УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ
КАТЕДРА ДРУШТВЕНО-ХУМАНИСТИЧКИХ НАУКА

Најчешћи појавни облици компјутерског криминалитета

– СПЕЦИЈАЛИСТИЧКИ РАД –

Ментор:

проф. др Владимир Н. Цветковић

Студент:

Јован Мрдак 33/22

Београд, 2022

С А Д Р Ж А Ј:

УВОД

Сајбер безбедност је један од најважнијих концепата сајбер света који обезбеђује заштиту сајбер простора од разних врста сајбер криминала. Злочин који се може десити уз помоћ компјутерског система и интернета познат је као сајбер криминал. Из историје сајбер напада на Интернет, закључује се да се трендови напада континуирано мењају из дана у дан. Сајбер криминал има много облика који су напредовали са развојем технологије. Сајбер напади не познају границе и развијају се брзим темпом. У оквиру таксономије сајбер криминалитета, подробније се објашњавају два најчешћа појавна облика компјутерског криминалитета: компјутерске крађе и преваре и компјутерски тероризам. Сајбер тероризам се фокусира на коришћење Интернета од стране недржавних актера како би се утицало на економску и технолошку инфраструктуру нације. Досадашња пракса указује на то да се многи облици компјутерског криминалитета не откривају све док неко од учинилаца не направи грешку у манипулацији компјутером, истиче се значај профилисања сајбер починилаца, превасходно вршећи класификацију мотива почининаца.

Рад је подељен на неколико делова. Поред уводног и закључног дела, у раду постоје три поглавља са својим целинама. Први део односи се на сајбер криминалитет у коме се приказује таксономија сајбер криминалитета, конкретније се приказује како новац, емоције, сексуални импулси, политика, религија, забава као мотиви за извршење сајбер криминала утичу на извршење кривичног дела сајбер криминалитета.

Други део се односи на подробније објашњење појединих облика сајбер криминалитета, као два најчешћа појавна облика компјутерског криминалитета детаљније се описују компјутерске крађе и преваре и компјутерска саботажа и тероризам. У трећем делу приказани су начини санкционисања починилаца сајбер криминалитета, представљени су облици превенције ове врсте криминалитета.

I ТЕОРИЈСКО РАЗЈАШЊЕЊЕ КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА

Дефинисање појма сајбер криминалитета

Компјутерски криминалитет подразумева и активно и пасивно коришћење компјутера, па чак и чување доказа о извршеном кривичном делу у рачунару или у електронској форми,[1] а жртве и могуће жртве су сва физичка и правна лица која се служе рачунарима и базама података или зависе од њихове употребе. „До једне јединствене и прихватљиве дефиниције компјутерског криминалитета тешко је доћи из неколико разлога. Врсте извршених кривичних дела која спадају у компјутерски криминалитет је изузетно велик, тако да их је немогуће обухватити једном јединственом дефиницијом. Како је реч о новом облику криминалног понашања, компјутерски криминалитет се још увек није искристалисао у односу на друге врсте криминалног понашања. Иако је у последње време повећан број држава које су донеле законе о борби против компјутерског криминалитета, кривичноправна наука и криминологија се не могу у одређивању компјутерског криминалитета ослањати на законску дефиницију.”[2] Термин *сајбер простор* први је употребио Вилијам Џибсон у научно – фантастичној новели Neuromanser 1984.[3] Термин *Cyber space* је требало да прикаже нематеријални простор незамисливе комплексности у коме рачунарски подаци путују као делићи светлости. Данас се под сајбер простором подразумева врста *заједнице* сачињене од мреже компјутера у којој се елементи традиционалног друштва налазе у облику бајтова и битова, или простор који креирају компјјутерске мреже, односно глобална информациона инфрестуктура кроз коју се врши масовна комуникација и у којој истовремено постоје виртуелно и реално.[4] Према једној дефиницији, компјутерски криминалитет представља такав облик криминалног понашања код кога се коришћење компјутерске технологије и информационих система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривично-правном смислу

[1] Report and Guidance on Privacy in Social Network Services *Rome Memorandum* - 43rdmeeting, 3-4 March 2008, Rome (Italy), http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

[2] Димовски Дарко, *Компјутерски криминалитет,* Правни факултет Универзитета у Нишу, зборник, LV, стр. 197-214, стр. 197.

[3] Радновић, Бранислав, Илић, Милена, Радовић, Немања (2012). *Економски сајбер криминал у Србији – аспект заштите интернет потошача*, Зборник радова, међународна научноструна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, стр. 129.,http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf

[4] Жунић Павловић, Весна, Ковачевић Лепојевић, Марина (2009). *Интерперсонално насиље у cyber простору*, Истраживања у специјалној педагогији, факултет за специјалну едукацију и рехабилитацију, Београд, стр. 227.

релевантна последица. Компјутерски криминалитет представља такође противправну повреду имовине код које се рачунарски подаци с предумишљајем мењају – манипулација рачунара, разарају – рачунарска саботажа, или се користе заједно са хардвером – крађа времена. Рањивост људи и претњи у виртуелном окружењу расте, јавност је забринута због сигурности на Интернету. Сајбер криминалитет је посебно штетан прекршај који се манифестује у различитим областима друштва и има озбиљан утицај на бројне облике – социјалне неорганизације, економски губитак и психолошки поремећај. Сајбер криминалитет као правни, практични и политички проблем је директна претња људским правима, предузетништву, држави и глобалном свету у целини. Сајбер криминалци могу да ометају или дестабилизују, повређују, други траже оснаживање, други добијају податке или идентитет, друштвено најопасније особе које воде политичке циљеве и нападају државну инфраструктуру. Тренутно су сајбер криминалитети најбрже растуће кривично дело у поређењу са другима. Ситуација је постала сложенија повећањем транснационалног карактера криминала.[5] Према прогнози стручњака, сајбер криминал прелазиће целокупно тржиште лекова у 2021. години и штета ће бити шест билиона широм света.[6] Подаци *Глобалне анкете о перцепцији сајбер ризика* 2018. показали су да је скоро две трећине испитаника оценило сајбер ризик као један од пет највиших ризика у њиховој организацији.[7] Подаци из Извештаја Еуробарометра о сајбер сигурности показују да већина испитаника у Летонији и међу европским грађанима је забринута због интернетских прекршаја. Главни страхови грађана односе се на мрежне трансакције и употребу интернет банкарства. На пример, 65% испитаника у Летонији признало је да се углавном осећају да су лоше информисани о ризицима кибернетичког криминала, док су у земљама у којима се већина корисника интернета осећа добро информисано, поверење у интернетску несигурност и немогућност да се заштите повећавају.[8] Проблем сајбер криминала одређује се брзим развојем, применом и употребом информационих технологија, као и употребом ових технологија за кривичне

[5] K. Jaishankar (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, FL, USA: CRC Press, Taylor and Francis Group, 2011)

[6] V. Tumalavičius, J. Ivančiks, O. Karpishchenko (2016*). Issues of society security: public safety under globalization conditions in Lithuania*, Journal of Security and Sustainability Issues 4(9): 545–573.

[7] Global Cyber Risk Perception Survey 2018. By the Numbers: Global Cyber Risk Perception Survey. https://www.marshmma.com/blog/2018-cyber-and-data-security-risk-survey-report

[8] Special Eurobarometr 390 Cyber Security. Report. 2012. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf

сврхе. На пример, брз развој технологија рачунања у облаку такође отвара повољно окружење за сајбер криминалне радње.

Специфичности компјутерског криминалитета

Специфичности компјутерског криминалитета и оперативног рада по компјутерским кривичним делима, захтевају одређени вид специјализације оперативних радника који раде на сузбијању овог вида криминалитета. У недостатку оперативних радника који располажу таквим знањима, потребно је од самог почетка у оперативни рад укључити и одговарајућег стручњака за компјутере, како би се заједничким радом допринело ефикаснијем проналажењу трагова и обезбеђењу материјалних доказа.

Проблематика откривања компјутерских кривичних дела сваким даном је све сложенија, с обзиром на то да је у почетној фази примене компјутерске технике и технологије мањи број људи поседовао одговарајућа стручна знања и вештине које су им омогућавале да компјутер користе у криминалне сврхе. Данас, нарочито појавом микро рачунара и персоналних рачунара створени су услови за много шири круг корисника компјутера, а самим тим и за већи број лица која су у ситуацији да компјутер користе као средство извршења кривичног дела или као објекат напада у реализацији своје криминалне делатности. Досадашња пракса указује на то да се многи облици компјутерског криминалитета не откривају све док неко од учинилаца не направи грешку у манипулацији компјутером. Такође, могуће је да се трагајући за неком другом уоченом грешком открије одређена криминална делатност било појединца или групе који су неовлашћено упали у компјутерски систем, па је могуће да се применом специјалног програма направи одговарајућа замка која ће послужити да се учиниоци открију. До сазнања о компјутерском кривичном делу може се доћи на више начина, међу којима су најчешћи *пријава радника, анонимне и псеудонимне пријаве и надзор и контрола.*[9]

Кривична дела у којим са рачунар јавља у одређеној вези са извршеним делом, углавном спадају у област општег и привредног криминалитета, али с обзиром на то да се извршавају уз помоћ компјутера, то им даје специфичности које се одражавају и на

[9]Алексић, Ж., Миловановић, З. (1994). *Криминалистика*, Београд, стр. 297.

трагове који могу настати од стране компјутера као средства извршења тих кривичних дела. Са становишта криминалистичко – оперативног коришћања трагова компјутера, веома је битно познавати и следеће специфичности у извршавању компјутерских кривичних дела:*место извршења компјутерских кривичних дела везано је за локацију компјутера, али не као код класичних облика криминалитета где учинилац углавном мора да буде на месту извршења кривичног дела.*[10]

За извршење појединих компјутерских кривичних дела потребно је сасвим мало времена, јер се оно мери секундама и минутама, лица која врше кривична дела компјутерског криминалитета морају да поседују одговарајући фонд знања и вештина из области компјутерске технике, компјутерски криминалитет има сопствени *modus operandi*, који његовиучиниоци стално усавршавају, последице компјутерског криминалитета могу се испољити у прибављању противправне имовинске користи, наношењу материјалне штете, затим у присвајању тајних података и других поверљивих информација, те у стварању неповерења према компјутерској техници. Сајбер криминалитет је озбиљна претња која се суочава са савременим светом. Извештаји показују да су трошкови сајбер криминала порасли са 445 милијарди долара у 2014. на 600 милијарди долара 2017.[11]Међународни опсег аката, анонимност починилаца и препреке које се суочавају са кривично–правним агенцијама, погоршавају дилему са сајбер криминалом. Различити законодавни системи су такође криви зашто су међународни споразуми о сајбер криминалу и изручења криминалаца уопште били неуспешни. Поред тога, неке стратегије које су на снази у неким земљама не могу да буду у другима због културних, политичких и управних разлога.

Док је литература која истражује казне за традиционалне врсте злочина обимна и емпиријски разнолика, постоји недостатак студија које би се фокусирале на обрасце изрицања казни за сајбер злочине, посебно изрицања казни међународним сајбер преступницима. Једну од првих студија које попуњавају празнину у литератури у вези са изрицањем казни за сајбер криминал спровели су Marcum, Higgins and Tewksbury(2011). [12]

[10]Матијевић, М., Бошковић, М. (2007). *Криминалистика оператива*, Бања Лука, стр. 399–403.
[11] Lau, L. (2018). Cybercrime 'pandemic' may have cost the world $600 billion last year. https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html
[12] Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2011). Doing Time for Cyber crime: An Examinationof the Correlates of Sentence Length in the United States. International Journal of CyberCriminology, 5(2), 825-835.

Међу најважнијим налазима ове студије је онај који потврђује тенденцију коју аутори и сами истичу – да су криминалци који су починили највише процесуираних сајбер злочина (превара са кредитним картицама и крађа идентитета) осуђени на дуже казне.У другој студији Marcum, Higginsand Tewksbury (2012) истраживачи се позивају на податке Министарства правде САД који показују да је између 2006. и 2010. 51,7% осуђених сајбер криминалаца добило затворску казну.[13] Smith, Grabosky и Urbas (2004)[14] наглашавају четири главна питања за тужиоце у међународним предметима: тешко је утврдити под чију надлежност спада предмет. Количина доказа која је или би могла бити прикупљена за кривично гоњење може представљати изазове. Утврђивање ко је починилац и њихова физичка локација може бити тешко. Такође, решавање проблема у вези са могућношћу екстрадиције и билатералним споразумима о правној помоћи има потенцијал да створи изазове. Јасно је да је сајбер криминал међународни проблем и да сајбер криминалци долазе из целог света. Међународна природа кривичних дела и преступника је експоненцијално порасла како се употреба технологије ширила широм света. То значи да је потенцијал за међународне сајбер преступе драматично порастао.

Компјутерски криминалитет у ужем и ширем смислу

Криминолошки аспект савремених технологија је разнолик. Сајбер криминал је *специфичан, сложен скуп кривичних дела, који, попут појаве криминала, не може се оценити само његовим врстама, методама извршења, штетности, социјалне опасности, штетним последицама, већ и личношћу криминалца.* На Десетом конгресу Уједињених нација за превенцију криминалитета и третман делинквената у Бечу 2000. дефинисан је компјутерски криминалитет (*cybercrime*) као општи појам који обухвата кривична дела која се врше посредством компјутерског система или мреже, у компјутерском систему или мрежи или против компјутерског система или мреже, а обухвата било који криминалитет извршен електронским путем или извршен у делу или у целости у електронском окружењу. У пленарном делу посвећеном компјутерском криминалитету,

[13] Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2012). Incarceration or community placement: examiningthe sentences of cybercriminals. Criminal Justice Studies, 25(1), 33-40.
[14] Smith, R. G., Grabosky, P., & Urbas, G. (2004). Cyber Criminals on Trial. Cambridge, UK: CambridgeUniversity Press.

констатовано је да је могуће препознати две врстекомпјутерског криминалитета:[15]

компјутерски криминалитет у ужем смислу	који подразумева свако незаконито понашање усмерено на електронске операције сигурностикомпјутерских система и података који се у њима обрађују (где спадају дела која се односе на неауторизовани приступ компјутерском систему или мрежи кршењем мера сигурности, оштећење компјутерских података или програма, компјутерске саботаже, неовлашћено пресретање комуникација од и у компјутерским системима и мрежама, компјутерска шпијунажа)
компјутерски криминалитет у ширем смислу	који подразумева свако незаконито понашање везано за или у односу на компјутерски систем и мрежу, укључујући и такав криминалитет какво је незаконито поседовање, нуђење и дистрибуирање информација преко компјутерских система и мрежа (попут компјутерских фалсификата, компјутерске крађе, техничке манипулације уређајима или електронским компонентама уређаја, злоупотребе система плаћања као што су манипулације и крађе електронских кредитних картица или коришћење лажних шифри у незаконитим финансијским активностима).

Облици испољавања компјутерског криминалитета су различити.

Једна од основних криминолошких подела је подела на традиционални компјутерски криминалитет и савремене облике компјутерског криминалитета који су се развили због злоупотреба компјутера и компјутерских мрежа.

Традиционални компјутерски криминалитет најчешће обухвата кривична дела која су уз помоћ рачунара извршена против имовине (*кривична дела крађе, проневере, утаје, уцене*), док савремени облици компјутерског криминалитета обухватају само она кривична дела која могу да изврше употребом рачунара и злоупотребом рачунарских мрежа без обзира нато да ли је мотив за њихово извршење стицање материјалне користи (*интернет прогањање, сајбер тероризам*). [16]

[15] Никић, Срђан: *Најчешће методе напада cyber криминалаца и како се одбранити*, http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf

[16] Тањевић, Наташа (2009). *Компјутерски криминал – правна заштита на националном нивоу*, Безбедност - Часопис Министарства унутрашњихпослова Републике Србије, број 1-2/2009, стр. 152-166, стр. 157.

Најчешћи циљеви сајбер нападача

Сајбер нападачи имају циљеве због којих врше сајбер нападе илити сајбер злочине. Овде ћемо поменути најчешће циљеве сајбер нападача.

Забава	Неки сајбер криминалци обављају своје активности сајбер напада да би тестирали своје хакерске способности. Осећају понос и радост у својим успешним покушајима. Спремни су да стекну славу у свету сајбер криминалаца. Осећају радост и понос када изврше напад који није извео ниједан други нападач или други нападачи нису успели да изведу тај напад.
Хактивисти[17]	Ови сајбер нападачи су мотивисани политичким, верским и друштвеним циљевима. Њихов мотив је да проповедају своје политичке и верске моте и да обесхрабре људе из других група. Они желе да прошире своју религију или политику како би постали популарни међу масама. Тренутни тренд из 2016. и 2017. године показује да хактивисти разоткривају појединце који имају тајне афере путем друштвених веб страница. *Пример је забављање Ешли Медисон чију листу корисника су разоткрили нападачи у јавном домену.*
Финансијска добит	Већина сајбер нападача изводи сајбер нападе ради финансијске добити. Желе да постану богати. Мета сајбер нападача може бити банкарски систем, велике компаније, организације, богати појединци или богате земље. Неке од ових сајбер нападача ангажује нека држава, организација, компанија или појединац.
Шпијунирање	Ове врсте сајбер криминалаца нападају мреже да украду поверљиве информације одређене земље, организације или појединца. Шпијунски хакери могу користити сличне тактике као хактивисти, али њихов једини циљ је да служе циљевима својих клијената и да заузврат добију плату.
Освета	Ове врсте сајбер криминалаца укључују избачене, изнервиране и понижене запослене. Они су познавали политику, тајне и слабе тачке своје компаније, организације или земље. Они обављају своје активности сајбер напада под

[17] *Особа која добија неовлашћени приступ компјутерским датотекама или мрежама у циљу остваривања друштвених или политичких циљева.*

	емоцијом мржње да би се осветили у виду финансијског губитка, нарушавања друштвеног имица, репутације и тако даље.

Најчешћи циљеви сајбер нападача

Најчешћи мотиви починиоца

Препознавање мотива за извршење одређеног сајбер криминала је суштински елемент или корак у процесу профилисања сајбер починиоца. Један од могућих одговора на питање зашто сајбер криминалац почини злочине је зато што су *криминалци.* У пракси, ствари нису тако једноставне, а људи крше законе због различитих мотива.

Поставља се питање: *Зашто је питање мотивације криминалца толико важно?* У већини националних законодавних система, доказ о кривици траже се у троуглу: средства: везано за средства за почињење злочина, мотиви: изражавање разлога за извршење кривичног дела и прилика: мерено постојањем у *правом* месту, у *исправном* времену да се почини злочин. „Поједини аутори, попут Фредерика Коена указивали су на неколико најчешћих мотивација услед којих долази до вршења оваквих кривичних дела.

Зарада новца се ретко појављује као мотив, много чешћи мотив је друштвено доказивање (*поготово код млађих извршилаца*) или освета према некоме рушењем његовог угледа у друштву, јавног компромитовања, манипулацијом истинитих података или уништавањем његових података.”[18] Мотив се генерално сматра важним елементом у изградњи кривичног предмета (*заједно са средствима и могућностима*).

Разумевање мотивације сајбер криминалаца корисно је за испитивање сајбер криминала на два начина: *приликом стварања кривичног профила и приликом доказивања кривице криминалаца.* Генерално, мотиви за извршење сајбер криминала укључују: *самоизражавање, забаву, задовољство, добитак финансијске користи за преступника или трећу страну, емоционалну мотивацију, политичке мотиве, сексуалне мотиви, озбиљне психијатријске болести.*

Новац	Ово укључује свакога ко остварује финансијску добит од злочина,

[18] Дракулић Мирјана (1996). *Основи Компјутерског права*, Друштво операционих истраживача Југославије, ДОПИС, Београд

	било да се ради о службенику банке који користи свој компјутерски приступ да преусмери средства са туђег рачуна на свој, аутсајдеру који хакује базу података компаније да би украо идентитете које може продати другим криминалцима, или професионалном *хакеру за изнајмљивање* кога плаћа једна компанија да украде пословне тајне друге. Новцем може бити мотивисан скоро свако – млади, стари, мушкарци, жене, они из свих социо–економских класа. Криминалац са белим оковратницима има тенденцију да се веома разликује од искусног преваранта или професионалног *дигиталног убице.*
Емоције	Најдеструктивнији сајбер криминалци често делују из емоција, било да је то бес, освета, *љубав* или очај. Ова категорија укључује одбачене љубавнике или супружнике, бивше супружнике (*сајбер ухођење, терористичке претње, узнемиравање путем е–поште, неовлашћени приступ*), незадовољне или отпуштене запослене (*увреда веб сајтова компаније, напади ускраћивањем услуге, крађа или уништавање података компаније, разоткривање поверљиве информације о компанији*), незадовољне муштерије, завађене комшије, ђаци љути због лоше оцене и тако даље. То чак може бити неко ко се наљути због бурне дискусије у групи друштвених мрежа.
Сексуални импулси	Иако је повезана са емоцијама, ова категорија је мало другачија и укључује неке од најнасилнијих сајбер криминалаца: серијске силоватеље, сексуалне садисте (чак и серијске убице) и педофиле. Дечји порнографи се могу уклопити у ову категорију или можда само искоришћавају сексуалне импулсе других за профит, у ком случају спадају у категорију *новац.*
Политика/религија	Уско повезано са категоријом *емоције*, јер људи постају веома емотивни у вези са својим политичким и верским уверењима и спремни су да почине гнусне злочине у име тих уверења. Ово је најчешћи мотиватор за сајбертеористе, али такође мотивише и многе мање злочине.
Само за забаву	Ова мотивација се односи на тинејџере (или чак и млађе) и друге који могу да хакују на мреже, деле музику/филмове заштићене ауторским правима, унаказују веб странице и тако даље – не из зле намере или

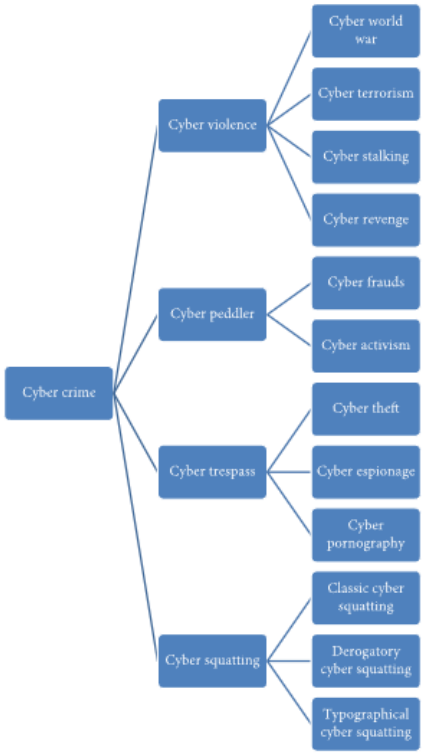
	било какве финансијске користи, већ једноставно *јер могу.* Они то могу даураде да докажу своје вештине својим вршњацима или себи, могу једноставно бити радознали, или то могу да виде као игру. Иако намерно не чине штету, њихови поступци могу коштати компаније новца, изазвати тугу појединаца и везати вредне ресурсе за спровођење закона.

Класификација мотива

Проналажење мотива за извршење одређене сајбер криминалне радње важно је јер помаже форензичком стручњаку да изгради користан профил за преступнике. На основу мотива починиоца криминалци се могу категорисати на два начина: криминалци чији је чин коришћења Интернета за извршење криминала случајан и криминалци који намерно и свесно користе Интернет да изврше криминалну радњу.

II КЛАСИФИКАЦИЈА КРИВИЧНИХ ДЕЛА

Већина злочина који се дешавају у данашњем свету заправо јесу сајбер злочини. Хакери проналазе нови начин да промене своје обрасце напада што професионалцима у области безбедности отежава одбрану информација и података на Интернету и његовим ресурсима. Хакери обезбеђују бесплатне алатке за напад на Интернету како би повећали број стопа напада на Интернет систем. Све већи број е – услуга као што су онлајн куповина, онлајн банкарство и друштвене апликације довео је до великог пораста броја корисника интернета који су лако на мети сајбер криминалаца. Различите врсте сајбер злочина који се дешавају у данашњем свету приказане су на слици и о њима се говори у наставку.



Таксономија сајбер криминала

Слика представља главне категорије сајбер злочина који се дешавају у данашњем свету. Било која врста сајбер криминала може се подкатегорисати у ову таксономију. Таксономија помаже да лако разумемо сличности између напада.

Компјутерске крађе

Сајбер крађа у сајбер простору може да се уради техничким хаковањем нечијег рачунарског система повезаног на Интернет. У сајбер свету, хакери имају за циљ да украду/оштете информације и податке у сајбер простору ради финансијске или личне користи. У основи, постоје две врсте крађа.

- ✧ То су *крађа сајбер простора*: Простор је један од важних фактора, који ако се не одржава правилно доводи до квара на Интернету. Сајбер нападачи имају за циљ да преплаве сајбер простор како би зауставили своје циљне услуге или хаковали своје мете.
- ✧ *Крађа података и информација*: Подаци и информације представљају поверљиву евиденцију појединца, организације и земље. Поверљивост, интегритет и доступност информација на Интернету и серверима морају бити заштићени од сајбер нападача.

Почетком 2008. године 88.000 људи је морало бити обавештено када је болнички рачунар украден са Стејтен Ајленда у Њујорку заједно са свим њиховим личним подацима. У ствари, истраживање *McAfee* и *Datamonitor's Data Loss Survey* о губитку података из 2007. године сугеришу да кршење података које открива личне податке у просеку кошта компаније 268.000 долара да обавесте своје клијенте, чак и ако се ти изгубљени подаци никада не користе.[19]

Крађа идентитета је уско повезана са *phishing* преварама (лажна пракса слања е – поште за које се тврди да су од реномираних компанија како би се појединци навели да открију личне податке, као што су лозинке и бројеви кредитних картица). Ове врсте превара постојале су много раније него што је Интернет постојао, али је свакако побољшао њихов домет и лакоћу извршења. Крађа идентитета постоји у два главна облика, у зависности од информација које су украдене.[20] Ови обрасци су лажно представљање као мање зло ако су украдени само лични подаци или налози без сачуваних начина плаћања. Међутим, може

[19] Интернет извор: https://www.mcafee.com/enterprise/en-us/products/total-protection-for-data-loss-prevention.html
[20] Carr Indira (2009). *Computer Crime,* School of Law, University of Surrey, UK, Routledge

бити много горе ако су подаци о кредитној картици или налози који их садрже украдени јер сајбер криминалац може да изврши куповину наплаћено са налога. Ово се такође односи на компаније. Најлакши и најјефтинији начин да се заштити идентитет на мрежи је да подели што је могуће мање информација. Такође треба да се обрати пажња на активности налога на мрежи и да се проактивно пријави свака сумњива активност чим се она догоди.

Крађа услуга: рачунарске услуге могу бити злоупотребљене на различите начине. Неки примери крађе компјутерских услуга укључивали су политичаре који користе градски рачунар за слање електронске поште за кампању и запослене који обављају неовлашћене слободне услуге на рачунару компаније након радног времена.[21] Системи за дељење времена су били изложени злоупотреби због неадекватних или непостојећих безбедносних мера предострожности. Много је лакше добити неовлашћени приступ систему за дељење времена него затвореном систему. Иако већина система захтева од корисника да има лозинку за приступ, систем је добар онолико колико је добар здрав разум и опрез његових корисника. Систем дељења времена који не захтева редовну промену приступних кодова изазива крађу драгоценог рачунарског времена.[22] Прислушкивање је још једна техника која се користи за добијање неовлашћеног приступа систему за дељење времена. Додиром на линију легитимног корисника, може се имати слободан приступ систему кад год се линија не користи од стране овлашћеног лица.[23] Један од најбољих примера крађе компјутерских услуга десио се на Универзитету Алберта. 1976. године студент на универзитету је започео самосталну студију под надзором професора. Сврха студије била је да се истражи безбедност универзитетског рачунарског система, система за дељење времена са више од 5.000 корисника, од којих су неки чак и у Енглеској. Након што је открио неколико пропуста у безбедности система, студент је успео да развије програм који је смањио могућност неовлашћеног коришћења и манипулисања.

Ученик је на овај програм скренуо пажњу рачунарског центра, који није предузео никакве мере по препорукама ученика. Претпостављало се да ће планиране промене у систему

[21] Romanus Okeke, Mahmood Shah (2016). *Information Theft Prevention, Theory and Practice*, Routledge

[22] Невероватан недостатак пажње наводно софистицираних корисника доспео је на насловне стране на националном нивоу када је откривено да група љубитеља компјутера у средњим школама у Милвокију приступа бројним информационим системима, укључујући банке, болнице и центар за истраживање одбране у Лос Аламосу, Нови Мексико. Студенти су наводно добили приступ коришћењем лозинке сваког система. Неке од лозинки нису мењане годинама, док су друге добијене из јавних извора.

[23] Carr Indira (2009). *Computer Crime,* School of Law, University of Surrey, UK, Routledge

отклонити безбедносне недостатке. Међутим, промене нису спроведене још девет месеци. Током тог периода, програм, који је могао да приказује лозинке, процурео је до неколико студената у кампусу. *Code Green* како је програм добио надимак, на крају је покренут неколико хиљада пута. [24]

Крађа имовине: крађе су постале све чешће са све већом минијатуризацијом рачунарских компоненти и појавом кућних рачунара. Ови злочини се лако апсорбују у традиционалне концепте злочина и не представљају јединствене правне проблеме. Још интригантније је питање шта заправо представља имовину у контексту компјутерског криминала. Различити судови су дошли до веома различитих закључака о овом питању. Компјутерски злочини крађе имовине често укључују робу компаније чије наруџбине обрађују компјутери. Ове злочине обично почини интерно особље које има темељно знање о операцији. Манипулисањем записима могу се креирати лажни налози, који упућују да се наруџбина производа пошаље саучеснику ван организације. Слично, неко може проузроковати исплату чекова за пријем непостојеће робе. Крађа имовине не мора бити ограничена на стварну робу, већ се може проширити и на софтвер. Људи са приступом библиотеци програма система могу лако да добију копије за личну употребу или, чешће, за препродају конкуренту. Техничке мере безбедности у рачунарској инсталацији су од мале користи када непоштено особље искоришћава своје одговорне положаје. Међутим, ова врста крађе никако није ограничена на оне унутар структуре компаније. Компјутерски сервис који има специјализоване програме, али лошу безбедност може да се отвори за неовлашћени приступ такмичара. Све што је неопходно је да аутсајдер добије приступ одговарајућим кодовима. Ово се постиже на више начина, укључујући тајно посматрање легитимног корисника који се пријављује са удаљеног терминала или коришћење удаљеног мини рачунара за тестирање могућих приступних кодова.

Компјутерске преваре

[24] Универзитет је покушао да обрачуна са неовлашћеним корисницима и укинуо је неколико привилегија приступа студентима. Два укључена студента су могла да натерају рачунар да прикаже комплетан списак свих корисничких лозинки, укључујући и оне са највишим нивоима привилегија. У суштини, ово им је дало неограничен приступ датотекама и програмима рачунара. Ови студенти су се осветили администрацији универзитета тако што су повремено чинили систем нефункционалним... Уз неограничену количину ID – а, успели су да избегну откривање, састављајући библиотеку компјутерских програма и надгледајући примену новог безбедносног система. Очајно универзитетско компјутерско особље фокусирало се искључиво на ову ситуацију, водећи детаљан дневник свих терминалних дијалога. Овај напор их је једне вечери довео до терминала на одељењу за геологију, а студенти су ухапшени.

Сајбер превара – чин стицања финансијске или личне користи обманом познат је као сајбер превара. Главни циљ преваре је стицање користи у виду новца. Сајбер преваре укључују нападе друштвеног инжењеринга као што су погађање лозинки, крађа идентитета и ДНС преусмеравање у којима хакер манипулише корисницима да би добио њихове поверљиве информације, а затим користи ове информације за своје интересе. Последњих неколико деценија донело је огромно повећање доступности електронских ресурса. Са повећаном доступношћу дошао је нови облик криминалне активности који користи предности електронских ресурса, односно компјутерски криминал и компјутерска превара. Тренутно, ови нови облици криминала расту и представљају нови и трајни изазов за спровођење закона на свим нивоима у томе како да спрече, истраже и кривично гоне ова кривична дела. [25]

„Конвенција ЦЕТС 185 предвиђа дело *Рачунарске преваре* и оно представља кривично дело које чини лице, у намери да прибави имовинску корист себи или другоме, које неовлашћено нанесе штету другоме путем: било какве измене, уношења, брисања или сакривања рачунарских података, било каквог утицаја на функционисање рачунарског система. Циљ инкриминисања овог дела је да се спрече манипулације у току процесирања података предузете у намери остваривања утицаја на нелегални трансфер средстава. Примери које за ово дело наводи приручник су превара платним или кредитним картицама (чл. 225. КЗ) и аукцијске преваре (чл. 208. КЗ). Као предмет напада се све више јављају електронски фондови, депозитни новац, е злато, као нови предмети класичног кривичног дела преваре."[26] Компјутерска превара је један од најбрже растућих облика компјутерског криминала. Компјутерска превара се такође обично назива интернет превара. У суштини, компјутерска/интернет превара је *било која врста шеме преваре која користи једну или више компоненти Интернета – као што су собе за ћаскање, е-пошта, огласне табле или веб локације за представљање лажних трансакција или за пренос прихода од преваре, финансијским институцијама или другима повезаним са шемом*. Постоји више облика интернет преваре.[27]

[25] Romanus Okeke, Mahmood Shah (2016). *Information Theft Prevention, Theory and Practice*, Routledge
[26] Прља Драган, Ивановић Звонимир, Рељановић Марио (2011). *Кривична дела високотехнолошког криминала*, Институт за упоредно право. Београд, стр. 169.
[27] Gačić, M. (1982). *Kompjuterski kriminal, inostrana iskustva*, 13. maj, br. 5, Zagreb

Једна врста интернет преваре је нигеријска превара е – поште. Ова врста преваре обично тражи од људи да пошаљу новац обећавајући много већу суму у кратком року. Најпознатија је *нигеријска* превара, позната и као 419 превара, што је број нигеријског закона који крши. Ове преваре су већ биле распрострањене путем факса, телефона и традиционалне поште, али их је интернет учинио много лакшим за извођење и распрострањенијим. Обично жртва добија комуникацију од некога коме је потребна помоћ да премести велику суму новца из стране земље. Постоји много варијација ове преваре и сваким даном се развија више. Од жртве ће се тражити да покрије мали део трошкова премештања новца или имовине, а биће јој обећан већи део бенефиција када се процес заврши. Ако жртва наседне на то и пребаци новац, биће јој речено да је дошло до компликација и да ће бити потребно више новца. Наравно, жртва неће ништа опоравити и то ће се наставити све док преварант не осети да од ове жртве нема шта да добије и пређе на другу. Још једна уобичајена превара је повезана са лажним огласима за посао, где се од жртве тражи да плати нешто новца да покрије трошкове папирологије или формирања пре пријаве. Здрав разум је наша најбоља одбрана од ове врсте сајбер криминала, као што је случај са преварама у лову, ако је понуда превише добра да би била истинита, обично није истинита. Не би требало веровати нежељеној комуникацији од странаца који нуде веома атрактивне понуде и никада не плаћати унапред ништа од тога.

Компјутерска превара се може описати као подскуп компјутерског криминала. Компјутерска превара користи електронске ресурсе за представљање лажних или погрешно представљених информација као средства обмане. Према Министарству правде, преварне активности које се тренутно одвијају и користе електронске ресурсе су у великој мери продужетак традиционалних постојећих активности превара које искоришћавају нови медиј. [28]Завод за статистику правде истиче превару као *...намерно лажно представљање информација или идентитета да би се други обманули...* и додаје квалификатор *употребе електронских средстава* да би се разграничила компјутерска превара.[29]

[28] National White Collar Crime Center. IFCC 2002 Internet Fraud Report: January 1, 2002- December 31, 2002. http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf

[29] Rantala, RR. Cybercrime Against Business. Bureau of Justice Statistics. March 2004.

Слично, Министарство правде дефинише интернет превару као превару која користи било коју компоненту интернета да би се извршила намеравана лажна активност. Претпоставља се да би се ова дефиниција могла прилагодити компјутерској превари, тако што би се захтевало коришћење рачунара или другог електронског ресурса у извршењу дела преваре. Уопштено говорећи, компјутерска превара треба да садржи исту основну дефиницију традиционалне преваре, уз употребу нових квалификатора који прилагођавају његову употребу електронским ресурсима.

Компјутерске саботаже

Компјутерска саботажа укључује намерне нападе који имају за циљ да онеспособе рачунаре или мреже у циљу ометања трговине, образовања и рекреације ради личне користи, вршења шпијунаже или омогућавања криминалних завера, као што су трговина дрогом и људима. Према Федералном истражном бироу, компјутерска саботажа кошта милијарде долара правних трошкова за надокнаду штете као што је крађа идентитета и за поправку виталне инфраструктуре која опслужује болнице, банке и службе 911.[30] Саботажа рачунара доводи до уништења или оштећења рачунарског хардвера. Ова врста компјутерског криминала често личи на традиционалну саботажу јер се сам рачунар не користи за извршење уништавања. Саботажа може захтевати извесну софистицираност ако се морају спречити компјутерски подржани безбедносни системи или ако се системом манипулише да нанесе штету самом себи. Компјутери су мете саботаже и вандализма, посебно у временима политичког активизма. На пример, дисидентске политичке групе током 1960их, вршиле су нападе на компјутерске инсталације, често изазивајући велику штету. Ова насилна дела не захтевају никакву посебну стручност од стране злочинца. Саботажу могу, међутим, да спроводе незадовољни бивши запослени који користе део свог знања о операцијама компаније да би добили приступ и уништили хардвер и софтвер. Још један облик саботаже који се користи на микрорачунарима је проблематичан програм који не само да омета рачунарску услугу, већ може и да уништи садржај хард диска или дискете. Такав програм је вирус, назван је зато што може да зарази рачунарске системе тако што се реплицира и везује за друге програме. Вируси могу да заразе друге системе са дискета или преко мрежа. Једном када се вирус нађе у систему и реплицира се унапред

[30] Sinton, Peter (2000). *10 Steps to Prevent Internet Sabotage*. SFGate.

одређени број пута, може покушати да избрише или промени податке на хард диску или дискети. Ово може бити изузетно штетно за корисника који ништа не сумња. Иако је веома тешко заштитити се од вируса, постоје програми који их могу открити и супротставити.[31]

Један од најобјављиванијих аката компјутерске саботаже догодио се 2. новембра 1988. када је вирус пропутовао Интернетом, некласификованом мрежом коју користе владини, пословни и универзитетски истраживачи за размену података и налаза. За неколико сати, овај вирус (самостални програм који се зове *црв*) заразио је приближно 6.000 војних, корпоративних и универзитетских рачунара.[32]

Сајбер тероризам

Сајбер тероризам (познат као *дигитални тероризам*) се дефинише као ометајући напади признатих терористичких организација на компјутерске системе са намером да изазову аларм, панику или физички поремећај информационог система. Иако смо навикли да слушамо о сајбер нападима, сајбер тероризам изазива другачију врсту бриге. Компјутерски хакери су дуго радили на добијању приступа поверљивим информацијама ради финансијске добити, што значи да би терористи могли даураде исто. Сајбер тероризам подразумева коришћење ИКТ инфраструктуре у циљу стварања штете у стварном животу или критичног поремећаја са циљем промовисања политичког, верског или друштвеног питања нападача. Терористи могу уметнути своје намере у дигитални простор како би унапредили своје циљеве.[33]Терористи могу да користе интернет за финансирање својих операција, обуку других терориста и планирање терористичких напада. Уобичајена идеја сајбер тероризма је хаковање владиних или приватних сервера за приступ осетљивим информацијама или чак извлачење средстава за коришћење у терористичким активностима. Око миленијума, многи стручњаци из различитих дисциплина показали су интересовање за потенцијал сајбер тероризма. Из тог разлога, предложен је широк спектар умерених дефиниција сајбер тероризма, посебно у периоду

[31] Giacomazzo, Bernadette R. (2014). *OpenSSL Heartbleed Computer Virus Fix and Security: How to Protect Yourself from the Latest Internet Bug.*
[32] У јануару 1990. Robert Tappan Morris, Jr. дипломирани студент Универзитета Корнел, осуђен је за ослобађање *црва*
[33] Veerasamy Namosha (2020). *Cyberterrorism – the spectre that is the convergence of the physical and virtual worlds* in Emerging Cyber Threats and Cognitive Vulnerabilities

између 1997. и 2001. Разлог за некохерентност дефиниција произилази из чињенице да је њихово порекло у сасвим различитим стручним областима као што је спровођење закона, међународне студије, антитерор, информациона безбедност и информационе операције. Популарна штампа чак ствара још више забуне. Марк Полит из FBI – а је 1997. дефинисао сајбер тероризам као: Смишљени, политички мотивисани напади на информације, компјутерске системе, компјутерске програме и податке који резултирају насиљем против неборачких циљева од стране суб – националних група или тајних агената.[34] Међутим, тренутно не постоји универзално прихваћена дефиниција сајбер тероризма.

Примери сајбер тероризма: *увођење вируса у рањиве мреже података, хаковање сервера ради ометања комуникације и крађе осетљивих информација, нарушавање веб – сајтова и њихово чињење недоступним јавности и на тај начин изазивају непријатности и финансијске губитке, хаковање комуникационих платформи за пресретање или заустављање комуникације и терористичке претње користећи интернет, напади на финансијске институције ради преноса новца и изазивања терора.*[35]

Сајбер напади могу доћи у облику вируса, малвера, крађе е – поште, превара на друштвеним мрежама, дакле спектар сајбер претњи је неограничен. Међусобно смо повезани више него икада раније, али уз све предности, та повезаност нас чини рањивима на ризике преваре, крађе, злоупотребе и напада. Организовани сајбер криминал, хакери које спонзорише држава и сајбер шпијунажа могу представљати ризик за националну безбедност за нашу земљу и нашу критичну инфраструктуру. Саобраћај, струја и друге услуге могу бити поремећене сајбер инцидентима великих размера. Обим поремећаја је веома неизвестан јер ће га одредити многи непознати фактори као што су мета и величина инцидента. Рањивост на кршење података и губитак се повећава ако је мрежа организације угрожена. Информације о компанији, њеним запосленима и клијентима могу бити угрожене.

Уређаји у индивидуалном власништву као што су рачунари, таблети, мобилни телефони и системи за игре који се повезују на Интернет су подложни упадима. Лични подаци могу бити угрожени без одговарајуће безбедности. Сајбер тероризам се сматра највишим

[34] Luiijf Eric (2014). *Definitions of Cyber Terrorism* in Cyber Crime and Cyber Terrorism Investigator's Handbook
[35] Cohen Daniel (2014). *Cyber terrorism* in Cyber Crime and Cyber Terrorism Investigator's Handbook

националним ризиком за многе владе с обзиром на потенцијалну штету и поремећаје које може изазвати због све веће зависности света од ИТ система.

Док очигледне мете могу бити владе, банке и комунална предузећа (*вода, нафта, струја, гас, хемијска и комуникациона инфраструктура*), пошто напади на њих имају могућност да изазову највећи економски, политички и физички хаос и штету критичној националној инфраструктури, сајбер терористичке групе постају све координисаније и софистицираније у својим нападима и користиће сваки рачунар повезан на Интернет да подрже напад. Због тога сајбер тероризам погађа све, од великих организација до свих грађана који поседују или користе рачунар повезан на Интернет. [36]

[36] MacKinnon Lachlan, Frangiskatos Dimitrios (2013). *Cyber Security Countermeasures to Combat Cyber Terrorism* in Strategic Intelligence Management

III САНКЦИОНИСАЊЕ И ПРЕВЕНЦИЈА
Облици превенције криминалитета сајбер починилаца

Пораст броја случајева сајбер криминала збунио је истражне агенције јер починиоци таквих злочина стално развијају или користе развијене и нове технике операција да почине сајбер злочине.

Може се рећи да је превенција само једна од фаза одбране, али веома значајна обзиром да представља први корак у одбрани од сајбер напада. Многи информационо – технолошки системи дизајнирани су тако да на што бољи начин пруже тражену услугу, производ својим корисницима, док њиховој заштити није посвећена посебна пажња. Нпр. сајбер тероризам, за разлику од осталих облика сајбер криминалитета има за циљ да причини штету што је могуће већих размера.

Услед велике динамике развоја технолошких достигнућа иновација, са аспекта безбедности и одбране готово да је немогуће пратити развој савремених технологија и ићи у корак са њима не би ли се пружиле адекватне мере заштите. Разни аутори предност дају методу предвиђања кибер напада, те наводе да у томе значајно могу да послуже кључни подаци, као што су: мотивација, омогућава предвиђање највероватнијег циља сајбер напада, могућност за извршење, омогућава детерминисање највероватније врсте сајбер напада и време, предвиђање тачног времена када би се десио напад. Дејвис сматра да су превенција и свест кључни елементи у смањењу преваленције девијантних аката, нарочито у борби против компјутерског криминала.[37] Клајн предлаже *холистичку стратегију превенције*. која укључује сва средства, односно интегрише војни и невојни приступ. Дакле, свеобухватна стратегија превенције подразумева да се војне и не-војне активности спроводе удружено у циљу превенције сајбер тероризма *одвраћањем и одговарањем* потенцијалног противника да изврши дело сајбер тероризма.[38]

[37] Davis, T. J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component, Policing: An International Journal of Police Strategies & Management 35 (2), 272-284, стр. 278.

[38] Klein, J.J (2018). Deterring and Dissuading Cyberterrorism, ASPJ Africa & Francophonie 9 (1), 21-34. https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue1/2018_1_e.pdf

Бослер и Холт су спровели истраживање да представе перцепцију полиције о њиховој тренутној способности да одговоре на дела сајбер криминала и прикажу предлоге за побољшање друштвеног одговора. Аутори наводе следеће смернице: корисници интернета треба да буду пажљивији када користе интернет, теже казне за сајбер криминалце, тежа кривична гоњења за сајбер криминалце, јасније законодавство против сајбер криминала би повећало успешност гоњења и истраге, специјални форензички алати и технологије, повећање средстава за обуку агенција које су у служби закона, стварање боље сарадње између државе и савезника по питању сајбер криминала, рад са провајдерима како би се надгледао интернет, боља едукација јавности у вези са сајбер криминалом, сарадња са пословном заједницом ради побољшања извештавања и истраживања криминала наменски структуриране локалне јединице за сајбер криминал.[39] Један од основних приступа који треба да користи сајбер истражитељ је профилисање сајбер криминалаца. Профилисање инсинуира оквир за анализу, идентификацију, праћење и кривично гоњење починилаца. Поменута техника укључује *опсежно профилисање података различитих појединаца и институционалних девијантних понашања*.

Помаже у категоризацији криминалних активности на основу модуса операнди девијаната, као и класа и слојева жртава. Профилисање сајбер преступника је драгоцено и неизбежно за успешно регулисање сајбер криминала. Идентификовање низа карактеристика као што су *мотивација за извршење таквог кривичног дела, идентитет, понашање, вештине и знање таквог преступника, ресурси и приступ* које преступник користи за извршење може бити корисна информација за профилисање сајбер преступника.

Развој базе података модуса сајбер криминалаца могао би допринети изградњи капацитета агенција за спровођење закона. Важно је напоменути да у профилисању сајбер криминала, откривање идентитета сајбер преступника игра кључну улогу у помагању држави у праћењу сајбер криминалаца.

Проширивање овог приступа за откривање починилаца сајбер криминала интеграцијом јединствених карактеристика, специфичних за овај облик криминала, могло би помоћи у

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

бољој регулативи сајбер криминала. Профилисање сајбер криминала може се користити за анализу података који се односе на сајбер преступнике. Испитивање обрасца понашања сајбер преступника може помоћи агенцијама за спровођење закона да имају далекосежне способности у превенцији и откривању криминала. Судови такође могу да искористе такву анализу у разумевању *modusa operandi* сајбер преступника, што резултира одговарајућим закључцима таквих случајева.

Конвенција о сајбер криминалу је осмишљена у циљу спречавања дела која су усмерена против интегритета, поверљивости и доступности компјутерских система, мрежа и података, а самим тим и спречавања злоупотребе тих система, мрежа и података тако што ће се покренути казнене мере за такво деловање као што је описано у Конвенцији и при чему ће се применити казне за ефикасну борбу против кривичних дела, и на тај начин ће се на унутрашњем и међународном нивоу олакшати откривање, истрага и гоњење за извршена кривична дела и омогућити да се обезбеде услови за брзу и поуздану међународну сарадњу.

Република Србија је потписала 16. априла 2005. у Хелсинкију како *Конвенцију о сајбер криминалу*, тако и *Додатни протокол* уз ту Конвенцију. Основни значај ове Конвенције је формирање посебних државних органа који су специјализовани за борбу против сајбер криминала. Законодавство Републике Србије је у периоду од априла 2005. до марта 2009. године усвојило више прописа којима се Конвенција сајбер криминала и Додатни протокол имплементирају у наш правни систем.

Санкционисање починилаца сајбер криминалитета

Одељења за сузбијање Високотехнолошког криминала МУП – а наводе да је приметан пораст кривичних дела, како из области високотехнолошког криминала, тако и класичних дела која се обављају преко интернета и друштвених мрежа, као што су превара, изазивање панике и нереда, угрожавања сигурности и недозвољена трговина.

Кључни фактори у борби против криминала и криминалаца су идентификовање починилаца сајбер криминала и разумевање метода напада. Откривање и избегавање сајбер напада су тешки задаци. Полиција стога мора да иде у корак са новим

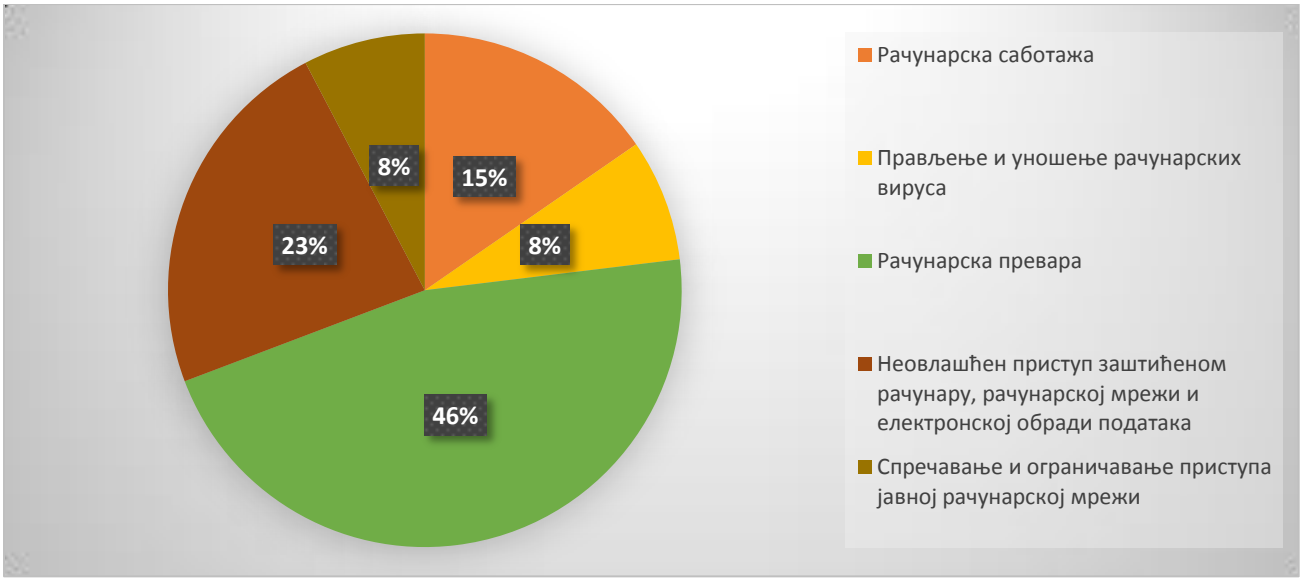
технологијама, да би разумела могућности које се стварају за криминалце и како се оне могу користити као оруђе за борбу против сајбер криминала. У области борбе против високотехнолошког криминала у Србији најзначајнији помак учињен је оснивањем специјализованих органа на нивоу полиције, тужилаштва и суда. *Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала*, који је ступио на правну снагу 25. јула 2005. основано је Посебно тужилаштво у оквиру Окружног јавног тужилаштва у Београду, посебно судско одељење у Окружном суду у Београду и специјализована полицијска јединица при Служби за борбу против организованог криминала.[40]

Месна надлежност наведених специјализованих органа успостављена је на целој територији Републике Србије, док је стварна надлежност прописана чланом 3. наведеног закона и односи се на кривична дела против безбедности рачунарских података прописаних *Кривичним закоником* (XXVIIX) као и на кривична дела против интелектуалне својине, имовине и правног саобраћаја код којих се као објекат или средство извршења јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако је број ауторских дела већи од 500 или настала материјална штета прелази износ од 850 000 динара.[41] Кривични законик у својој XXVII глави прописује следећа кривична дела против безбедности рачунарских података: Оштећење рачунарских података и програма (члан 298), Рачунарска саботажа (члан 299), Прибављање и уношење рачунарских вируса (члан 300), Рачунарска превара (члан 301), Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302), Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303), Неовлашћено коришћење рачунара или рачунарске мреже (члан 304), и Прибављање, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а).[42] Објект заштите наведених кривичних дела је безбедност рачунарских програма. Када су у питању кривичне санкције, прописана је примена казне затвора или новчане казне у зависности од тежине учињеног дела.

[40] *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*, Службени гласник РС, број 61/05, 18. јул 2005.
[41] 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 и 35/2019.
[42] Ибидем

Пријављена пунолетна лица према кривичном делу, 2021.[43]

КРИВИЧНА ДЕЛА	укупно	СРБИЈА СЕВЕР		СРБИЈА ЈУГ	
		Београд	Војводина	Шумадија и Западна Србија	Јужна и Источна Србија
Против безбедности рачунарских података	13	5	1	5	2
Рачунарска саботажа	2	-	-	2	-
Прављење и уношење рачунарских вируса	1	-	-	1	-
Рачунарска превара	6	2	1	1	2
Неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података	3	3	-	-	-
Спречавање и ограничавање приступа јавној рачунарској мрежи	1	-	-	1	-

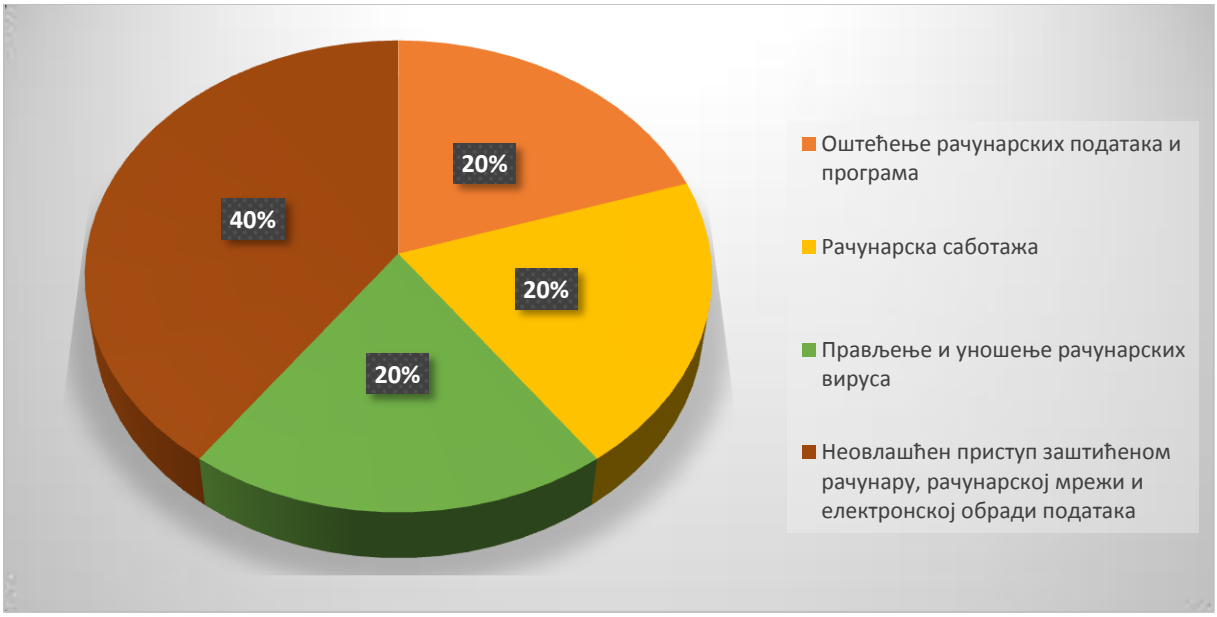


Кривична дела против безбедности рачунарских података – кривичне пријаве

Осуђена пунолетна лица према кривичном делу и изреченим кривичним санкцијама, 2021.

[43] Република Србија, Републички завод за статистику, саопштење број LXXII, 14.07.2022., Статистика правосуђа, Пунолетни учиниоци кривичних дела у Републици Србији, 2021.

	Укупно	Затвор	Новчана казна	Условна осуда
Против безбедности рачунарских података[44]	5	-	2	3
Оштећење рачунарских података и програма	1	-	-	1
Рачунарска саботажа	1	-	-	1
Прављење и уношење рачунарских вируса	1	-	1	-
Неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података	2	-	1	1



Кривична дела против безбедности рачунарских података – број осуђених пунолетних лица

[44] Кривичне санкције за које није одређено ниједно лице: *У кућном затвору, Рад у јавном интересу и одузимање возачке дозволе, Судска опомена, Васпитна мера, Проглашено кривим а ослобођено од казне.*

ЗАКЉУЧАК

Сајбер криминал обухвата низ активности. На једном крају су злочини који укључују фундаментална кршења личне или корпоративне приватности, као што су напади на интегритет информација које се чувају у дигиталним депоима и употреба нелегално добијених дигиталних информација за уцену фирме или појединца. Такође на овом крају спектра је растући злочин крађе идентитета. На средини спектра леже кривична дела која су заснована на трансакцијама: превара, трговина дечјом порнографијом, дигитална пиратерија, прање новца и фалсификовање. То су конкретни злочини са конкретним жртвама, али се злочинац крије у релативној анонимности коју пружа интернет. Други део ове врсте криминала укључује појединце унутар корпорација или владиних бирократија који намерно мењају податке било за профит или политичке циљеве. На другом крају спектра су они злочини који укључују покушаје да се поремети стварни рад Интернета. Они се крећу од нежељене поште, хаковања и напада ускраћивањем услуге на одређене сајтове до дела сајбер тероризма то јест, коришћења интернета за изазивање нереда јавности, па чак и смрти.

У првој великој целини мотив је прибављање противправне имовинске користи, пре свега новца. Све чешће се ти токови новчани преливају у виртуелне валуте – монеро и биткоин, са циљем скривања трансакција. Та група укључује злоупотребу платних картица, рачунарске преваре, уцене. Другу велику групу представљају кривична дела против полних слобода, пре свега малолетних лица, док трећу групу чине кривична дела која су мотивисана мржњом осветом у која се убрајају кривична дела мржња, прогањања, расна и друга дискриминација и слично.

Сајбер тероризам се фокусира на коришћење Интернета од стране недржавних актера како би се утицало на економску и технолошку инфраструктуру нације. Од напада 11. септембра 2001. свест јавности о претњи сајбер тероризма је драматично порасла. Све је теже супротставити се таквим активностима. Још је теже открити и зауставити сајбер криминалце у тренутку кад врши своје деловање, јер управо је то најбољи моменат за његово идентификовање и хватање. Почини се много више сајбер криминала него што се починиоца открије.

Бројни привредни субјекти зарада очувања репутације упаде у компјутерске системе не пријављују и јавно не објављују.

Сајбер напади не познају границе и развијају се брзим темпом. Речи и фразе које су једва постојале пре деценију сада су део нашег свакодневног језика, јер криминалци користе нове технологије да изврше сајбер нападе на владе, предузећа и појединце. Ови злочини не познају границе, физичке или виртуелне, наносе озбиљну штету и представљају веома стварну претњу жртвама широм света. Сложене криминалне мреже функционишу широм света, координирајући замршене нападе за неколико минута. Као што смо видели, сајбер криминал има много облика, и нису сви нешто ново, само је постао лакши и раширенији са новим технологијама. Веома је важно да ми, како у приватном тако и у професионалном животу, будемо свесни ових и других сајбер криминалитета и да држимо *очи отворене,* посебно у време кризе када се број преступника повећава. Изнете чињенице указују да је савремено друштво принуђено стално усавршавати механизме борбе против сајбер криминала, организовано, континуирано, стратегијски, са посебним акцентом ефикасног процесуирања који би обесхрабрио потенцијалне извршиоце.

ЛИТЕРАТУРА

- Bossler, A.M. & Holt, T.J.(2012). Patrol officers' perceived role in responding to cybercrime. Policing: An International Journal of Police Strategies & Management 35 (1), 165-181.
- Carr Indira (2009). *Computer Crime*, School of Law, University of Surrey, UK, Routledge
- Cohen Daniel (2014). *Cyber terrorism* in Cyber Crime and Cyber Terrorism Investigator's Handbook
- Davis, T. J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component, Policing: An International Journal of Police Strategies & Management 35 (2), 272 – 284.
- Gačić, M. (1982). *Kompjuterski kriminal, inostrana iskustva*, 13. maj, br. 5, Zagreb
- Giacomazzo, Bernadette R. (2014). *OpenSSL Heartbleed Computer Virus Fix and Security: How to Protect Yourself from the Latest Internet Bug*.
- Global Cyber Risk Perception Survey 2018. By the Numbers: Global Cyber Risk Perception Survey. https://www.marshmma.com/blog/2018-cyber-and-data-security-risk-survey-report
- K. Jaishankar (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, FL, USA: CRC Press, Taylor and Francis Group, 2011)
- Klein, J.J (2018). Deterring and Dissuading Cyberterrorism, ASPJ Africa & Francophonie 9 (1), 21 – 34. https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/Volume-09_Issue1/2018_1_e.pdf
- Lau, L. (2018). Cybercrime ’pandemic’ may have cost the world $600 billion last year. https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html
- Luiijf Eric (2014). *Definitions of Cyber Terrorism* in Cyber Crime and Cyber Terrorism Investigator's Handbook

— MacKinnon Lachlan, Frangiskatos Dimitrios (2013). *Cyber Security Countermeasures to Combat Cyber Terrorism* in Strategic Intelligence Management
— Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2011). Doing Time for Cyber crime: An Examinationof the Correlates of Sentence Length in the United States. International Journal of CyberCriminology, 5(2), 825 – 835.
— Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2012). Incarceration or community placement: examiningthe sentences of cybercriminals. Criminal Justice Studies, 25(1), 33 – 40.
— National White Collar Crime Center. IFCC 2002 Internet Fraud Report: January 1, 2002-December 31, 2002. http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf
— Rantala, RR. Cybercrime Against Business. Bureau of Justice Statistics. March 2004.
— Report and Guidance on Privacy in Social Network Services *Rome Memorandum* - 43rd meeting, 3-4 March 2008, Rome (Italy), http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf
— Romanus Okeke, Mahmood Shah (2016). *Information Theft Prevention, Theory and Practice,* Routledge
— Sinton, Peter (2000). *10 Steps to Prevent Internet Sabotage*. SFGate.
— Smith, R. G., Grabosky, P., & Urbas, G. (2004). Cyber Criminals on Trial. Cambridge, UK: CambridgeUniversity Press.
— Special Eurobarometr 390 Cyber Security. Report. 2012. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf
— V. Tumalavičius, J. Ivančiks, O. Karpishchenko (2016*). Issues of society security: public safety under globalization conditions in Lithuania*, Journal of Security and Sustainability Issues 4(9): 545–573.
— Veerasamy Namosha (2020). *Cyberterrorism – the spectre that is the convergence of the physical and virtual worlds* in Emerging Cyber Threats and Cognitive Vulnerabilities
— Алексић, Ж., Миловановић, З. (1994). *Криминалистика*, Београд
— Димовски Дарко, *Компјутерски криминалитет,* Правни факултет Универзитета у Нишу, зборник, LV, стр. 197 – 214.
— Дракулић Мирјана (1996). *Основи Компјутерског права*, Друштво операционих истраживача Југославије, ДОПИС, Београд

— Жунић Павловић, Весна, Ковачевић Лепојевић, Марина (2009). *Интерперсонално насиље у cyber простору*, Истраживања у специјалној педагогији, факултет за специјалну едукацију и рехабилитацију, Београд
— *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*, Службени гласник РС, број 61/05, 18. јул 2005
— Интернет извор: https://www.mcafee.com/enterprise/en-us/products/total-protection-for-data-loss-prevention.html
— *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 и 35/2019.
— Матијевић, М., Бошковић, М. (2007). *Криминалистика оперативa*, Бања Лука, стр. 399–403.
— Никић, Срђан: *Најчешће методе напада cyber криминалаца и како се одбранити*, http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf
— Прља Драган, Ивановић Звонимир, Рељановић Марио (2011). *Кривична дела високотехнолошког криминала*, Институт за упоредно право. Београд
— Радновић, Бранислав, Илић, Милена, Радовић, Немања (2012). *Економски сајбер криминал у Србији – аспект заштите интернетпотошача*, Зборник радова, међународна научностручна конференција, Сузбијање криминала и европске интеграције с освртом на вискотехнолошки криминал, http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf
— Република Србија, Републички завод за статистику, саопштење број LXXII, 14.07.2022., Статистика правосуђа, Пунолетни учиниоци кривичних дела у Републици Србији, 2021.
— Тањевић, Наташа (2009). *Компјутерски криминал − правна заштита на националном нивоу*, Безбедност - Часопис Министарства унутрашњихпослова Републике Србије, број 1 – 2/2009, стр. 152 – 166.