиви за терористичко насиље уопште су политичке, идеолошке или верске природе и ако сајбер тероризам заиста представља

[38] Д. Вулетић, *Одбрана од претњи у сајбер простору,* Институт за стратегијска истраживања, Београд, 2011, стр. 28.

[39] И. Лукнар, Злоупотреба информационих и комуникационих технологија: појам и уређење у Републици Србији, *Политика националне безбедности бр. 22, вол. 2022*, стр. 181.

приближавање тероризма и сајбер простора, онда ће се исти мотиви примењивати за њега, само у другом медију. [40]

Велики број различитих дефиниција сајбер тероризма указује на сложеност и вишедимензионалност овог феномена. На основу анализе релевантне литературе која се бави сајбер тероризмом, овај појам се може одредити као криминална активност у сајбер простору чији је циљ застрашивање владе или њених грађана ради остваривања политичких циљева.

Маура Конвеј (Maura Conway) предлаже скалу која активности терористе на Интернету разврстава на употребу, злоупотребу, офанзивну употребу и сајбер тероризам. Са друге стране, у стручној јавности је углавном прихваћена класификација која издваја четири основна начина деловања сајбер терористе: одбијање, обману, уништавање и експлоатацију. То подразумева неовлашћен улазак у информационе системе или рачунарске мреже ради онемогућавања њиховог рада, уношење лажних података или злонамерних програма, уништавање система, као и прикључивање на систем у циљу прибављања поверљивих информација.

Кларк Стејт (Clark State), извршни директор Института за истраживања и хитан одговор у Чикагу, упозоравао је да припадници појединих радикалних исламистичких организација настоје да развију мреже хакера, које би у будућности могле бити ангажоване у сајбер нападима. Према приручнику „Војни водич за тероризам у двадесетпрвом веку“, сајбер тероризам представља један сегмент ширих сајбер операција, док други сегмент обухвата сајбер подршку, као што су планирање, регрутовање и пропаганда.

У оквиру сајбер тероризма, рачунарска мрежа може имати улогу оружја, средства комуникације или циља напада. Према истом извору, деструктивни напади на рачунарске мреже могу бити изведени са намером да појачају ефекте физичких терористичких напада.[41]

Пет основних одредница сајбер тероризма су следеће:[42]

---

[40] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016,* стр. 98-100.

[41] Д. Вулетић, *Одбрана од претњи у сајбер простору,* Институт за стратегијска истраживања, Београд, 2011, стр. 29.

[42] И. Лукнар, Злоупотреба информационих и комуникационих технологија: појам и уређење у Републици Србији, *Политика националне безбедности бр. 22, вол. 2022*, стр. 182.

- употреба информационих/компјутерских технологија као оружја (а не само као логистичке подршке, средства комуникације или мете)
- политичка мотивација
- оријентација ка симболици/спектакуларности/публицитету
- значајна материјална штета и/или људске жртве, или претња таквим последицама
- ширење страха већих размера

## 3.2. Разлика компјутерског тероризма од сајбер напада

Иако многи тврде да је сајбер-тероризам само још једно средство за пропаганду и смицалице владе за креирање страха у јавности, било је неколико случајева који јасно показују да је претња је веома реална и способност да се спроведе акт је заиста остварива. Сајбер тероризам има неколико различитих карактеристика и оне помажу да се боље разумеју разлике на танкој линији између сајбер терористичког напада у односу на сајбер напад или активности хакера.

Најмање половина свих рачунарских инцидената нису узроковани намерно, што подразумева не само несреће већ и ненамерне последице рањивости. Та рањивост произилази из злоупотребљене конфигурације мрежа, софтверских грешака, неправилно или лоше техничке или административне примене информационе безбедносне политике, неадекватно обучени рачунарски корисници и људска грешка.[43]

Док су сајбер инциденти мотивисани политичким и социјалним разлозима, поставља се питање да ли су заиста довољно штетни или застрашујући да би се оквалификовали као сајбер тероризам? Док многи хакери поседују знање, вештине и алате да нападну компјутерске системе, они генерално немају мотивацију да доведу до насиља или озбиљне економске или социјалне штете.

Осим тога, успешан сајбер терористички догађај би могао да захтева више предуслова него знања - средства која су у суштини једном стечена, доступна су

[43] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016.,* стр. 99.

власнику и може их користити изнова. На тај начин, било би могуће да такав амбијент омогући стварање потпуно нових терористичких група: нема новчаних средстава неопходних за реализовање акција, а чланови би могли да се организују доста брзо и лако побегну у анонимност сајбер простора.[44]

Оно што разликује сајбер тероризам од осталих врсти сајбер напада је политички мотив. Сајбер терористи неретко прибегавају извршењу осталих врсти сајбер напада како би прибавили неку корист за себе, која им даље омогућава једноставнији и бржи долазак до коначног циља. Основне одреднице којима се прецизно дефинише сајбер тероризам и јасно разликује од осталих сајбер злоупотреба су:[45]

- правни оквир – разликује се по намери извршења дела, као што су планирање или упућивање претњи;
- коришћење сајбер простора за спровођење напада, при чему сајбер простор истовремено може представљати и мету, односно циљ напада;
- подразумева злонамерно деловање које укључује одређени облик насиља са тежњом да се остваре далекосежни психолошки ефекти на циљану публику;
- намера извршења усклађена је са дугорочним циљевима терориста или терористичких група, као што су настојање ка друштвеним или политичким променама и утицај на процес политичког одлучивања.

## 3.3. Специфичности компјутерског тероризма у односи на конвенционални тероризам

Предности које информационе и комуникационе технологије пружају својим корисницима истовремено омогућавају терористима да прибегну разним облицима злоупотреба ИКТ. Пре свега, ово обухвата: 1) могућност корисника да сачува своју анонимност у сајбер простору користећи креирани, односно виртуелни (сајбер)

[44] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016.,* стр. 100.

[45] И. Лукнар, Злоупотреба информационих и комуникационих технологија: појам и уређење у Републици Србији, *Политика националне безбедности бр. 22, вол. 2022*, стр. 182.

идентитет; 2) релативно мали однос између штете причињене у реалном (физичком) свету и напора, односно конкретних улагања потребних за извршење сајбер напада; 3) за извршење оваквих дела, поред знања из ИТ области и технолошке опремљености, нису потребне додатне организационе структуре или велики ризици. Управо због ових предности, сајбер тероризам превазилази традиционалне облике тероризма, што га чини актуелним и релевантним феноменом у савременом друштву.[46]

Терористи су се преселили у сајбер простор да олакшају традиционалне облике тероризма као што је нпр. бомбардовање. Пропустљивост сајабер простора знатно олакшава тероризам у њему и овај простор се разликује у том погледу од физичких граница где нпр. имигрициони службеници контролишу улазак странаца и њихов улазак у земљу, док цариници контролишу увезену робу како би се утврдило да није кријумчарена. Сајбер простор може да се користи да победи овај систем и избегне контроле и инспекције и терористи у различитим земљама могу да размењују електронску пошту са мало страха да ће бити праћени и ухваћени.[47]

Средства и знања стечена од стране сајбер терористе су власнику увек доступна и он их може користити више пута. То ствара потпуно нов амбијент терористичких група: нема новчаних средстава неопходних за реализовање акција, а чланови могу да се организују доста брзо и лако побегну у анонимност сајбер простора.

Повећање информација, комуникација и комуникационих технологија не утичу само на терористичке групе. Информација представља нову крв међународног система и много промена се десило као резултат ширења информационе инфраструктуре. Данас, западна друштва зависе у скоро сваком аспекту живота од рачунарске комуникације. Компјутерски системи контролишу скоро све што је потребно за нашу свакодневницу и наше планове за ванредне ситуације. Сајбер тероризам  је сличан по својим карактеристикама и са другим раније поменутим облицима тероризма. Као и конвенционални настојаће да промени мишљење циљане публике, међутим, може да користи различите начине деловања у ту сврху.

Уколико сајбер тероризам заиста представља приближавање тероризма и сајбер простора, онда ће се исти мотиви примењивати за њега, само у другом медију. Многи

[46] И. Лукнар, Злоупотреба информационих и комуникационих технологија: појам и уређење у Републици Србији, *Политика националне безбедности бр. 22, вол. 2022*, стр. 181.

[47] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016,* стр. 99.

од веб локација постављених од стране терористичких група се служе политичким циљевима, идеологијом или религијом и заиста, сајбер простор нуди одређене предности над физичком медијуму. За почетак омогућава сајбер терористима погодности за удаљене и анонимне операције и такође, избегава потребу за руковањем физичким оружјем и експлозивом, као и пратећим ризицима од спектакуларне пропасти пропалог покушаја када бомбе експлодирају прерано. Осим офанзивних операција терориста, они могу ефикасно да користе сајбер простор за безбедне комуникације.[48]

## 3.4. Покушаји борбе против компјутерског тероризма на глобалном плану

У националним законодавствима још увек није развијен концепт сајбер тероризма. Исто важи и за међународно кривично право. Ни у једној од антитерористичких конвенција Уједињених нација не налазимо појам сајбер тероризма, иако прве међународне иницијативе за универзалним одређењем тог појма датирају још од друге половине деведесетих година XX века. Почетком октобра 1998. године, руски министар спољних послова упутио је службени захтев тадашњем Главном секретару Уједињених нација да та организација размотри примереност доношења међународне конвенције којом би се успоставила контрола над „нарочито опасном појавом информацијског тероризма и криминалитета, укључујући и стварање међународног система за праћење претњи упућених сигурности глобалних информационих и телекомуникацијских система“. Премда је та иницијатива стављена на дневни ред 54 седнице Опште скупштине Уједињених нација, на нивоу глобалне светске организације до данас није донесен правно обавезујући документ који би регулисао сајбер тероризам.

Расправа око потребе доношења посебног међународног инструмента за сузбијање сајбер тероризма вођена је и у оквиру Мултидисциплинарне групе против тероризма Већа Европе (GMT) основане одлуком Одбора министара те организације убрзо после напада на САД, 11. септембра 2001. године. У свом извештају о напретку GMT је закључио како, с обзиром на постојеће стање, није реално очекивати рад на

[48] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016,* стр. 100.

припреми Другог додатног протокола уз Конвенцију о кибернетичком криминалу, који би регулисао питања значајна за превенцију и сузбијање кибернетичког тероризма у државама странкама. Уместо тога, наводи се у Извештају, потребно је појачати напоре у вези са ратификацијом Конвенције о кибернетичком криминалу од стране што већег броја држава, како би она што пре ступила на снагу.

Доношење међународног правно обавезујућег инструмента (конвенција, протокол), којим би се регулисали различити аспекти кибернетичког тероризма (дефиниција, међународна сарадња итд.), актуализовано је кроз Одбор стручњака против тероризма Савета Европе (CODEXTER.) , чије се активности настављају на већ споменути GMT и посебно кроз Одбор за Конвенцију о кибернетичком криминалу (T-CY). Такав развој догађаја у потпуности је разумљив, ако се има у виду да су се околности од краја 2001. и почетка 2002. године до данас значајно промениле. Наиме, Конвенција о кибернетичком криминалу с додатним протоколом ступила је на снагу, а у њеном спровођењу уочена је потреба да се одређене констатоване правне празнине, које се односе на кибернетички тероризам, допуне кроз доношење новог међународног инструмента.[49]

У првом реду, сасвим је сигурно да Конвенција о кибернетичком криминалу не може ефикасно да одговори новој претњи кибернетичког тероризма. У тој конвенцији, наиме, није дефинисана терористичка намера већ само у члану 2 „нечасна намера“ (dishonest intent). Тај појам није довољно прецизан, да би се под њега могла подвести терористичка намера која увек иде за остваривањем одређених политичких циљева, односно изазивања застрашености грађанства, изазивања несигурности, хаоса и слично. Осим тога, Конвенција не предвиђа механизме којима би се некажњивост свела на најмању могућу меру.

То је очигледно, између осталог, и из одредбе члана 24. Конвенције, која није толико стриктна као у антитерористичким конвенцијама. Коначно, у Конвенцији нема одредбе ни о ограничењу изузетка политичког казненог дела, што може да успори, а у неким ситуацијама и у потпуности да блокира међународну сарадњу. Други додатни протокол уз Конвенцију о кибернетичком криминалу је донет 2021. године, али он се бави међународном сарадњом и доказима и не уводи дефиницију сајбер тероризма нити

[49] Р. Соколовић, *Електронски надзор комуникација у борби против тероризма и људска права и слободе грађана – докторска дисертација*, Правни факултет, Ниш, 2010, стр. 53.

га материјално регулише. Постојеће антитерористичке конвенције не би било могуће применити на кибернтички тероризам. Разлог томе је чињеница да дефиниције кривичних дела из конвенцијског каталога експлицитно или имплицитно одређују терористичко дело као акт насиља, а како је у виртуелном свету, за разлику од физичког, насиље по природи ствари искључено, тако кибернетички тероризам не би било могуће подвести под тако дефинисане забрањене поступке. Све то указује на потребу да се приступи разматрању могућности доношења једног међународног правно обавезујућег инструмента (конвенција, протокол), којим би се нормативно регулисали најважнији аспекти сузбијања сајбер тероризма.[50]

Након сазнања да се интернет користи за врбовање нових чланова, за ширење пропаганда, обезбеђивање материјалних средстава, имамо сајбер нападе на државе, владине институције, директну угроженост грађана нападом на владине секторе, хаковање банковних рачуна и информација од значаја, постајемо свесни да борба са тероризмом преузима један веома софистициран тип сукоба у коме више нема садржаја који би се поистовећивали са традицијом ни у најмањем случају. Сама чињеница да су софтверски системи умрежени и да су информације расположиве у сваком тренутку, саме владе и државне институције излаже опасности од напада који адекватним радом служби безбедности може бити предупређен. Ово захтева веома динамичну и константну борбу не само са хакерима и сајбер терористима, већ и са све новијим технологијама које освајају свет незапамћеном брзином.[51]

[50] Р. Соколовић, *Електронски надзор комуникација у борби против тероризма и људска права и слободе грађана – докторска дисертација*, Правни факултет, Ниш, 2010, стр. 54.

[51] С. Клисарић, Сајбер тероризам као окидач све интензивније потребе за безбедност система од опасности која долази са интернета, *Мегатренд Ревија бр. 18. вол. 2021,* стр. 252.

# 4. ОБЛИЦИ ДЕЛОВАЊА САЈБЕР ТЕРОРИСТА

Сајбер простор терористима нуди много потенцијала и представља алат за регрутовање, радикализацију, пропаганду и прикупљање средстава, као и пружање брзе и једноставне команде и контроле. С обзиром на једноставност употребе и све веће ослањање на развијена друштва на интернету, могућност за терористичку експлоатацију се свакодневно шири. Чак и пре експанзије интернета, примећено је да је комуникациона револуција 20. века значајно променила лице тероризма. После догађаја од 9/11 и антитерористичке кампање која је уследила, велики број терористичких група се преселио у сајбер-простор , креирајући хиљаде сајтова преко којих промовишу своје поруке и активности. Социјални медији се разликују од традиционалних и конвенционалних у многим аспектима, као што су интерактивност, достизање задовољавајуће фреквенције, употребљивост, непосредност.[52]

Сајбер тероризам може да се реализује на више различитих нивоа где је најједноставнији напад једне особе на другу преко рачунара. Али различите методе напада циљају различите рањивости и укључују различите врсте оружја, од којих неке могу бити у оквиру постојећих могућности неких терористичких група.

Сајбер терористи користе интернет за комуникацију, координацију догађаја и унапређење њиховог програма и иако таква активност не представља сајбер тероризам у ужем смислу, показује да терористи имају извесну надлежност и примат користећи нове информационе технологије.

Уколико су терористи у стању да се адекватно обуче и стекну одговарајуће технолошке вештине, то би било опасно за цео свет. Да би се разумела потенцијална опасност од сајбер-тероризма, морају се узети у обзир два фактора: прво, да ли постоје циљеви који су рањиви на нападе који могу довести до насиља или тешких повреда и друго, да ли постоје актери са способношћу и мотивацијом да их спроведу.[53]

Свет сајбер технологије постао је поприште идеалне терористичке манифестације јер на основу свих расположивих информација терористи не морају да

[52] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016,* стр. 101.

[53] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016,* стр. 98-99.

улажу ни време, ни новац у операционе послове на терену како би сакупили потребне информације. Њихов простор је свет рачунара, интернета и нових технологија уз помоћ којих остварују своје планове. Веома софистицираном технологијом сајбер терористи нису само сакупљачи великог броја информација, нити им интернет служи само за размену идеологија, врбовање и новчане трансакције.

Они су захваљујући овладавању сајбер светом приступили једном веома озбиљном пољу знања ком владају и са ког маскирани попут неког другог програма или обичне алатке у некој од мрежа интернета могу да допру до оних информација до којих им је циљ да прођу, истовремено изазивајући напад несагледивих размера.

Уколико укуцате сајбер нападе уживо бићете дословно запрепашћени колико напада се дешава у секунди. У само једном дану имамо преко 11 милиона сајбер напада широм света чији се број сваке стотинке увећава, па је јасно је да је овај вид сукоба постао дефинитивно најдоминантнији. Наиме, никада пре у историји човечанства није забележен толики број сукоба чиром света у једном дану. Овај податак јасно указује на ескалацију сајбер тероризма као озбиљног и драматичног оружја терориста.

Највећи број сајбер напада је извршен на образовање и на државне институције, а као државе које су претрпеле највеће нападе набројане су: Непал, Боливија, Монголија, Чиле и Грузија. Посматрајући хакерске нападе уживо, стиче се утисак да се посматра некаква видео игра, а не реалан терористички напад пред нашим очима. Разлог за такав утисак је надреалност фреквенције напада који се остварују сваке стотинке широм света.

Интересантно је истаћи да су очито највише осетљиве државе са најслабијом сајбер одбраном и да хакерски напади таргетирају највише оне владе које немају адекватну одбрану. Непрестано се врше напади између најмоћнијих држава, али већина тих напада се не остварује управо због снажне одбране сајбер простора тих држава. Тероризам је нашао готово неуништиво поље са ког може да дела не укидајући своју разорну моћ и не померајући се од својих идеологија, напротив користећи технологију која је настала у Западним државама као средство против ње.[54]

[54] С. Клисарић, Сајбер тероризам као окидач све интензивније потребе за безбедност система од опасности која долази са интернета, *Мегатренд Ревија бр. 18, вол. 2021,* стр. 253.

Имајући ове податке у виду, веома је неодговорно веровати да терористи нису довољно едуковани или технички подупрти да организују нападе који угрожавају безбедност сајбер простора. Ако у једном дану имамо 300 милиона напада, нека је само 1% тих напада од стране озлоглашених терористичких организација, то је 3 милиона напада. Дакле, може ли ико да замисли 3 милиона терористичких напада у истом дану? То је са овом технологијом данас могуће само у сајбер простору и терористи како ствари стоје веома добро користе тај простор за своје намере.

Веома интензиван допринос сајбер тероризму и уопште развоју сајбер технологија унутар терористичког испољавања, тачније, овладавњу сајбер технологија драстично су помогли исламисти унутар Европе који су направили велики пробој у овој области активирајући значајан и алармантан број нових сајбер терориста. Ову чињеницу треба разумевати у контексту оне стварности која нам је свима позната, а тиче се социјализације унутар сајбер простора. У том свету потрага за садржајима од интереса далеко је лакша од исте на било ком другом месту са ког би се потражиле похрањене информације.

Дакле, сама структура сајбер простора омогућава развој сајбер терористе од политичких ставова, до праћења свих дешавања, самоедукације и развоја сајбер вештина, до финалног извођења напада. Сада, по први пут у историји имамо незапамћен феномен да обичан цивил може да постигне потпуно самостално оно знање неопходно за сајбер напад, да иста та особа може да прикупи информације и коначно потпуно самостално изврши сајбер тероризам на сајбер простору не померајући се са свог радног простора.

Оваква чињеница упућује на логичну забринутост јер онда када је непријатељ несагледив, он је онда свуда претпостављен. А када је опасност на сваком кораку, потребна су огромна материјална и ресурсна средства да би се омогућила адекватна армија сајбер војника који ће штитити системе непрекидно.[55]

[55] С. Клисарић, Сајбер тероризам као окидач све интензивније потребе за безбедност система од опасности која долази са интернета, *Мегатренд Ревија бр. 18, вол. 2021,* стр. 254.

## 4.1. Регрутовање чланова

Регрутовање у сајбер терористичким групама најчешће се одвија путем интернета и дигиталних платформи. Онлајн простори омогућавају анонимност, брзу комуникацију и приступ великом броју потенцијалних кандидата широм света. За разлику од класичних терористичких организација, где је физички контакт често неопходан, сајбер терористи могу да привуку, идеолошки обликују и укључују нове чланове без иједног директног сусрета. Ово значајно отежава рад безбедносних служби и помера границе традиционалног схватања регрутовања.

Посебно рањиву групу у овом процесу чине млади људи са израженим техничким знањем, али и они који се осећају друштвено изоловано, маргинализовано или фрустрирано. Сајбер терористичке групе често користе идеолошке наративе који обећавају смисао, припадност и „вишу сврху“, комбинујући их са наглашавањем интелектуалне надмоћи и технолошке вештине. На тај начин, регрутовање није засновано искључиво на идеологији, већ и на осећају личне вредности и моћи коју појединац може да стекне у дигиталном окружењу.

Терористичке групе користе савремена средства комуникације како би ефикасно регрутовале нове чланове, при чему Исламска држава предњачи у оваквим активностима. Вештом манипулацијом друштвеним мрежама, терористи успевају да привуку нове следбенике, углавном младе особе које се прикључују групи. Компјутерске мреже показале су се као знатно ефикасније и јефтиније решење у односу на тајну инфраструктуру потребну за функционисање и одржавање самих терористичких организација.[56]

## 4.2. Комуникација

Интернет је значајно олакшао глобалну комуникацију, па терористи ову предност радо користе приликом планирања и координације својих активности. Поред форума, чет-соба и профила на различитим друштвеним мрежама, они се ослањају и на

[56] К. Јонев, Сајбер тероризам и употреба сајбер простора у терористичке сврхе, *Безбедност бр. 2, вол. 2016*, стр. 214.

електронску комуникацију путем мејлова, при чему прикривају ИП адресе, користе криптоване и шифроване поруке, као и технике стеганографије.

Бројни интернет сајтови терористичких организација имају за циљ да својим присталицама пруже информације о деловању групе, укључујући и упутства за обуку, као што су израда експлозива, постављање бомби, као и тумачења заснована на верским догмама за која сматрају да дају легитимитет масовном насиљу у областима под њиховом контролом. Један од најпознатијих онлајн магазина те врсте, „Inspire“, наводно је издавала Ал Каида. У овим публикацијама, поред упутстава за обуку и деловање „од куће“, објављиване су и идеолошке поруке које подстичу извршење терористичких аката..[57]

Нове комуникационе технологије, као што су релативно јефтине и доступне мобилне и веб мреже, стварају високо интерактивне платформе кроз које би појединци планирали акције, дискутовали и мењали њихов садржај. Интернет нуди моћан, јефтин и продоран алат за комуникацију и координацију акција, са око 300 милиона људи на мрежи само од 2000. године. Групе било које величине, могу достићи једни друге и користити интернет да промовишу свој програм. Њихови чланови и пратиоци могу доћи из било ког географског подручја на Интернету, а могу покушати да утичу на спољну политику било где у свету.[58]

## 4.3. Бављење организованим криминалом

Поред финансирања, интернет је терористима омогућио и развој сајбер тероризма као новог облика претње. Кроз дигиталне платформе, групе могу да планирају, координишу и спроводе нападе, шире пропаганду, рекрутују нове чланове и врше психолошки притисак на циљне заједнице. Сајбер тероризам се не ограничава само на нападе на компјутерске системе, већ укључује и крађу података, дистрибуцију злонамерног софтвера и саботаже критичне инфраструктуре, што додатно показује колико је дигитални простор постао кључно поље сукоба савременог тероризма.

[57] К. Јонев, Сајбер тероризам и употреба сајбер простора у терористичке сврхе, *Безбедност бр. 2, вол. 2016*, стр. 214.

[58] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016,* стр. 101.

Различити облици организованог криминала, а пре свега прање новца, представљају саставни део савременог тероризма. Присуство на интернету омогућило је терористичким организацијама једноставније и ефикасније финансирање спровођења њихових циљева у стварном свету. Донације се све чешће прикупљају путем онлајн платформи, при чему се на интернет сајтовима отворено објављују рачуни на које се може уплатити такозвана „помоћ“. Поједине терористичке групе користе и параван у виду наводних хуманитарних организација, на чије рачуне донатори уплаћују средства, често не знајући да на тај начин заправо финансирају терористичке активности.[59]

## 4.4. Могућност вођења асиметричног сукоба

Поред већ поменуте пропагандне димензије, потребно је указати и на асиметрични сукоб, односно сукоб који се води између неравноправних страна чија се војна моћ знатно разликује, а који терористи често користе у свом деловању. У асиметричном ратовању слабија страна примењује различите стратегије и тактике, користи слабости противника и елемент изненађења, са циљем остваривања предности и победе.

Асиметрични рат је посебно изводљив у сајбер простору, јер појединац или мања група могу за противника имати и најмоћнију државу на свету. У дигиталном окружењу офанзивне активности се развијају много брже од одбрамбених. Асиметрија је ефикасна само уколико терористичка инфраструктура остаје прикривена, а сама природа сајбер простора омогућава успешно скривање идентитета и локације нападача.[60]

## 4.5. Ширење пропаганде

Ширење пропаганде представља једну од кључних активности терористичких организација у сајбер простору. Процењује се да постоје десетине хиљада интернет

[59] К. Јонев, Сајбер тероризам и употреба сајбер простора у терористичке сврхе, *Безбедност бр. 2, вол. 2016*, стр. 214-215.

[60] К. Јонев, Сајбер тероризам и употреба сајбер простора у терористичке сврхе, *Безбедност бр. 2. вол. 2016*, стр. 215.

сајтова који подржавају Ал Каиду и уопште исламски тероризам. Поред тога, путем рачунара и глобалне мреже терористи могу лако да остваре контакт са својом „публиком“, што им омогућава да проширују своје редове, при чему пропаганда има значајну улогу као ефикасна тактика деловања.

У потрази за светском пажњом, терористи снимају своје акције и постављају их на интернет платформе или их достављају медијима, тако да се такви садржаји веома брзо шире широм света. Исламска држава је посебно позната по интензивном коришћењу интернета у циљу застрашивања противника, путем великог броја видео материјала којима настоји да изазове страх и несигурност. Ова организација је у великој мери унапредила начин употребе друштвених мрежа, комбинујући оружане активности са снажним медијским наступом, што је допринело угрожавању безбедности ширег подручја Блиског истока.

Поред екстремистичких дејстава на терену, група је у кратком року привукла пажњу јавности захваљујући агресивним и добро осмишљеним кампањама на друштвеним мрежама. Страх се не шири само на подручјима под њеном контролом, већ и глобално, кроз активности у сајбер простору и на платформама као што су Фејсбук, Јутјуб, Инстаграм и друге. Исламска држава поседује једну од најразвијенијих пропагандних структура у поређењу са другим терористичким организацијама.

За разлику од Ал Каиде, која се углавном обраћа истомишљеницима, ИД се на популистички и масовнији начин усмерава ка широј светској јавности. Свесна значајне моћи друштвених мрежа, ова група користи интернет као ефикасно средство за ширење своје идеологије и слање политичких порука. Путем различитих пропагандних материјала, као што су билтени на више језика, видео и аудио садржаји, као и комуникација на друштвеним мрежама, форумима и чет-собама, сајбер терористи шире своје кампање, оправдавају своје поступке, привлаче симпатизере и јачају сопствене редове.[61]

Један од главних циљева употребе интернета од стране терористе је ширење пропаганде која обично има облик мултимедијалне комуникације и пружа идеолошку или практичну наставу, објашњења, оправдања или промоцију терористичких активности. Оне могу да садрже виртуелне поруке, презентације, часописе, расправе,

[61] К. Јонев, Сајбер тероризам и употреба сајбер простора у терористичке сврхе, *Безбедност бр. 2, вол. 2016,* стр. 213-214.

аудио и видео фајлове и видео игре развијене од стране терористичких организација или њихових симпатизера . Даље, ширење пропаганде генерално није, само по себи, забрањена активност, ипак, оно што чини овај вид пропаганде, за разлику од легитимног заступања са тачке гледишта, често је субјективна процена.

Промоција насиља је заједничка тема у пропаганди тероризма и широк домет садржаја дистрибуиран преко интернета експоненцијално повећава публику која на коју може да се утиче. Терористи морају имати у својим рукама медиј да би објаснили своју поруку и оправдали своје поступке, јер пре појаве интернета, релативно је било тешко привући масовну публику.

Поред класичних претњи тероризма, утицај савремених медија је покренуло тзв пропагандни рат, коме терористичке организације придају велики значај. Овај рат може бити веома моћно психолошко оружје и може значајно повећати ефекат одређених радњи. Терористи, с једне стране, практикују медијску пропаганду како би показали апсолутно пространство својих циљева , али у исто време они су свесни колико им штети негативан публицитет у њиховој реализацији.

Значење терористичке пропаганде, тј четири главна циља у коришћењу масовних медија су: 1) да пренесу пропагандна дела и да се усади екстремни страх циљној групи; 2) мобилисати ширу подршку за своју ствар у општој популацији и међународно мишљење са акцентом на теме као што су праведност свог циља и неминовности победе; 3) осујетити и пореметити одговор владе и безбедносних снага; 4) мобилисати, подстаћи и повећати своје бираче, стварне и потенцијалне присталице и на тај начин да се повећа запошљавање, подизање више новца и самим тим инспирисати нове нападе.[62]

Питање које се поставља је, ко заправо представља праву публику и следбенике терориста на интернету? Да ли је то влада која ће потрошити свој новац и енергију и гонити их када утврди потенцијалне трагове или је то онај широк аудиторијум који ће следити терористе и заступа њихову идеологију. Тероризам је тесно повезан са концептом пропагандне и појединци који се њиме се у јавној сфери су жигосани као терористи: семантичари истичу да начин на који ми видимо једну особу

[62] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35. вол. 2016,* стр. 102.

умногоме зависи од наших потреба, пројекција и процена али суд о њој се после не мења када се промени оквир посматрања.

Укратко, пропаганда је дизајнирана за манипулацију веровања и изазива акцију у интересу пропагатора убризгавањем порука у главе слушалаца. То укључује коришћење слика, слогана и симбола у игри предрасуда и емоција, а њен крајњи циљ је да се заведе примаоц поруке како би дошао на добровољно прихватање позиције пропагандиста као да је њихов лични. Често се под пропагандом сматрају лажне информације које треба да увере оне који већ верују и у својој модерној употреби.

Услед процеса глобализације, нарочито у области технологије, терористичке групе теже да контролишу медијске технологије да раде у њиховом најбољем интересу. Повећање Интернет услуга и приступа ефикаснијим и јефтинијим рачунарима, софтверима и бежичним технологијама, терористима се пружа могућност да рекламирају и пропагирају своје циљеве путем интернета. Данас смо сведоци све веће и све софистицираније терористичког присуства на интернету и то представља веома динамичан феномен: изненада се појави, често мења своје формате, а затим брзо нестаје или што је још чешћи случај, привидно нестаје мењајући своју интернет адресу, али задржавајући готово исти садржај.

Како би се идентификовали терористички сајтови, спроведена су бројна систематска скенирања интернета, хранећи огроман број имена и термина у претраживањима и улазећи у форуме присталица и симпатизера геодетских линкова и других организација .Ово је веома напоран труд, поготово због тога што у неким случајевима (нпр. Ал Каида) локације и садржај се мењају готово свакодневно.[63]

## 4.6. Значај друштвених мрежа за деловање сајбер терористa

Од самих почетака, основни циљ терористa био је да путем насилних аката своју поруку пренесу што ширем кругу људи, али су тек са појавом интернета и друштвених мрежа добили глобалну публику за ширење идеологије, међусобну комуникацију, као и за прикупљање финансијских средстава и набавку оружја.

[63] М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35. вол. 2016,* стр. 103.

Развојем интернета и друштвених платформи створен је виртуелни простор утицаја који омогућава знатно већи степен слободе за самопромоцију терористичких активности.

Тако, нпр. када авганистански талибански покрет постави апликацију у Гуглову онлајн продавницу (Play Store) која води ка њиховом сајту на паштунском језику, циљ је да корисницима омогући приступ званичним саопштењима и видео садржајима, пре свега становништву које говори тим језиком. На тај начин мреже постају кључни облик деловања, јер захваљујући флексибилности, прикривености и високом степену неконтролисане комуникације омогућавају брзину, повезаност и снажан продор, као и могућност обраћања прецизно одређеним циљним групама, било на локалном или глобалном нивоу.[64]

Нове стандарде у области пропаганде поставила је такозвана Исламска држава, која је вештим коришћењем друштвених мрежа и ширењем радикалних верских идеја подстакла велики број појединачних напада широм света. Анализом њених облика спољне комуникације уочава се висок степен професионалности аутора садржаја, који су посебну пажњу посветили свим елементима карактеристичним за брендирање, од обраћања пажљиво одабраним циљним групама, преко јасног и упечатљивог идентитета са препознатљивим симболима, до доследности у слању порука и начинима њихове дистрибуције. Примењујући савремене ПР технике, ова организација полази од идеје екстериторијалности маркетинга на друштвеним мрежама, градећи међународну виртуелну заједницу истомишљеника и симпатизера.

Друштвене мреже практично немају ограничења, па је и ширење страха готово неограничено, што терористи злоупотребљавају пласирањем шокантних садржаја. Физичка ограниченост појединца уступа место дигиталној покретљивости група, чиме се ствара утисак блискости и повезаности на глобалном нивоу. Због тога и утицај државне моћи слаби са опадањем медијске доминације, што не значи њено нестајање, већ преусмеравање деловања на регионални или светски план.

Значај медијске слике за терористичке идеје уочио је и Абу Мусаб ел Заркави, некадашњи вођа Ал Каиде у Ираку, који је инсистирао да се све операције снимају и да се материјал што пре објављује на друштвеним мрежама. Он је истицао да се велики

[64] З. Јевтовић, Улога друштвених мрежа у промоцији сајбер тероризма, *Политика националне безбедности бр. 7, вол. 2016,* стр. 104.

део борбе одвија управо у медијском простору, наглашавајући снагу визуелних порука у односу на класична средства борбе.

У поређењу са класичним интернет страницама и форумима, друштвене мреже су знатно отвореније и креативније, јер омогућавају директну и интерактивну комуникацију. Док су раније терористи покретали сајтове и чекали да им се заинтересовани сами јаве, данас они активно допиру до публике. Некада је тероризам у домове улазио преко телевизијских екрана, а са развојем интернета и друштвених мрежа публика је сама почела да приступа терористичким садржајима.

Са оваквом тактиком прва је започела Ал Каида, достављајући медијима велики број снимака својих активности, али је напреднији и систематичнији приступ развила Исламска држава, која је друштвене мреже, а нарочито Твитер, користила за мотивисање и придобијање нових присталица. Дубина, анонимност и осећај изолованости који често прате интернет заједнице доприносе стварању окружења у којем екстремистичка пропаганда лако проналази незадовољне појединце и претвара их у потенцијалне носиоце радикалних идеја.[65]

[65] З. Јевтовић, Улога друштвених мрежа у промоцији сајбер тероризма, *Политика националне безбедности бр. 7, вол. 2016,* стр. 106-113.

# ЗАКЉУЧАК

Компјутерски тероризам представља све већу претњу у модерном добу, имајући у виду да су информационе и комуникационе технологије главни елементи функционисања друштва и државних система. Истраживање је показало да, иако се традиционални тероризам и сајбер напади разликују по методама извршења, њихова главна сврха остаје иста и састоји се у ширењу страха, остваривању политичких или верских циљева и утицају на јавност.

Први део рада указује на еволуцију тероризма и одређује карактеристике самих терористичких аката, док је у другом поглављу одређен појам компјутерског криминала, који често постаје алат или претходница сајбер терористичких активности. Такође су одређени и облици компјутерског криминала у другом делу рада. Трећи део рада одређује сам појам компјутерског тероризма, његове специфичности у односу на конвенционални тероризам, као и облике деловања сајбер терористе, у оквиру којих се издвајају ширење пропаганде, комуникација и регрутовање чланова терористичких група, а мање сами хакерски и други напади којима је угрожен неки кључни систем заснован на информационим технологијама.

Тешко је предвидети шта би се могло догодити уколико би неки сајбер терориста одлучио да нападне неке од кључних области за функционисање друштва, а који су зависни од информационо-комуникационих технологија и рачунарских система, као што су: водоснабдевање, дистрибуција електричне енергије, војни системи и сл. Уколико би нпр. нека терористичка група одлучила да хакерским нападом наруши функционисање нуклеарне електране и у томе успела, последице би биле несагледиве.

Закључак је да компјутерски тероризам захтева координисану сарадњу међународне заједнице у креирању јединственог правног оквира, унапређења сајбер безбедности и едукације грађана у циљу спречавања несагледивих последица, нарочито у добу када вештачка интелигенција све више напредује и прети да постане нови полигон борбе терористе. Вероватно свет у будућности чека нови облик тероризма – AI тероризам, чија је претеча и чији ће саставни део бити компјутерски тероризам.

# ЛИТЕРАТУРА


1. А. Ђукић, Организовани високотехнолошки криминал, појам, развој и карактеристике, *Војно дело бр. 3, вол. 2018*.
2. Д. Вулетић, *Одбрана од претњи у сајбер простору,* Институт за стратегијска истраживања, Београд, 2011.
3. Д. Живаљевић, А. Југовић, Тероризам као безбедносни проблем и друштвена девијација*, Журнал за криминалистику и право бр. 1, vol. 2014.*
4. Д. Симеуновић, *Тероризам, општи део*, Правни факултет, Београд, 2009.
5. И. Лукнар, Злоупотреба информационих и комуникационих технологија: појам и уређење у Републици Србији, *Политика националне безбедности бр. 22, вол. 2022.*
6. К. Јонев, Сајбер тероризам и употреба сајбер простора у терористичке сврхе, *Безбедност бр. 2, вол. 2016.*
7. М. Дробац, *Тероризам – цивилизацијка пошаст*, *Култура полиса*
8. М. Крстић, Тероризам у сајбер простору, *Зборник института за криминолошка и социолошка истраживања бр. 35, вол. 2016*.
9. М. Крстић, Улога обавештајног фактора у борби против тероризма, *Цивитас бр. 6. vol 2016.*
10. М. Милошевић, *Кривично право,* Факултет за образовање дипломираних правника и дипломираних економиста за руководеће кадрове, Нови Сад, 2013.
11. М. Симовић, М. Шикман, Тероризам – злочин VS норма, *Криминалистичке теме бр. 1-2, vol. 2017.*
12. Н. Станковић, *Тероризам и финансирање тероризма,* Европски универзитет, Брчко, 2014.
13. П. Мишевић, *Утјецај тероризма на приљев иноземних директних инветиција – докторска дисертација,* Економски факултет, Ријека, 2016.
14. Р. Соколовић Р, *Електронски надзор комуникација у борби против тероризма и људска права и слободе грађана – докторска дисертација*, Правни факултет, Ниш, 2010.
15. С. Клисарић, Сајбер тероризам као окидач све интензивније потребе за безбедност система од опасности која долази са интернета, *Мегатренд Ревија бр. 18, вол. 2021.*
16. С. Николска, Израда и употреба лажних платежних картица као масовни облик компјутерског криминала у Републици Македонији, у: ур. М. Шикман, *Сузбијање криминала и европске интеграције, с освртом на високотехнолошки криминал*, ВШУП, Бања Лука, 2012.
17. З. Јевтовић, Улога друштвених мрежа у промоцији сајбер тероризма, *Политика националне безбедности бр. 7, вол. 2016.*

18. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *„Сл. гласник РС“, бр. 61/2005, 104/2009 10/2023 и 10/2023 - др. закон*
19. Кривични законик, *„Сл. гласник РС“, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 и 94/2024*.
20. Републички завод за статистику, https://publikacije.stat.gov.rs/G2019/Pdf/G20195653.pdf, Приступљено: 01.12.2025. у 11:00h

# СПИСАК ИЛУСТРАЦИЈА



# СПИСАК ТАБЕЛА

# САЖЕТАК

Рад се бави феноменом сајбер тероризма, као савременом претњом у области безбедности и информационих технологија. Анализирани су појам и карактеристике тероризма, као и компјутерског криминалитета, чиме се ствара основа за разумевање сајбер тероризма. Рад истражује специфичности сајбер тероризма у односу на конвенционални тероризам и сајбер нападе, као и глобалне и националне напоре у спречавању ових аката. Такође, разматрани су облици деловања сајбер терориста, укључујући регрутовање, комуникацију, организовани криминал, асиметричне нападе, пропаганду и улогу друштвених мрежа. Закључак истиче значај превентивних мера, контрамера и континуираног унапређења законских и техничких решења у борби против сајбер тероризма.

Кључке речи: *Уливање страха; Сајбер простор; Друштвене мреже; Компјутерски криминалитет.*

## Computer terrorism-SUMMARY

The paper addresses the phenomenon of cyber terrorism as a contemporary threat in the field of security and information technology. The concept and characteristics of terrorism, as well as computer crime, are analyzed, providing a foundation for understanding cyber terrorism. The study examines the specific features of cyber terrorism in comparison to conventional terrorism and cyber attacks, as well as global and national efforts to prevent such acts. Additionally, the paper considers the modes of operation of cyber terrorists, including recruitment, communication, organized crime, asymmetric attacks, propaganda, and the role of social networks. The conclusion emphasizes the importance of preventive measures, countermeasures, and the continuous improvement of legal and technical solutions in the fight against cyber terrorism.

Keywords: *Spreading fear; Cyberspace; Social networks; Computer crime.*

# БИОГРАФИЈА

Марија Клејић рођена је 26.05.1992. године у Мајданпеку. Завршила је средњу угоститељско-туристичку школу, а потом Правни факултет у Нишу. Приправнички стаж је одрадила у Општинској управи општине Сурдулица, где након обављеног приправничког стажа почиње са радом у Туристичкој организацији општине Сурдулица на радном месту правника. Године 2024. уписала је Мастер студије на смеру унутрашњих послова, чиме је наставила да развија своје образовање и професионални пут у области права и безбедности.

**ИЗЈАВА О ИСТОВЕТНОСТИ**
**ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА**

Име и презиме аутора мастер рада: Марија Клејић

Наслов мастер рада: Копмјутерски тероризам

Ментор: Проф. др Дарко Димовски

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, _____

Потпис аутора

_____

**ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА**

Изјављујем да је мастер рад, под насловом Копмјутерски тероризам
пријављен и одбрањен на Правном факултету Универзитета у Нишу:
• резултат сопственог истраживачког рада;
• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;
• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: Марија Клејић

У Нишу, _____

Потпис аутора

_____