УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

МАСТЕР РАД

Cyber криминалитет и профилисање починилаца

Ментор
Проф.Дарко Димовски

Студент
Маја Вукман
Бр.индекса: М018/19-УП

Ниш, 2022.

С А Д Р Ж А Ј:

УВОД

Безбедност нације данас није ограничена само на изградњу утврђења или чување граница, већ укључује и обезбеђење сајбер простора заштитним зидовима и другим мерама и стратегијама сајбер безбедности. Већина активности данас се повезује са интернетом, било да се ради о проналажењу једноставног одговора на питање или куповини или обављању банкарских и пословних трансакција. Лакоћа коју пружа технологија је таква да пружа удобност и завршава процес *притиском на дугмад.* Али лак и економичан приступ интернету такође је довео девијантне до злоупотребе информационе технологије јер сајбер простору недостају географска ограничења и проширује предности анонимности која је у ствари највећи штит за такве погрешне људе. Стварање псеудо идентитета у сајбер свету обезбеђује већу анонимност сајбер криминалцима.

Сајбер безбедност је један од најважнијих концепата сајбер света који обезбеђује заштиту сајбер простора од разних врста сајбер криминала. У овом модерном добу, свет постаје све познатији и људи су ближи један другом уз помоћ Интернета и нових мрежних технологија. У постојећем свету Интернета можемо пронаћи огроман обим и разне сајбер нападе. Из историје сајбер напада на Интернет, закључује се да се трендови напада континуирано мењају из дана у дан. Злочин који се може десити уз помоћ компјутерског система и интернета познат је као **сајбер криминал**. То је злонамерна активност која може да утиче на три основна принципа мрежне безбедности, односно на поверљивост, интегритет и доступност. Сајбер криминал укључује појмове као што су превара, крађа, туче и светски рат. Ови термини се такође користе у злочинима из стварног живота, али у свету Интернета ови термини имају скоро исто значење, али са различитим техникама. Сајбер криминал напредује невероватно брзим темпом, са новим трендовима који се стално појављују. Сајбер криминалци постају агилнији, искоришћавају нове технологије муњевитом брзином, прилагођавају своје нападе новим методама и сарађују једни са другима на начине које до сада нисмо видели.

Сајбер криминал у данашњем свету технологије увелико расте. Злочинци светске мреже искоришћавају личне податке корисника интернета за своју корист.

Они зарањају дубоко у мрачну мрежу да купују и продају илегалне производе и услуге. Они чак добијају приступ поверљивим државним информацијама.

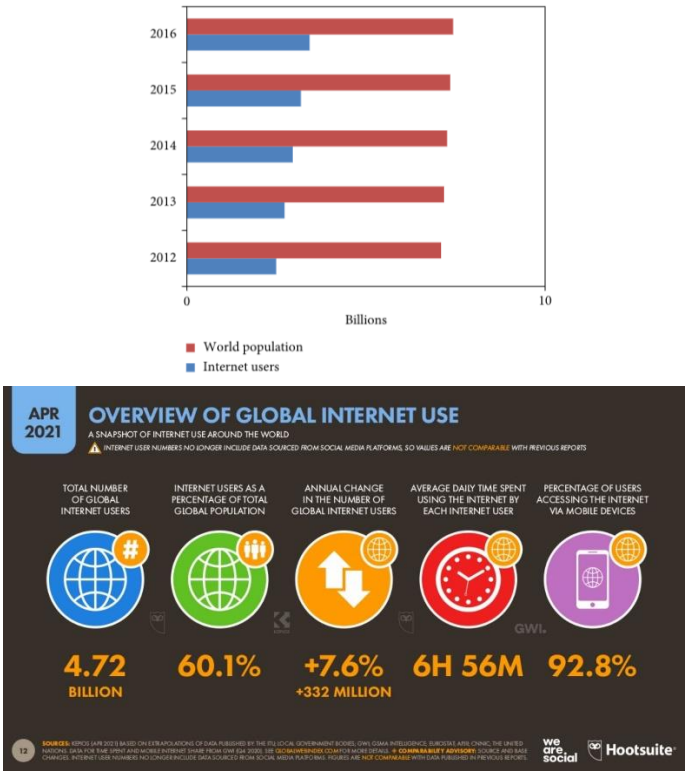
Криминални профил је психолошка процена направљена без познавања идентитета злочинца. Укључује карактеристике личности, а може чак и физичке карактеристике. *Уклапање профила* не значи да је особа починила злочин, али профилисање помаже да се сузи поље осумњичених и може помоћи да се неке особе искључе из сумње. Профилери користе и статистичке податке (индуктивно профилисање) и тестирање хипотеза *здравим разумом* (дедуктивно профилисање) да би формулисали профиле. Профилисање је само један од многих алата који се могу користити у истрази.

Рад је подељен на неколико делова. Поред уводног и закључног дела, у раду постоје два поглавља са својим целинама.

Први део рада односи се на сајбер криминалитет у коме се даје таксономија сајбер криминалитета – где су подробније објашњени сви облици сајбер криминалитета. У раду су као најчешћи појавни облици компјутерског криминалитета детаљније описане *компјутерске крађе и преваре, неовлашћено прибављање информација уз помоћ компјутера, компјутерска саботажа и тероризам, повреде интелектуалне својине, узнемиравање на мрежи и сајбер ухођење.* У другом делу говори се о профилисању сајбер починилаца где се превасходно врши класификација мотива почининаца јер је разумевање мотивације сајбер криминалаца корисно је за испитивање сајбер криминала. У раду детаљније приказујемо како *новац, емоције, сексуални импулси, политика, религија, забава* као мотиви за извршење сајбер криминала утичу на извршење кривичног дела сајбер криминалитета. У последњем делу рада говоримо конкретније о самом стварању профила сајбер криминалаца, где приказујемо и резултате једног спроведеног истраживања који нам показују социо – демографске карајтеристике (*пол, старосно доба, образовање и раније почињена кривична дела*) починиоца сајбер криминала у Србији.

Дефинисање основних појмова

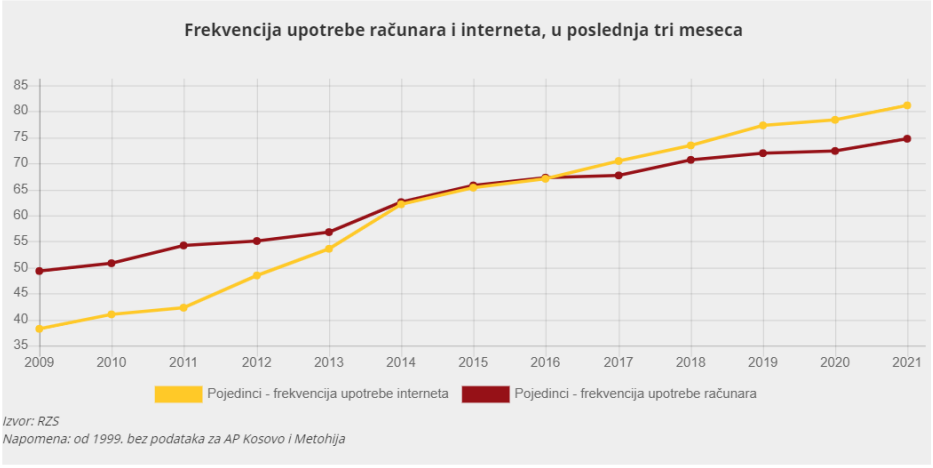
Мрежна инфраструктура је основа за размену информација међу појединцима, приватним секторима, војним и владиним секторима. Приближно 50% светске популације има интернет везу до јануара 2017. Број корисника интернета је у порасту од 10% од јануара 2016. до јануара 2017. [1]Према другом извору у 2016. години има 6,4 милијарде повезаних уређаја и те године су постављене претпоставке да ће број достићи 20,8 милијарди до 2020.[2]Садашње светске технологије хардвера и софтвера дају нова крила процесу повезивања различитих уређаја (*мобилних и паметних сатова*) са Интернетом. Свако може да добије, види и дели информације на Интернету са било ког места на овом свету. Постоји огроман раст уређаја повезаних на Интернет од прошлости до садашњости који стварају подручје сајбер простора. Раст броја корисника интернета у свету и светске популације приказан је на слици 1.



Слика 1.*Корисници интернета у свету*[3]

[1]Интернет извор https://wearesocial.com/special-reports/digital-in-2017-global-overview датум приступа: 20.12. 2021.
[2]Интернет извор http://www.gartner.com/newsroom/id/3165317 датум приступа: 24.12. 2021.
[3]Интернет извор слике: https://smartlife.mondo.rs/tech/platforme/a27438/koliko-ljudi-na-svetu-koristi-internet-i-drustvene-mreze.html датум приступа: 22.12. 2021.

За годину дана број Интернет корисника је порастао за невероватних 300 милиона и стигао до 4,7 милијарди људи на почетку априла месеца 2021. Од укупних 7,85 милијарди људи на свету, то је око 60% глобалне популације. Интересантно је и да од 4,7 милијарди људи на Интернету, чак 4,33 милијарде поседују друштвене мреже, и да је у последњих годину дана забележен раст од невероватних пола милијарде нових корисника.



Фреквенција употребе рачунара и Интернета у последња три месеца у Србији[4]

Говорећи о појму глобалне безбедности Радослав Гаћиновић у свом раду „Класификација безбедности“ износи следећи став: „Процес глобализације имао је за последицу и неке деструктивне појаве које су изазвале регионалне и локалне напетости и конфликте. Нови изазови, ризици и претње безбедности условљени су све израженијим разликама у економском развоју појединих држава и народа. Савремени свет је због тога постао оптерећен многим неизвесностима, с тим што је његово главно обележје у области безбедности смањење опасности од традиционалних војних сукобљавања и директног конфронтирања великих сила, с једне стране, и појава мноштва нових невојних изазова, ризика и претњи, с друге стране.”[5]

[4]Интернет извор слике: https://www.stat.gov.rs/sr-Latn/oblasti/upotreba-ikt/upotreba-ikt-pojedinci датум приступа: 22.12. 2021.
[5] Гаћиновић Радослав (2007). *Класификација безбедности,* Наука, безбедност, полиција, 2/07, стр. 21.

Редни број	ИЗАЗОВИ, РИЗИЦИ И ПРЕТЊЕ	СТЕПЕН ИНТЕЗИТЕТА		
		Краткорочни	средњорочни	Дугорочни
1.	Агресија	НИЗАК	НИЗАК	НИЗАК
2.	Оружане побуне	ВИСОК	СРЕДЊИ	СРЕДЊИ
3.	Сепаратистичке тежње	ВИСОК	СРЕДЊИ	СРЕДЊИ
4.	Тероризам	ВИСОК	СРЕДЊИ	СРЕДЊИ
5.	Организовани криминал	ВИСОК	СРЕДЊИ	СРЕДЊИ
6.	Етничке напетости	ВИСОК	СРЕДЊИ	СРЕДЊИ
7.	Национални и верски екстремизам	ВИСОК	СРЕДЊИ	СРЕДЊИ
8.	Илегалне миграције становништва	СРЕДЊИ	СРЕДЊИ	СРЕДЊИ
9.	Природне непогоде и индустријске и друге катастрофе	ВИСОК	СРЕДЊИ	СРЕДЊИ
10.	Сајбер претње	НИЗАК	СРЕДЊИ	ВИСОК

Изазови, ризици и претње и степен интензитета[6]

До данас је незнатан број аутора покушао да објасни природу сајбер напада, међутим нико од њих није успео да дође до јаснијег закључка каква ће бити њихова природа у будућности.[7] Из историјске перспективе, сваки технолошки напредак довео је до стварања нових концепата који су постали веома важни за теоретичаре националне безбедности. Након авијације, нуклеарног и термонуклеарног оружја и дефинисања свемира као простора у којем могу да се одвијају сукоби, *сајбер* је постао нови популарни термин у литератури која се бави питањима безбедности. Иако су првобитни творци интернета, као глобалне мреже која је и покренула сајбер као феномен, видели само позитивне стране у смислу лакшег умрежавања и размене података, сајбер је донео и велики број нових безбедносних изазова и претњи, између осталог и претњу сукоба између држава у сајбер сфери. Постоји сагласност да сајбер напади заиста представљају праву опасност за националну безбедност, и да је у питању **савршено стратешко оружје** за државе, пошто отвара нове могућности ратовања.[8]

Сајбер напади су постали један од највећих проблема на свету. Они свакодневно наносе озбиљне финансијске штете земљама и људима. Пораст сајбер напада такође доноси сајбер криминал. Сајбер криминал се дефинише као

[6] *Стратегијски преглед одбране Републике Србије*, 2009, стр.18.
[7] Liff, Adam P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies 35 no.3
[8] Geers, Kenneth (2010).*Sun Tzu and Cyber War*, NATO Cooperative Cyber Defence Centre of Excellence

злочин где је рачунар предмет злочина или се користи као средство за извршење кривичног дела. Сајбер криминалац може да користи уређај да приступи личним подацима корисника, поверљивим пословним информацијама, државним информацијама или да онемогући уређај. Такође је сајбер криминалитет продати или извући горе наведене информације на мрежи. Злонамерна веза са хаковањем први пут је документована 1970 – их када су рани компјутеризовани телефони постали мета. Технолошки упућени људи познати као *фрикери* пронашли су начин да плате међуградске позиве кроз низ кодова. Они су били први хакери који су научили како да експлоатишу систем модификовањем хардвера и софтвера да би украли телефонско време на даљину. Ово је навело људе да схвате да су компјутерски системи рањиви на криминалне активности и што су системи постајали сложенији, то су били подложнији сајбер криминалу 1990. године је откривен велики пројекат под називом Операција *Sundevil.* Агенти FBI запленили су 42 компјутера и преко 20.000 дискета које су криминалци користили за илегално коришћење кредитних картица и телефонских услуга. У овој операцији учествовало је преко 100 FBI агената и требало је две године да се уђе у траг само неколицини осумњичених. Међутим, то је виђено као велики напор у односима с јавношћу, јер је то био начин да се покаже хакерима да ће бити праћени и кривично гоњени. Фондација *Electronic Frontier* је формирана као одговор на претње јавним слободама које се дешавају када органи за спровођење закона погреше или учествују у непотребним активностима на истрази сајбер злочина. Њихова мисија је била да заштите и бране потрошаче од незаконитог кривичног гоњења. Иако је био од помоћи, такође је отворио врата за хакерске рупе и анонимно прегледавање где многи криминалци практикују своје нелегалне услуге. Криминал и сајбер криминал постају све већи проблем у нашем друштву, чак и са постојећим системом кривичног правосуђа. И у јавном веб простору и у мрачном вебу, сајбер криминалци су веома вешти и није их лако пронаћи. Због раног и широко распрострањеног усвајања рачунара и интернета у Сједињеним Државама, већина најранијих жртава и зликоваца сајбер криминала били су Американци. До XXI века, међутим, једва да је остало засеоке било где у свету које није било дирнуто сајбер криминалом ове или оне врсте.[9]

[9]Интернет извор: https://www.britannica.com/topic/cybercrime датум приступа: 22.12. 2021.

Сајбер безбедност више не може да се посматра одвојено од безбедности у реалном свету. Штета која настане као резултат сајбер напада је врло стварна и изазива стварне последице и у физичком свету. Ипак, због специфичности везаних за технологију, врсте, починиоце и жртве оваквих напада питање сајбер безбедности захтева посебну бригу свих који се баве Интернетом.

Може се рећи да је сајбер криминал присутан од самих зачетака Интернета. Наиме, упоредо са развојем рачунарских мрежа (РМ) и Интернета као система глобалне мреже, нарасле су и претње од различитих напада са њега (*као што су бројни малициозни програми, социјални инжињеринг, напади хакера, кракера, вандала, компјутерских терориста*). Ослонцем на злоћудне програме (*вирусе, компјутерске црве, тројанце*) врше се упади у персоналне компјутере, компјутерске системе и паметне телефоне, краду профили на друштвеним мрежама, краду подаци са Интернет банкарства.

Постоје три главне категорије у које спада сајбер криминал: појединац, власништво и влада. Врсте коришћених метода и нивои тежине разликују се у зависности од категорије.

Имовина: Ово је слично случају у стварном животу када криминалац незаконито поседује банковне податке или податке о кредитној картици појединца. Хакер краде нечије банковне податке да би добио приступ средствима, обавио куповину на мрежи или покренуо преваре како би натерао људе да одају своје податке. Такође би могли да користе злонамерни софтвер да би добили приступ веб страници са поверљивим информацијама.

Појединац: Ова категорија сајбер криминала укључује једну особу која дистрибуира злонамерне или незаконите информације на мрежи. Ово може укључивати сајбер ухођење, дистрибуцију порнографије и трговину људима.

Влада: Ово је најређи сајбер криминал, али је најтежи прекршај. Злочин против владе познат је и као сајбер тероризам. Овај вид криминала укључује хаковање владиних веб локација, војних веб страница или дистрибуцију пропаганде. Ови криминалци су обично терористи или непријатељске владе других нација.

Радна група експерата под овим криминалом подразумева *криминал који се односи на било који облик криминала који се може извршавати са компјутерским системима и мрежама, у компјутерским системима и мрежама или против компјутерских система и мрежа.*

То је, у суштини, **криминал који се одвија у електронском окружењу.**

Циљ напада – нападају се сервиси, функције и садржаји који се на мрежи налазе. Краду се услуге, подаци или идентитет, оштећују се или уништавају делови или цела мрежа и компјутерски системи, или се ометају функције њиховог рада. У сваком случају циљ починилаца је мрежа у коју се убацују вируси или црви, обарају сајтови, упадају хакери, врши се *одбијање услуга.* **Алат** – криминалци од памтивека користе камен, нож, отров, пиштољ и слична оружја и оруђа, а данас модерни криминалци не *прљају* руке користећи мрежу у чињењу дела и реализовању намера. Некада ова употреба мреже представља потпуно нови алат, док се у другим приликама већ постојећи толико усавршава да га је тешко и препознати (*чак се спомињу и две варијанте: нова дела са новим алатима и стара дела са новим алатима*). Коришћење овог новог оружја нарочито је популарно код дечије порнографије, злоупотреба интелектуалне својине или онлине продаје недозвољене робе (дроге, људских органа, деце, невеста, оружја). **Окружење** у коме се напади реализују – најчешће то окружење служи за прикривање криминалних радњи, као што то веома вешто успевају да ураде педофили, а ни други криминалци нису ништа мање успешни. **Доказ**– као што се у класичном криминалу појављује нож, отров, пиштољ или неко друго средство извршења дела, тако се и мрежа и ICT могу јавити у доказном поступку за сајбер криминал. Истовремено, компјутерска мрежа служи као мрежа за повезивање разних субјеката, она је подршка и симбол. Ова последња улога је везана за застрашивање, обмањивање, уплитање.

Већина сајбер криминала је напад на информације о појединцима, корпорацијама или владама. Иако се напади не дешавају на физичком телу, они се дешавају на личном или корпоративном виртуелном телу, што је скуп информационих атрибута који дефинишу људе и институције на Интернету. Другим речима, у дигиталном добу наши виртуелни идентитети су суштински елементи свакодневног живота: *ми смо скуп бројева и идентификатора у више*

компјутерских база података у власништву влада и корпорација. Сајбер криминал наглашава централну улогу умрежених рачунара у нашим животима, као и крхкост таквих наизглед чврстих чињеница као што је индивидуални идентитет.

САЈБЕР КРИМИНАЛИТЕТ

Компјутерски криминалитет подразумева и активно и пасивно коришћење компјутера, па чак и чување доказа о извршеном кривичном делу у рачунару или у електронској форми,[10]а жртве и могуће жртве су сва физичка иправна 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."[11]

Термин *сајбер простор* први је употребио Вилијам Џибсон у научно – фантастичној новели Neuromanser 1984.[12] Термин *Cyberspace* 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 компјутерске мреже, односно глобална информациона инфрестуктура кроз коју се врши масовна комуникација и у којој истовремено постоје виртуелно

[10] Report and Guidance on Privacy in Social Network Services *Rome Memorandum* - 43rdmeeting,3-4March2008, Rome (Italy),http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf датум приступа: 15.12. 2021.
[11] Димовски Дарко, *Компјутерски криминалитет,*Правни факултет Универзитета у Нишу, зборник, LV, стр. 197-214, стр. 197.
[12] Радновић,Бранислав,Илић,Милена,Радовић,Немања (2012).*ЕкономскисајберкриминалуСрбији–аспектзаштитеинтернетпотошача*,Зборникрадова,међународнанаучностручнаконференција,Сузбијањекриминалаиевропскеинтеграцијесосвртомнавискотехнолошкикриминал,стр. 129.,http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf датум приступа: 15.12. 2021.

и реално.[13]Према једној дефиницији, компјутерски криминалитет представља такав облик криминалног понашања код кога се коришћење компјутерске технологије иинформационих система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, чиме се остварује нека у кривично-правном смислу 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.[14]Према прогнози стручњака, сајбер криминал прелазиће целокупно тржиште лекова у 2021. години и штета ће бити шест билиона широм света.[15] 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.[16]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

[13] Жунић Павловић, Весна, Ковачевић Лепојевић, Марина (2009). *Интерперсонално насиље у cybernpростору*,Истраживањауспецијалнојпедагогији,факултетзаспецијалнуедукацијуирехабилитацију,Београд,стр.227.
[14] K. Jaishankar (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, FL, USA: CRC Press, Taylor and Francis Group, 2011)
[15] 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.
[16] 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-reportдатум приступа: 17.12. 2021.

земљама у којима се већина корисника интернета осећа добро информисано, поверење у интернетску несигурност и немогућност да се заштите повећавају.[17]Проблем сајбер криминала одређује се брзим развојем, применом и употребом информационих технологија, као и употребом ових технологија за кривичне сврхе. На пример, брз развој технологија рачунања у облаку такође отвара повољно окружење за сајбер криминалне радње.

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, констатовано је да је могуће препознати две врсте компјутерског криминалитета:[18]

компјутерски криминалитет у ужем смислу	који подразумева свако незаконито понашање усмерено на електронске операције сигурности компјутерских 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

[17] Special Eurobarometr 390 Cyber Security. Report. 2012. http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdfдатум приступа: 17.12. 2021.
[18] Никић,Срђан:*Најчешћеметоденападасуберкриминалацаикакоседобранити*, http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdfдатум приступа: 15.12. 2021.

	мрежама , компјутерска шпијунажа)
компјутерски криминалитет у ширем смислу	који подразумева сваконезаконито 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 на то да ли је мотив за њихово извршење стицање материјалне користи (интернет прогањање, сајбер тероризам).[19]

Специфичности компјутерског криминалитета и оперативног рада по компјутерским кривичним делима, захтевају одређени вид специјализације оперативних радника који раде на сузбијању овог вида криминалитета. У

[19] Тањевић, Наташа (2009). *Компјутерски криминал − правна заштита нанационалном нивоу*, Безбедност - Часопис Министарства унутрашњихпословаРепублике Србије,број1-2/2009,стр.152-166, стр. 157.

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.*[20]

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 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*

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

класичних облика криминалитета где учинилац углавном мора да буде на месту извршења кривичног дела.[21]

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 његови учиниоци 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.[22]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). [23]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

[21]Матијевић, М., Бошковић, М. (2007). *Криминалистика оперативa*, Бања Лука, стр. 399–403.
[22] 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 датум приступа: 22.12. 2021.
[23] 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.

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.[24] Smith, Grabosky и Urbas (2004)[25] 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.

Сајбер криминалитет: таксономија

Поплава личних мрежних уређаја створила је експоненцијални раст личних података на Интернету. Према једном извештају, претпоставка је била да ће број уређаја наставити да расте и по обиму и у разноврсности, а предвиђају да ће овај број достићи 200 милијарди до 2020. године и наставити да расте у будућности. Дакле, сајбер простор се свакодневно шири. Ова експанзија је довела до различитих могућности за сајбер криминалце да чине злонамерне радње на Интернету, а такође је довела до нивоа потешкоћа за професионалце у области безбедности да поставе безбедносни *кишобран* на цео сајбер простор. Из горње дискусије је јасно да сајбер простор има огроман обим података и информација који су доступни на Интернету и да његови ресурси морају бити заштићени од сајбер криминалаца.[26]

Данас је постало изузетно тешко обезбедити безбедност наших система, укључујући и корпоративне и личне податке. Велике земље, попут Сједињених Држава и Уједињеног Краљевства, боре се са сајбер нападима и злочинима тако

[24] Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2012). Incarceration or community placement: examiningthe sentences of cybercriminals. Criminal Justice Studies, 25(1), 33-40.
[25] Smith, R. G., Grabosky, P., & Urbas, G. (2004). Cyber Criminals on Trial. Cambridge, UK: CambridgeUniversity Press.
[26] Report of McAfee Labs 2016 Threat Predictions by Intel Security, November 2016.

што производе различите безбедносне стратегије.[27]Земље настоје да обезбеде безбедност у сајбер простору и прилагоде се овој области.[28]Заштита критичне инфраструктуре има витални значај за земље. Хемијски, финансијски, здравствени и енергетски сектори, чак и нуклеарне електране у неким земљама могу се убројати у њих.[29]Због милиона сајбер напада, финансијски губици значајно расту из дана у дан.[30]

2020. године подаци украдени из информационог система компаније *Airbus* стављени су на тржиште црног веба. Украдени су медицински подаци милиона људи, а чак је и проглашено ванредно стање због напада на неке градове.[31]

Најважнији елементи који обезбеђују сајбер безбедност су *интегритет, поверљивост, аутентификација, ауторизација, непорицање и доступност*.[32]Сваким даном радна снага постаје недовољна у борби против сајбер инцидената и траже се нова решења. Решења као што су аутономни системи сајбер одбране архитектура помоћника за паметну сајбер безбедност и системи за откривање упада се истражују у борби против сајбер напада и злочина. Значај борбе против оваквих сајбер напада, сајбер злочина и сајбер безбедности је истакнут у различитим студијама. Сајбер безбедност је заштита физичко–дигиталних података, мрежа и технолошких система од сајбер напада, неовлашћених приступа, прекида, модификација, уништења и оштећења кроз различите процесе, апликације и примењене технологије.[33]Сајбер напади као што су дистрибуирани напади ускраћивања услуге слањем злонамерних пакета phishing напади (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) на сајтове за банкарство и

[27]Reid & Van Niekerk (2014) Reid R, Van Niekerk J. *From information security to cyber security cultures—information security for South Africa.* Piscataway: IEEE; 2014. pp. 1–7.
[28] Goel (2020) Goel S. *National cyber security strategy and the emergence of strong digital borders.* Connections: The Quarterly Journal. 2020;19(1):73–86.
[29]CISA (2020) CISA Critical infrastructure sectors. 2020. https://www.cisa.gov/critical-infrastructure-sectorshttps://www.cisa.gov/critical-infrastructure-sectors датум приступа: 15.12. 2021.
[30] Jang-Jaccard & Nepal (2014) Jang-Jaccard J, Nepal S. *A survey of emerging threats in cybersecurity*. Journal of Computer and System Sciences. 2014;80(5):973–993.
[31]Check Point Security Report (2020) Check Point Security Report Check point research. 2020. https://research.checkpoint.com/https://research.checkpoint.com/ датум приступа: 04.12. 2021.
[32]Bayuk et al. (2012) Bayuk JL, Healey J, Rohmeyer P, Sachs MH, Schmidt J, Weiss J. *Cyber security policy guidebook*. Hoboken: Wiley; 2012. pp. 3–4.
[33]Fischer (2009) Fischer EA. *Creating a framework for cybersecurity: an analysis of issues and options*. Hauppauge: Nova Science Publishers; 2009.

куповину који обмањују корисника значајно су порасли.[34]Поред тога, нападачи све чешће користе злонамерни софтвер за нападе (*вирус, црве, тројанце, шпијунски софтвер*) који се инсталира на корисников рачунар без икакве сагласности корисника.[35]Опет, најчешћи од ових напада и један од напада које је најтеже спречити су напади социјалног инжењеринга. Они се заснивају на техничкој вештини, лукавству и убеђивању, направљеним искоришћавањем слабости жртве. Кевин Митник, један од светских познатих хакера у нападима друштвеног инжењеринга, продро је у већину система које је напао овом методом.[36]У раду Бреда, Барбоса и Мораиса овај напад се помиње као једна од највећих безбедносних рањивости у систему без обзира колико је технички систем безбедан.[37]Исто тако, напади на ИоТ уређаје, који су нагло порасли последњих година, значајно утичу на друштво. Дакле, нападе и претње ИоТ структури треба разумети у безбедносне сврхе.[38]Студије спроведене ради разумевања и борбе против сајбер напада откривају важност предвиђања злочина.

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

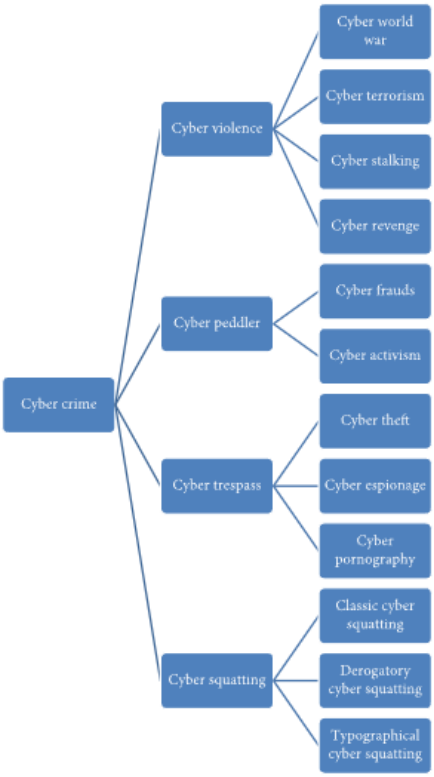
Забава	Неки сајбер криминалци обављају своје активности сајбер напада да би тестирали своје хакерске способности. Осећају понос и радост у својим успешним покушајима. Спремни су да стекну славу у свету сајбер криминалаца. Осећају радост и понос када изврше напад који није извео ниједан други нападач или други нападачи нису успели да изведу тај напад.
Хактивисти[39]	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

[34] Sahingoz et al. (2019) Sahingoz OK, Buber E, Demir O, Diri B. *Machine learning based phishing detection from URLs. Expert Systems with Applications*. 2019;117(4):345–357.
[35]Biju, Gopal & Prakash (2019) Biju JM, Gopal N, Prakash AJ. *Cyber attacks and its different types.* International Research Journal of Engineering and Technology. 2019;6(3):4849–4852.
[36] Mitnick & Simon (2009) Mitnick KD, Simon WL. *The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers.* Hoboken: John Wiley & Sons; 2009.
[37] Breda, Barbosa & Morais (2017) Breda F, Barbosa H, Morais T. *Social engineering and cyber security.* International Technology, Education and Development Conference. 2017;3(3):106–108.
[38] Kagita et al. (2020) Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PKR, Singh S. A review on cyber crimes on the Internet of Things. http://arxiv.org/abs/2009.05708arXiv датум приступа: 04.12. 2021.
[39]*Особа која добија неовлашћени приступ компјутерским датотекама или мрежама у циљу остваривања друштвених или политичких циљева*.

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

Најчешћи циљеви сајбер нападача

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.

Сајбер насиље – насиље које се ствара у стварном свету уз помоћ компјутерског система или било ког уређаја (попут мобилног) повезаног на Интернет је познато као сајбернасиље. Тамо где је присутна реч *насиље*, биће

присутан и њен ефекат у смислу штете. У свету сајбер система, компоненте које могу бити оштећене су уређаји повезани на Интернет, подаци на серверима, информације на Интернету и сваки појединац или организација која може бити уништена сајбер насиљем.[40]Постоје различити облици сајбер – насиља од којих су најчешћи размотрени у наставку.

Сајбер светски ратима максималан ниво насиља које делује међу разним земљама света. Сајбер светски рат чини сваког појединца, војску, државу, хакере и државне и приватне службенике. Циљ је да поквари, онемогући или уништи инфраструктуру и ресурсе засноване на Интернет систему ривалске или непријатељске земље. У овом рату, свака врста сајбер напада се користи за постизање победе над циљном земљом.

Сајбер тероризам– постоје неки људи или групе које имају само за циљ да униште човечанство, познати су као терористи. Они верују да то раде да би своју религију учинили моћнијом у свету или имају само право да заповедају светом или нико други не може бити јачи од њих. Овакав тероризам у дигиталном свету познат је као сајбертероризам. Немају емоције или симпатије. Они су као машине чији је циљ у њих убачен. Они могу користити било коју врсту сајбер напада да би испунили свој циљ.

Сајбер узнемиравање – је злочин у коме неко узнемирава или уходи жртву користећи електронска или дигитална средства, као што су друштвени медији, е–пошта, инстант поруке или поруке постављене на дискусиону групу или форум. Сајберпрогонитељи користе предност анонимности коју пружа интернет да уходе или узнемиравају своје жртве, понекад без да буду ухваћени, кажњени или чак откривени.[41]

Сајбер освета – освета значи повредити некога као одговор на нечију претходну акцију. Циљ сајбер освете је да уништи непријатеља на различите начине, као што је разоткривање њихових поверљивих информација, уништавање њихове рачунарске инфраструктуре и ресурса и стварање њихове лажне слике на Интернет систему. Циљ сајбер освете је да се украду и промене поверљиве информације непријатеља за његове интересе.

[40]M. Yar, *Cybercrime and Society*, SAGE Publications, Thousand Oaks, CA, USA, 2013.
[41]Интернет извор: http://searchsecurity.techtarget.com/definition/cyberstalking датум приступа: 01.12. 2021.

Сајбер разносачи – радња нечег незаконитог или крађе нечијих поверљивих података уз помоћ рачунарског система повезаног на Интернет. У основи постоје две врсте сајбер злочина у овој категорији, а то су: *сајбер превара* и *сајбер активизам.*

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.

Сајбер активизам – то је најновија врста злочина. У овој врсти криминала, друштвене и комуникационе апликације засноване на Интернету се користе за креирање, управљање и управљање активизмом као што је бржа комуникација са људима или дистрибуција информација широкој публици за неколико секунди. Комуникационе технологије које се користе у овом активизму су Twitter, Facebook, YouTube, LinkedIn, Whatsapp, Gmail итд. Ове технологије су направљене за добре сврхе као што су боља повезаност са пријатељима, колегама и запосленима и лако ширење најновијих информација на огромном географском подручју. Али неки људи користе ове технологије за ширење гласина како би оштетили имиџ свог ривала или ширили лажне информације о својој организацији или појединцима како би добили различите врсте користи.[42]

Сајбер преступ– преступ значи прелазак граница за које неко није овлашћен. То је злочин у коме се крши сајбер закон хаковањем овлашћеног корисничког система. Ова врста напада нарушава поверљивост и интегритет који су фундаментални за сајбер безбедност.[43]

Сајбер крађа – крађа значи да постоји страх од нечег важног што може бити оштећено или украдено. У стварном животу, крађа или оштећење се врши тако што се физички уђе у нечију кућу или организацију и украде нешто попут датотеке, телевизије, злата и тако даље. Али у случају сајбер света, он се

[42]Kumar, G., Kaur, A., Sethi, S. (2014). *Computer network attacks–a study*, International Journal of Computer Science and Mobile Applications, vol. 2, no. 11, pp. 24–32
[43] D. Wall, *Crime and the Internet*, Routledge, Abingdon, UK, 2003.

разликује од стварног света. 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. *Сајбер шпијунажа* – позната је и као сајбер шпијунирање. То је чин праћења активности појединца, компаније, организације, земље, непријатеља или ривала вршењем злонамерних активности на мрежи. То су технички здрави људи које је тешко открити. Нелегално анализирају мрежни саобраћај или могу да хакују сигурносне камере и камере лаптопа како би добили информације о својим метама, односно којој врсти информација приступају, какву врсту посла обављају и када напусте своје радно место или кући.[44]*Сајбер порнографија*је напад у којем нападач објављује сексуални или *голи* материјал своје мете на јавним веб страницама. Нападач може да пронађе приватни материјал своје мете хаковањем циљаног рачунарског система, мобилног телефона, сигурносних камера или таблета. Ова врста излагања приватних слика или видео снимака изазива срамоту за мету нападача, или чак у неким случајевима, мета изврши самоубиство.[45]

Сајбер *сквотер* је сајбер злочин у којем нападач незаконито региструје назив родне марке (жига) других као име домена тако да власник жига не региструје свој жиг као име домена. Различити типови сајбер сквотинга биће поменути у наставку.[46]*Класични сајбер сквотер* – главни циљ сајбер сквотера је да буде плаћен. Када сајбер сквотер добије откупнину од своје мете, он/она продаје или брише име свог домена. Али сада су закони промењени, тако да тренд ове врсте напада данас није много популаран. Погрдно сајбер *сквотирање* – код овог типа, главни циљ сајбер сквотера је да уништи репутацију своје мете.

[44] Kumar, G., Kaur, A., Sethi, S. (2014). *Computer network attacks–a study*, International Journal of Computer Science and Mobile Applications, vol. 2, no. 11, pp. 24–32
[45] Yar, M.(2013). *Cybercrime and Society*, SAGE Publications, Thousand Oaks, CA, USA, 2013.
[46] Sreenivasulu N. S. (2013).*Law Relating to Intellectual Property*, Partridge Publishing, Gurugram, India

Сајберсквотер то ради на различите начине као што је постављање порнографског материјала, говор мржње или нарушени садржај на том називу домена. Типографски сајбер *сквотинг* – уовој врсти напада, нападач не може да користи исто име као жиг јер се власник жига већ регистровао за име домена. Дакле, у овом случају, нападач се региструје са именом веома сличним оригиналном називу жига. На пример, ако нападач региструје име домена Gmail – а које је веома слично Gmail – у, онда он може успети да нанесе губитак оригиналном власнику жига.[47]

Најчешћи појавни облици компјутерског криминалитета

Као што је горе поменуто, постоји много различитих врста сајбер криминала. Већина сајбер криминалитета се спроводи са очекивањем финансијске добити од стране нападача, иако начини на које сајбер криминалци желе да буду плаћени могу варирати.

Најчешћи појавни облици компјутерског криминалитета јесу: компјутерске крађе,компјутерскеп реваре, неовлашћено прибављање информација уз помоћ компјутера, неовлашћено прибављање или уништење информација садржаних у компјутеру, онемогућавање или отежавање приступа таквим информацијама (компјутерска саботажа), компјутерски тероризам."[48]

Неке специфичне врсте сајбер злочина укључују следеће:

Сајбер изнуда	Злочин који укључује напад или претњу нападом заједно са захтевом за новцем за заустављање напада. Један облик сајбер изнуде је напад ransomware – а. Дакле, то је врста злонамерног софтвера дизајнираног да блокира приступ рачунарском систему док се не исплати одређена сума новца. Иако је обично усмерен на појединце, само је питање времена када ће и компаније бити на мети. Дакле, овде нападач добија приступ

[47]Sreenivasulu N. S. (2013). *Law Relating to Intellectual Property*, Partridge Publishing, Gurugram, India
[48] Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна,Костић, Миомира (2012). *Криминологија,* 5. измењено и допуњено издање,Ниш:Правнифакултет,Центарза публикације,стр.178-182.

	системима организације и шифрује њене документе и датотеке – све што има потенцијалну вредност – чинећи податке недоступним док се не плати откупнина. Обично је то у неком облику криптовалуте, као што је биткоин.
Crypto jacking	Напад који користи скрипте за рударење криптовалута у претраживачима без сагласности корисника. Ови напади могу укључивати учитавање софтвера за рударење криптовалута у систем жртве. Међутим, многи напади зависе од JavaScriptкода који врши рударење у прегледачу ако претраживач корисника има отворену картицу или прозор на злонамерном сајту. Није потребно инсталирати злонамерни софтвер јер учитавање погођене странице извршава код за рударење у прегледачу.
Крађа идентитета	Напад који се дешава када појединац приступи рачунару како би прикупио личне податке корисника, које затим користи за крађу идентитета те особе или приступ њиховим вредним рачунима, као што су банковне и кредитне картице. Сајбер криминалци купују и продају информације о идентитету на црним интернет тржиштима, нудећи финансијске рачуне, као и друге врсте налога, као што су услуге видео стримовања, веб пошта, видео и аудио стриминг, онлајн аукције и још много тога. Лични здравствени подаци су још једна честа мета крадљиваца идентитета.
Превара са кредитним картицама	напад који се дешава када се хакери инфилтрирају у системе трговаца да би добили информације о кредитној картици и/или банковним подацима купаца. Украдене платне картице се могу купити и продати на велико на црним интернет тржиштима, где хакерске групе које су украле велике количине кредитних картица зарађују продајом сајбер криминалцима нижег нивоа који зарађују преварама са кредитним картицама на индивидуалним рачунима.

Компјутерске крађе

Сада су сви свесни растућег проблема крађе идентитета, то је огроман глобални проблем. Сви лични подаци су невероватно драгоцени за криминалце који их могу користити за отварање банковних рачуна, добијање кредитних картица, зајмова, државних бенефиција и докумената као што су пасоши и возачке дозволе.Било код куће или на послу, људи су сада потпуно свесни да личне информације које поседују, од финансијских извештаја до здравствених картона, морају бити заштићене, морамо битиосигурани да су наше активности на мрежи заштићене заштитним зидовима и антивирусним софтвером.Неке компаније, укључујући банке и болнице, осигуравају да њихови харддискови буду потпуно уништени након употребе због многих нових владиних мандата који присиљавају на заштиту личних података људи.Међутим, све ове мере су узалудне ако сам рачунар буде украден, заједно са харддиском и свим личним датотекама и датотекама клијената.

Ипак, процењује се да се сваке године широм света украде милион рачунара и лаптопова, откривајући личне податке стотина хиљада људи. Нпр. за само последње три године сматра се да је украдено 150 милиона личних досијеа, што је дупло више од целокупне популације Велике Британије. Болнице су међу најугроженијим местима где се рецепције или административне зграде често остављају без надзора. [49]

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.[50]

Али не само предузећа и јавне зграде морају да размишљају о крађи рачунара. Кућни корисници све више користе рачунаре за интернет банкарство и финансијске трансакције, поред чувања личних датотека као што су фотографије. Док ће осигурање покрити трошкове губитка рачунара, и постојању резервних

[49] Romanus Okeke, Mahmood Shah (2016). *Information Theft Prevention, Theory and Practice,* Routledge
[50]Интернет извор: https://www.mcafee.com/enterprise/en-us/products/total-protection-for-data-loss-prevention.html датум приступа: 13.01.2022.

копија свих фајлова, детаљи банковног рачуна, погодно су ускладиштени на машини за приступ сваком криминалцу. Неке компаније су идентификовале проблем и сада су развијени јефтини сефови за рачунаре који могу безбедно да сместе рачунаре, а истовремено омогућавају корисницима да им приступе. Ови сефови су отпорни на неовлашћено коришћење и могу да издрже чак и најиздржљивијег *лопова*. Такође се могу причврстити за под или зидове омогућавајући рачунарима да остану без надзора у јавним просторима и такође обезбеђујући идеалну сигурност за пословне и кућне кориснике, штитећи машине и што је још важније податке које држе.

Крађа идентитетаје 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.[51]

Ови обрасци су лажно представљање као мање зло ако су украдени само лични подаци или налози без сачуваних начина плаћања. Међутим, може 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.[52]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

[51]Carr Indira (2009). *Computer Crime*, School of Law, University of Surrey, UK, Routledge
[52] Romanus Okeke, Mahmood Shah (2016). *Information Theft Prevention, Theory and Practice,* Routledge

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.[53]

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.[54]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 иу 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 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.[55]

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

[53] 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.

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

[55] 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.

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

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. [56]

„Конвенција ЦЕТС 185 предвиђа дело *Рачунарске преваре*и онопредставља кривично дело које чини лице, у намери да прибави имовинску користсеби или другоме, које неовлашћено нанесе штету другоме путем: било каквеизмене, уношења, брисања или сакривања рачунарских података,било каквог утицаја на функционисање рачунарског система.Циљ инкриминисања овог дела је да се

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

спрече манипулације у токупроцесирања података предузете у намери остваривања утицаја на нелегалнитрансфер средстава.Примери које за ово дело наводи приручник су превара платним иликредитним картицама (чл. 225. КЗ) и аукцијске преваре (чл. 208. КЗ). Као предмет напада се све више јављајуелектронски фондови, депозитни новац, е злато, као нови предмети класичногкривичног дела преваре."[57]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.[58]

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

[57]Прља Драган, Ивановић Звонимир, Рељановић Марио (2011). *Кривична дела високотехнолошког криминала*, Институт за упоредно право. Београд, стр. 169.
[58] Gačić, M. (1982). *Kompjuterski kriminal, inostrana iskustva*,13. maj, br. 5, Zagreb

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.[59]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.[60] 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.

Неовлашћено прибављање информација уз помоћ компјутера

У не тако далекој прошлости индустријска шпијунажа се састојала од фотокопирања и преношења досијеа и крађе идентитета, што је до последњих година ретко злочин, који се дешавао када би неко изгубио свој новчаник у џепу. Компјутер и интернет су драматично променили терен. Сада се листе купаца, маркетиншки и стратешки планови и финансијске информације могу пренети конкуренцији једноставним кликом миша, а средњошколски хакер може упасти у рачунаре који чувају мноштво личних података.[61]

[59]National White Collar Crime Center. IFCC 2002 Internet Fraud Report: January 1, 2002- December 31, 2002. http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdfдатум приступа: 01.12. 2021.
[60]Rantala, RR. Cybercrime Against Business. Bureau of Justice Statistics. March 2004.
[61] Цетинић, М. (1998).*Компјутерска кривична дела и њихови појавни облици*, Правни живот, број 10, Удружење правника Србије

„Први облик овог дела чини оно лице које се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступиелектронској обради података, казниће се новчаном казном или затвором до шестмесеци. Радња првог облика састоји се у неовлашћеном укључивању у рачунар, кршењем мера заштите, или у неовлашћеном приступу ЕОП –у. Други, квалификовани, облик чини лице које употреби податак добијен на претходноописан начин, казниће се новчаном казном или затвором до две године. Као јоштежи облик јавља се случај ако је услед дела дошло до застоја или озбиљногпоремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице, учинилац ће се казнити затвором до тригодине.”[62]

„У нашем законодавству у првом облику кривично дело *Неовлашћено коришћење рачунара или рачунарске мреже*чини оно лицекоје неовлашћено користи рачунарске услуге или рачунарску мрежу у намери дасеби или другом прибави противправну имовинску корист. За ово дело запрећењаје новчана казна или затвор до три месеца. Такође, је предвиђено да се гоњење заово дело предузима се по приватној тужби. Радња кривичног дела је одређена каонеовлашћено коришћење рачунарских услуга или рачунарске мреже. Ово јесувише широко постављена формулација, што може довести до значајнихзлоупотреба. За постојање овог кривичног дела је неопходно утврдити и намеруизвршиоца да себи или другом прибави противправну имовинску корист. Извршилац може бити свако лице, а у погледу виности потребан је директанумишљај.”[63]Неовлашћени приступ је предуслов за многе облике компјутерског криминала и компјутерске преваре. Овај облик криминала представља електронски упад или добијање приступа ресурсима преко рачунарског ресурса без дозволе. До неовлашћеног приступа може доћи како на личним рачунарима појединаца, тако и на радном месту.

Један од главних облика неовлашћеног приступа је познат као хаковање. Хаковање је *чин стицања неовлашћеног приступа рачунарском систему или мрежи и у неким случајевима неовлашћено коришћење овог приступа*.[64]Као што је

[62]Прља Драган, Ивановић Звонимир, Рељановић Марио (2011). *Кривична дела високотехнолошког криминала*, Институт за упоредно право. Београд, стр. 174.
[63]Лазаревић, Љ. (2006). *Коментар кривичног законика Републике Србије*, Савременаадминистрација, Београд, стр. 751.
[64]Rushinek, A, Rushinek, SF. (1993). U*sing Experts for Detecting and Litigating Computer Crime*. Managerial Auditing Journal. 19-22.

раније речено, неовлашћени приступ може бити пролаз за чињење других прекршаја. Случај неовлашћеног приступа који је истражио Федерални истражни биро укључује Алексеја В. Иванова, који је, између осталог, оптужен за компјутерски упад, компјутерску превару и изнуду.

Те оптужбе су произашле из активности Иванова и других који су пословали из Русије и хаковали десетине рачунара широм Сједињених Држава, крали корисничка имена, лозинке, податке о кредитним картицама и друге финансијске податке, а затим изнуђивали те жртве претњом брисања њихових података и уништавања њихових компјутерских система.[65]

Као што се може видети у овом случају, неовлашћени приступ рачунарским ресурсима је био сам по себи оптужба, као и метод за чињење већих, сложенијих кривичних дела у вези са рачунаром.

Заштита се може обавити на неколико начина. Прво, у рачунарску мрежу могу се уградити правила ко може, а ко не може да користи одређене податке. Заштита лозинком, на пример, може олакшати политику *потребе да се зна* која ограничава приступ онима који морају да користе одређене информације у обављању својих послова. Ограничења лозинки, међутим, постају бесмислена када се рачунарски подаци могу копирати на дискету или штампати у неограниченом броју копија. Да би се избегли ови проблеми, компанија би могла размислити о покретању апликације за документе која се може прилагодити тако да забрани штампање. У већини пословних окружења забрана копирања није практично решење, копирање информација на флопи дискове може се спречити једноставним онемогућавањем и забраном употребе флопи драјвова на радном месту, али то не спречава некога да преузме информације на усб привезак за кључеве. Наравно, још један практичнији начин заштите рачунарских податакајесте шифровање података. Сада на тржишту постоје и софтверска решења која могу помоћи компанијама у креирању ауторизације над одређеним подацима у рачунарској мрежи.

Сајбер шпијунажа –злочин који укључује сајбер криминалца који хакује системе или мреже да би добио приступ поверљивим информацијама које држи влада или друга организација. Напади могу бити мотивисани профитом или

[65]Department of Justice. Russian Man Sentenced for Hacking into Computers in the United States. http://www.cybercrime.gov/ivanovSent.htmдатум приступа: 01.12. 2021.

идеологијом. Активности сајбер шпијунаже могу укључивати сваку врсту сајбер напада за прикупљање, модификовање или уништавање података, као и коришћење уређаја повезаних на мрежу, као што су веб камере или ТВ камере затвореног круга, за шпијунирање циљаног појединца или групе и надгледање комуникације, укључујући е–поруке, текстуалне поруке и тренутне поруке.

Компјутерска саботажа

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.[66]

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 одређени број пута,

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

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. [67]

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 (заправо самостални програм који се зове *црв*) заразио је приближно 6.000 војних, корпоративних и универзитетских рачунара.[68]

Компјутерски тероризам

Сајбер тероризам (такође 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 да ураде 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.[69]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.

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

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 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.[70]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.*[71]

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

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

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 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. [72]

Повреде интелектуалне својине

Злоупотреба бренда је један од оних израза у индустрији заштите бренда који се широко користи – често уз извесну конфузију и недоследност. То је кровни термин, који се генерално односи на покушај да се искористи репутација бренда треће стране за профит, личну корист или са било којом злонамерном намером. [73]

Ово може доћи у облику преваре кроз незаконито коришћење једног или више елемената интелектуалне својине бренда, као што су жигови, дела заштићена ауторским правима, патенти и други. Повреде интелектуалне својине варирају од продаје фалсификоване робе или реплика, пиратерије садржаја, кршења патента и још много тога.

Фалсификована и реплика робе: производ креиран да изгледа идентично постојећем производу бренда треће стране, док су фалсификати брендирани, реплике нису.Пиратерија је неовлашћено умножавање, копирање и ширење

[72] MacKinnonLachlan, FrangiskatosDimitrios (2013). *Cyber Security Countermeasures to Combat Cyber Terrorism*in Strategic Intelligence Management
[73] Gercke Marco, *Understanding cybercrime: Phenomena, challenges and legal response*, September 2012, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf датум приступа: 10.01.2022.

материјала заштићених ауторским правима.Повреда патента су производи који тачно копирају функционалност и механизам производа заштићених патентима за употребу.Софтверска пиратерија је напад који укључује незаконито копирање, дистрибуцију и употребу софтверских програма са намером комерцијалне или личне употребе. Повреда жига, кршења ауторских права и кршења патента често се повезују са овом врстом сајбер криминала.[74]

Узнемиравање на мрежи и сајбер ухођење

Узнемиравање је нажалост веома распрострањено у данашњем свету, још више када се људи осећају заштићеним анонимношћу коју нам интернет даје. Једно од најбрже растућих и најпознатијих онлајн узнемиравања у последњих неколико година је осветничка порнографија. Узнемиравање на мрежи и малтретирање путем интернета обично су садржани у друштвеним медијима у облику постова, коментара или директних порука, али се може послати и путем е – поште. Главни облик ових порука је углавном клеветнички или претећи, било против једног појединца или групе. Сајбер ухођење је још једна врста узнемиравања која се фокусира на једну особу, коју криминалац помно прати. Вероватно је да се послодавци, колеге и познаници жртве такође контактирају како би клеветали жртву и покушали да извуку више личних података како би продубили активност ухођења.Сајбер прогонитељи обично прибегавају *doxxing* – у ако желе јаче да гурну жртву, што подразумева објављивање личних података жртве са злонамерним намерама, обично у токсичним онлајн заједницама где се надају да ће пронаћи друге који су спремни да се придруже ухођењу.Ови сајбер злочини су изузетно штетни по ментално здравље жртве, а било је више извештаја о жртвама које су развиле менталне болести, па чак и извршиле самоубиство.Заштитити се од тога је прилично једноставно, ове случајеве треба пријавити платформи друштвених медија ако се тамо дешава узнемиравање или ухођење и надлежним органима. Проблем је обично у томе што се жртва може уплашити да пријави ове сајбер злочине у случају да криминалац појача своје напоре и узнемиравање постане још горе, посебно у случају да жртва познаје

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

нападача. Зато је толико важно да околина жртве идентификује овај проблем и реагује на њега.

Неки од најчешће виђених напада сајбер криминала укључују дистрибуиране DoS (DDoS) нападе, који се често користе за гашење система и мрежа. Ова врста напада користи сопствени комуникациони протокол мреже против себе тако што надмашује њену способност да одговори на захтеве за повезивање. [75]DDoSнапади се понекад изводе једноставно из злонамерних разлога или као део шеме сајбер изнуде, али се такође могу користити да одврате организацију жртве од неког другог напада или експлоатације који се изводе у исто време. Инфицирање система и мрежа малвером је пример напада који се користи за оштећење система или наношење штете корисницима. Ово се може учинити оштећењем система, софтвера или података ускладиштених на систему. Напади ransomware – а су слични, али злонамерни софтвер делује тако што шифрује или искључује системе жртава док се не плати откупнина.

Phishing кампање се користе за инфилтрирање у корпоративне мреже. То може бити слањем лажних е–порука корисницима у организацији, подстичући их да преузму прилоге или кликну на везе које затим шире вирусе или малвер на њихове системе и преко њихових система на мреже њихове компаније. Напади на акредитиве су када сајбер криминалац има за циљ да украде или погоди корисничке ID –ове и лозинке за системе жртве или личне налоге. Они се могу спровести коришћењем напада грубом силом инсталирањем софтвера кејлогера или искоришћавањем рањивости у софтверу или хардверу који могу да открију акредитиве жртве.[76]

Сајбер криминалци такође могу покушати да отму веб локацију да би променили или избрисали садржај или приступили или модификовали базе података без овлашћења. На пример, нападач може да користи искоришћавање језика структурираних упита (SQL) за убацивање злонамерног кода у веб локацију, који се затим може користити за искоришћавање рањивости у бази података веб локације, омогућавајући хакеру да приступи и мења записе или добије неовлашћени приступ на осетљиве информације и податке, као што су корисничке

[75] Ignjatović, Đ. *Pojmovno određenje kompjuterskogkriminaliteta,* Anali Pravnog fakulteta, 1-3/91
[76] Gercke Marco, *Understanding cybercrime: Phenomena, challenges and legal response*, September 2012, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf датум приступа: 10.01.2022.

лозинке, бројеви кредитних картица, информације које могу да идентификују личности (PII), пословне тајне и IP.

Други уобичајени примери сајбер криминала укључују *илегално коцкање, продају илегалних предмета, попут оружја, дроге или фалсификоване робе и наговарање, производњу, поседовање или дистрибуцију дечје порнографије.*

ПРОФИЛИСАЊЕ САЈБЕР ПОЧИНИЛАЦА

Профилисање извршиоца кривичног дела представља поступак којим се на основу извршеног злочина доносе закључци о карактеристикама извршиоца. Подаци о карактеристикама злочина добијају се на основу анализе криминалног догађаја. Карактеристике извршиоца се односе на *демографске и физичке карактеристике, образовање, брачни статус, радни статус, карактеристике личности, навике и склоности*. Профилисање је истражни метод у функцији откривања извршиоца кривичног дела, заснован на одговору на питање шта кривично дело говори о лицу које га је извршило.[77]„У том смислу, основ израде профила представљају две основне хипотезе: кривично дело је одраз учиниоца и узрока и услова који су утицали на ток и динамику радње кривичног дела (жртва и детерминанте места и времена), последица кривичног дела је основа за извођење закључака о учиниоцу.”[78]

Стварање профила као низа закључака о карактеристикама извршиоца има за циљ да пружи помоћ у проналажењу извршиоца који није доступан органима кривичног гоњења. Израда првих п*рофила* везује се за четрдесете године XX века, када је направљен профил *бомбардера* у Њујорку који је за 16 година поставио више од 50 стручно направљених бомби. *Профајлера* највише има у Америци и они *уче занат* у Националном центру за анализу кривичних дела. Профилисање представља ментално –логички процес који путем анализе, синтезе и евалуације доказа (*о извршиоцу, месту криминалног догађаја и жртви*) за циљ има израду профила, општих и посебних карактеристика извршиоца (мотивације, психолошких принуда, модус операндија).Највеће заслуге у развоју области

[77]Stefoff, R. (2011). *Criminal Profiling*, New York, 38–70.
[78]Ђурђевић З. и сарадници (2012). *Криминалистичко профилисање,* Београд, стр. 6

профилисања извршиоца имају амерички FBI стручњаци. Они су због потребе решавања тешких и бизарних серијских злочина попут убиства и силовања седамдесетих година прошлог века основали Јединицу за бихевиоралне науке. [79]„Ault и Reese, FBI профајлери, истичу да извршено кривично дело указује на карактеристике личности извршиоца кривичног дела као што наши домови указују на неке карактеристике наше личности.”[80]

„Све технике профилисања, без обзира на терминолошке или разлике у начину спровођења,имају исти циљ, а то је помоћи државним органима који спроводе криминалистичке истрагеда из укупног броја осумњичених елиминишу неке од њих, да укажу на потенцијалне(вероватне) извршиоце, односно да усмере ове органе у правцу стицања нових сазнања.Како истичу Нејпијер и Бејкер сврха профилисања учинилаца кривичнихдела јесте да открије оне њихове особине које ће криминалистима помоћи у сужавањукруга осумњичених, на основу карактеристика лица места кривичног дела и иницијалнихистражних информација.”[81]

Циљ профилисања није да открије идентитет конкретне особе која је извршила неко дело и тако нешто је мало вероватно, тј. веома ретко се дешава у пракси. Због чињенице да профилисање личности није подједнако примењиво на све врсте кривичних дела, пре његовог коришћења пожељно је размотрити погодност примене овеметоде у конкретном случају. Опште је прихваћено мишљење да је профилисање најделотворније код дела са психопатолошком мотивацијом извршиоца, затим злочина извршених из сексуалних и ниских побуда, као и других дела која су по својој природи насилна и код којих учиниоци показују тенденцију поновног вршења, тј. рецидива. Према Тетенувећина дела која су погодна за профилисање карактерише преступникова отворенасексуална активност или губитак контакта са реалношћу. Профилисање је техника или приступ за решавање криминала. Saroha га дефинише као форензичку технику коју користе форензички истражитељи и агенције за спровођење закона како би разумели зашто криминалци почињу бити криминалци, да би класификовали

[79]*Behavioral Science Unit*
[80] Кривокапић, В., Жарковић, М., Симоновић, Б. (2005): *Криминалистичка тактика*, Виша школа унутрашњих послова, Земун, Београд
[81]Napier, M., Baker, K. (2005). Criminal personality profiling, objavljeno u: *Forensic science: An introduction to scientificand investigative techniques* (eds. S. James, J. Nordby), Boca Raton, 615

криминално понашање и решили злочине који су већ почињени.[82]Други сматрају то алатом који користе форензички стручњаци за идентификацију понашања у понашању прекршиоца, особине личности, демографске варијабле и географске варијабле на основу информација и карактеристика злочина.[83]Међутим, генерални консензус је да кривично профилирање укључује прикупљање закључака о особинама појединца одговорног за низ криминалних дела или за одређени злочин. То укључује разумевање шта одређени злочин каже о починиоцу. Користе га форензички истражитељи и агенције за спровођење закона како би разумеле и ухапсили криминалне прекршиоце. Као форензичка техника, кривично профилисање омогућава истраживачким агенцијама да користе посебне информације како би усмерили своју пажњу на особеса особинама личности које су паралелне са преступницима који су починили друга слична кривична дела.[84]

У потрази за починиоцем сајбер злочина, истражитељ често не успева због различитих потреба. Праћење сајбер преступника захтева изузетну вештину истражитеља, али он би ипак требало да буде криминални истражитељ који сарађује са стручњаком за информационе технологије који познаје право, форензику и још много тога. Како се технологија развија, илегалне активности такође пролазе кроз драстичне промене. Међутим, да би се пратили дигитални отисци девијантног субјекта, истраживач мора предузети специјализован, кохезиван и идиографски приступ.

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.

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. Неопходно је разумети да постоји велика

[82] Saroha, R. (2014). Profiling a Cyber Criminal. International Journal of Information and Computation Technology, 4(3): 253-258.
[83]Lickiewicz, J. (2011). *Cyber Crime psychology-proposal of an offender psychological profile*. Problems of forensic sciences, 2(3): 239-252.
[84] Kirwan, G., & Power, A. (2013). Cybercrime: Psychology of cybercrime. Dublin: Dun Laoghaire Institute of Art, Design and Technology.

разлика између операнда у традиционалним злочинима и технолошким злочинима.

У традиционалним злочинима, праћење злочинца је релативно лакше јер криминалац може оставити физичке трагове доказа на месту злочина и после њега. Док је у технолошком облику сајбер криминала, присуство починиоца је удаљено од места злочина.

Много пута жртва неће ни бити свесна идентификације починиоца. Сајбер криминалци у непознатом мрачном простору који имају приступ моћној интернет технологији могу створити хаос који утиче на корпорације, земље или чак обичне људе. Они чак могу да преузму контролу над појединачним рачунарским системима и користе их за незаконите активности, укључујући и за злонамерне сврхе, укључујући откупнину, превару. Интернет пружа *гвоздену завесу* за таквог преступника, иза које он може да се сакрије и почини дело виктимизирајући било кога или сваког из било ког дела света. Због разлика између општинских закона и међународних закона, сајбер преступник може остати неоткривен, а случај неистражен и кривично гоњен.

Идеја да појединац који чини злочин у сајбер простору може да одговара одређеном обрису (профилу) може изгледати претерано, али докази сугеришу да одређене карактеристике које се разликују код сајбер криминалаца редовно постоје.[85]Криминално профилисање се обично користи као алат за подршку истрази да би се обезбедио могући психолошки профил и профил понашања преступника. Профилисање сајбер криминала је употреба конвенционалног метода профилисања криминала у области сајбер криминала.

Профилисање сајбер криминала може се дефинисати као истрага, анализа, процена и реконструкција података из бихејвиоралне или психолошке перспективе извучених из компјутерских система, мрежа и људи који су починили злочине.[86]Профилисање криминалаца се већ неколико година користи за идентификацију криминалних типова од конкретних злочина.[87]Криминолошка

[85] Hemamali Tennakoon, *The need for a comprehensive methodology for profiling cyber-criminals,* Quoting Nykodym et al. (2005), http://www.newsecuritylearning.com/index.php/archive/150-the-need-for-a-comprehensive-methodology-for-profiling-cyber-criminalsдатум приступа: 25.11. 2021.
[86] Shaw, R., Atkins, A. S. (2007), *Conceptual Analysis of Cybercrime Events in Profiling Business Attacks*, IADIS International Conference e-Society 2007, https://www.researchgate.net/publication/266214930 датум приступа: 25.11. 2021.
[87]Turvey, B.E. (1999), *Criminal Profiling: an introduction to Behavioural Evidence analysis*. London: Academic Press.

истраживања криминалне личности врше се како би се идентификовале и проценили појединачне особине, што доводе до кривичног дела. Злочинци, укључујући сајбер криминалце имају неколико оштрих особина личности: импулсивност, агресивност (*висок ниво агресије*), потешкоће предвиђања последице својих поступака, крутост, лажи, себичност, егоцентричност, афлуалне засићене осећаје, осебујне оријентације и пресуде, апстиненција од друштвене стварности, немогућност интернализације моралних и правних норми, непријатељстава. Особине личности играју кључну улогу у понашању личности. Човек има и својствене и типичне особине. Личност преступника је скуп негативних личних особина које су специфичне за појединачну врсту криминалаца. Сајбер криминалац није само особа са одређеним статусом, који има права, дужности, одговорности, већ и појединац као сложен систем са неколико структура: *потребе, емоције, темперамент, оријентација вредности.*

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 тај преступник користи за извршење може бити корисна информација за профилисање сајбер преступника. Проширивање овог приступа за откривање починилаца сајбер криминала интеграцијом јединствених карактеристика, специфичних за овај облик криминала, могло би помоћи у бољој регулативи сајбер криминала. На пример – познавање мотивације неетичких хакера може помоћи истражитељима да схвате понашање таквих криминалаца и то може помоћи да се не законе агенције за спровођење закона, али такође може бити средство да се осигура мрежна заштита земље и институција. Такође може помоћи у стварању безбедног екосистема сајбер простора, који има осигуран оквир.

Профилисање сајбер криминала може се користити за добијање увида у профилисање преступника успостављањем везе између форензичких клиничких практичара и агенција за спровођење закона. Клинички психолог такође може да искористи своју вештину да предвиди понашање преступника повезујући га са неразјашњеним злочинима. Он може, у сарадњи са истражним агенцијама, да их саветује о тактикама истраге, доприносећи на тај начин развоју бољег екосистема

и оквира за откривање злочина. Анализа профилисања преступника такође се може користити заједно са компјутерском форензиком. Ово се такође може користити за пружање информација предузећима како би се побољшале њихове процедуре сајбер безбедности. 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. Нажалост, профилисање сајбер криминала обавља се на рутински начин. Развој и структурална употреба профилисања сајбер криминала је добила значајан фокус кроз истраживања спроведена широм света. Како је сајбер криминал у порасту, професионална помоћ психолога, социолога и криминолога постала је неопходна да се конструишу поуздани профили хакера и других сајбер криминалаца како би се ојачале одбрамбене стратегије.[88]Нова стратегија – идиографски приступ, однедавно више не добија на значају. Идиографски приступ помаже у испитивању дигиталних отисака стопала одређеног субјекта за непосредну употребу у истрази која је у току. Он пружа оквир истражитељима да анализирају дигиталне доказе о понашању у сврху планирања случаја, идентификације субјекта, стварања потенцијалних клијената и кривичног гоњења преступника.[89]Интегрисани систем од две области, односно информационе безбедности и кривичне истраге, омогућава побољшани поступак анализе познат као анализа криминалистичке истраге.[90]Велики број сајбер злочина показује везу између жртава и преступника. Однос између понашања особе на мрежи и виктимизације рачунара захтева детаљну анализу која се може урадити кроз процес профилисања сајбер криминала.

Профилисање сајбер криминалала може укључити технике рударења података које се користе у управљању односима са клијентима као алат за стицање знања о догађајима сајбер криминала.[91]Истражне агенције морају

[88]Saroha, Rashmi (2014). *Profiling a Cyber Criminal*, International Journal of Information and Computation Technology. Vol 4, No 3, pp. 253-258, http://www.irphouse.com/ijict.htm датум приступа: 25.11. 2021.
[89]Steel, M. Chad, *Idiographic Digital Profiling: Behavioral Analysis Based on Digital Forensics*, Journal of Digital Forensics, Security and Law, Vol. 9(1).
[90]Bongardt Steven (2010). *A Forensic Examiner*, Springfield Vol.19 Iss 3, 20-25
[91]Shaw, R., Atkins, AS. (2007), *Conceptual Analysis of Cybercrime Events in Profiling Business Attacks*, IADIS International Conference e-Society 2007, https://www.researchgate.net/publication/266214930 датум приступа: 25.11. 2021.

проучити и анализирати починиоце сајбер криминала, организоване банде и њихово присуство на сајтовима друштвених мрежа. Претраге по кључним речима су суштински алат за откривање криминалних организација на сајтовима друштвених мрежа.[92]Овај приступ се може користити за регулисање злочина у вези са илегалним садржајима који се врше у сајбер простору, као што је порнографија.

Методологија анализе доказа понашања у сајбер профилисању помаже процесу дигиталне истраге.[93]Посебна пажња се, међутим, мора посветити правним и етичким разматрањима која произилазе из аутоматског прикупљања података на мрежи, пошто то поставља питања приватности и поверљивости. Ови подаци, ако су у облику личних података или осетљивих личних података, морају бити анонимизовани и коришћени. Аутоматско прикупљање података заснованих на Интернету је узбудљив развој у којем агенције за спровођење закона прикупљањем података креирају претраживаче за откривање сајбер злочина.[94]Да би мера за сузбијање сајбер криминала била ефикаснија, захтева чврст оквир профилисања сајбер криминалаца и њиховог начина рада. Тренутно је усвојена техника истраге традиционална са недостатком техничког знања. Он занемарује потребе данашње технолошке помоћи коју би преступник могао да предузме или техничке аспекте које би докази таквог случаја могли захтевати. Држава мора размотрити нове димензије технолошког развоја и проценити његов утицај на криминалне активности. Технички напредак се такође може користити као средство за регулисање криминала. Стога је важно развити стратегију интегрисану са одговарајућим механизмом профилисања сајбер криминала. Органи за спровођење закона морају да користе такву стратегију за спречавање злочина, као и за истрагу злочина.

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. Решавање

[92] Décary-Hétu David & Morselli, Carlo, (2011), *Gang Presence in Social Network Sites*, International Journal of Cyber Criminology, July- December 2011, Vol. 5 (2), 876-890.
[93]Silde, Alice & Dr Angelopoulou, Olga, (2014), *A Digital Forensics Profiling Methodology for the Cyber stalker*, International Conference on Intelligent Networking and Collaborative Systems, 2014 IEEE, https://www.researchgate.net/publication/282275955 датум приступа: 27.11. 2021.
[94]Décary-Hétu David & Aldridge Judith, (2015), *Sifting through the Net: Monitoring of Online Offenders by Researchers*, The European Review of Organised Crime, 2(2) 2015, 122-141

идентификације је ефикасно када је починилац користио онлајн услуге за чињење кривичних дела као што су пхисхинг или спеар пхисхинг јер би оставио онлајн трагове који се могу прикупити и профилисати. Дакле, ако користи исти модус за накнадно кривично дело, истражитељ може да му уђе у траг помоћу таквог профила. За друге врсте сајбер преступа са употребом телефона и интернет технологије, као што је *Vishing,*ако се новац скида са банковних рачуна жртве, могло би постати тешкоући у траг починиоцима, посебно ако су користили лажне бројеве телефона док преносе плен. Дакле, уколико постоји стално праћење и профилисање активности починилаца злочина и њихове обично циљане класе жртава, онда истражитељ може покушати да предвиди будућа дела таквих преступника и заштити потенцијалне жртве, као и да уђе у траг таквим преступницима. Дакле, не постоји само ефикасна истрага, већ могу постојати и ефикасне детективске и превентивне стратегије које такав истражитељ може планирати. Институционализација сајбер криминала и профилисања криминала може довести до снажног механизма за ефикасну кривичну истрагу и тужилачке агенције. Илустрације ради, у злогласном случају *Пута свиле* у којем су потрошачи користили darknetза продају и куповину дроге и сличних кријумчарских роба, FBI је након опсежног истраживања о профилисању успео да ухапси Ross Ulbriht – а, главног оператера сајта. FBI је такође запленио 3,6 милиона долара средстава са есцров рачуна.[95]Ефикасно праћење потенцијалних сајбер криминалаца захтева одговарајућу употребу претраживача, специфичних фраза и слика сумњивих кријумчарских роба и термина, добро осмишљено профилисање урађено на основу таквих прикупљених информација.

„Јединствени профил учиниоца кривичног дела компјутерског криминалитета не постоји, али се сви они означавају заједничким називом – хакер. Појам *хакер* има више значења: новајлија, почетник у игри голфа који раскопава терен; копачровова или таксиста; креативни програмер или онај који неовлашћено улази у туђи компјутерски систем. Додатне карактеристике хакера јесу: доминирају припадници мушког пола, екстремно су бистри, склониистраживачком и логичком размишљању и увек такмичарски расположени, са сваком успешномреализацијом на тастатури они виде себе као афирмисане

[95]Wesley Lacson & Beata Jones, The 21st Century DarkNet Market*: Lessons from the Fall of Silk Road,* International Journal of Cyber Criminology Vol 10 Issue 1 January – June 2016, http://www.cybercrimejournal.com/Lacson&Jonesvol10issue1IJCC2016.pdf датум приступа: 27.11. 2021.

ауторитете над рачунаром и над било ким ко јеповезан са њим, што им даје осјећај снаге и контроле, теже да се информатичким производима баве површно, имају мало респекта према онима који не знају ништа о њиховој омиљеној теми – компјутеру.”[96]

Починиоци сајбер превара сада користе софистицираније методе као што су слање линкова за интернет странице на којима се врши *пецање*, копирање интернет презентација и коришћење домена великих компанија за слање нежељених електронских порука и програма који садрже вирусе.Истовремено, многи запослени људи који су прешли на рад од куће за време актуелне панемије вируса COVID 19 користили су јавне интернет мреже а нису инсталирали или ажурирали антивирусне програме на својим рачунарима, чиме су постали подложнији сајбер нападима.

Класификација мотива починилаца

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. *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.

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.*

[96]Крстић, О. (2009).*Малољетничка делинквенција*, Бања Лука, 2009, стр. 197–199.

„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."[97]Мотив се генерално сматра важним елементом у изградњи кривичног предмета (*заједно са средствима и могућностима*).

Новац	Ово укључује свакога ко остварује финансијску добит од злочина, 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, ћаци 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.

[97] Дракулић,Мирјана (1996). *ОсновиКомпјутерскогправа*,ДруштвооперационихистраживачаЈугославије-ДОПИС,Београд

	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 да ураде 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 одређенесајбер криминалне радње криминала важно је јер помаже форензичком стручњаку да изгради користан профил за преступнике. На основу мотива починиоца криминалци се могу категорисати на два: криминалци чији је чин коришћења Интернета за извршење криминала случајан и криминалци који намерно и свесно користе Интернет да изврше криминалну радњу. Злочинци који свесно користе Интернет за извршење криминала укључују криминалце у *белом овратнику*, хакере, рачунарске уметнике, мрежне нападаче и крекере. [98] Друга врста криминалаца користи рачунар да води евиденцију, користи мрежу за препознавање и проналажење жртава и оних који користе е – пошту и друге услуге да комуницирају са својим саучесницима. На пример, индустрија рачунарске безбедности оптужена је за претерано наглашавање патолошког аспекта хаковања. Мотивација иза хакерског учешћа у хаковању може се категорисати у шест: *признање вршњака, уживајући у осећају моћи, порива радозналости, осећања зависности, досада у корелацији са*

[98]Long, L. (2012). Profiling Hackers. SANS Institute. http://www.sans.org/readingroom/whitepapers/hackers/profiling-hackers-33864 датум приступа: 25.11. 2021.

образовним системом и политичким актима. За неке злочинце мотивација је да уради забрањени чин док за друге, злочин нуди могућност манипулације и управљања другима. Већина криминалаца који почини злочин у сајбер простору снажно је мотивисана њиховом мотивацијом у распону од једноставне жеље да се забаве до потребе за емоционалним или сексуалним импулсом, новцем, политичким мотивима или присилом узрокованом психијатријским условима менталних болести. С друге стране, неки сајбер криминалце покрећу мање племенити мотиви као што су пожуда, очај, гнев или обична досада. Важно је да се разликују мотиви за извршење одређеног криминалог дела јер важан део стварања корисног профила.[99] Због утицаја Холивуда и нетипичне природе злочина данас, постоји много стереотипа о томе како се појављују сајбер криминалци. Неки од стереотипа укључују да су сви сајбер криминалци социјално неспретни, али интелигентни умови, имају велике техничке вештине и знање и веома високе ИК, они су мушкарци. Сви сајбер криминалци никада нису насилни. Према појединим ауторима приликом креирања профила за сајбер починиоце службеник за спровођење закона треба увек почети са општем значајностима који су идентификоване за типичне сајбер починиоце.[100] Према поменутом аутору, да би неко био сајбер починилац, он би требало да има могућност да обавља основне задатке на Интернету. Неки злочини такође захтевају већу вештину рачунара и знања. Ове врсте криминалаца су исти као и они који почине криминал у физичком свету. Не верују и поштују закон. Они верују да би неки закони требало да буду сломљени јер су неразумни. Многи од ових криминалаца користе Интернет да испуне своје фантазије. Они га користе за изградњу нових идентитета и да играју улогу других људи. Разумевање мотива криминалаца је такође важно јер је у многим јурисдикцијама, један од елемената да оптужени појединац показује кривицу је да он или она поседују сваки од троугла злочина: *мотив, прилику и средств*а. Мотив је разлог починилаца за извршење кривичног дела.

Подцењивање мотива криминалца у истрази није корисно из два разлога: *приликом креирања профила прекршиоца мотив ће помоћи у идентификацији исправног починиоца и приликом представљања предмета против осумњиченог.*

[99]Schinder, D. (2010). Profiling and categorizing cybercriminals. http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/handling датум приступа: 02.12. 2021.
[100] Lickiewicz, J. (2011). Cyber Crime psychology-proposal of an offender psychological profile. Problems of forensic sciences, 2(3): 239-252.

Заједнички мотиви за криминалце који почине сајбер криминал укључују: с*ексуалне импулсе, политичке мотиве, монетарну добит, само за забаву, освету, љутњу и друге емоционалне потребе и озбиљне психијатријске болести.*[101]

Ове карактеристике треба да се користе приликом профилисања починиоца сајбер криминала. **Свака порука, реч и траг је важан приликом креирања криминалног профила.**

Стварање профила сајбер криминалаца

Стварање профила сајберкриминалаца је процес који пролази кроз неколико корака или фаза. Као први корак, може се успоставити формулација неких уобичајених карактеристика сајберкриминалаца. Ове заједничке карактеристике се виде као нешто што је могуће, а не као мандатна правила. Такође би требало да буде упамћено да увек може бити изузетак од усвојених заједничких правила.

Према томе, велики удео сајбер почининаца има следеће карактеристике: [102]

- **минимално техничко знање и вештине**: многи корисници интернета за илегалне сврхе могу се кретати сајбер простором без икакве спољне помоћи. Обично, људи користе алате које добро познају у своје сврхе, посебно када су акције укључивале висок ризик. Типичан сајбер починилац не може се дефинисати искључиво као *рачунар генија* нити као особа која први пут улази на Интернет.
- **непоштовање закона**, осећај да је изван оквира закона: углавном они себе не доживљавају као лоше људе, већ као жртве лоше писаних закона. Штавише, они верују да такви закони морају бити сломљени. Често њихове вештине, интелигенција, положај и околности чине да су изнад или изван постојећих закона. Неки сајберкриминалци деле идеју да се закони не треба примењивати у сајбер простору на основу њеног виртуалног *нестварног* карактера.
- **људи са апетитом високог ризика**: *Зашто су сајбер криминалци спремни да ризикују* - одговор није недвосмислен. За неке је то прилика да се учини

[101] Atkinson, S., & Walker, C. (2015). Psychology and the hacker – Psychological Incident. SANS Institute InfoSec Reading Room.
[102] Nick Nykodym, Robert Taylor, and Julia Vilela (2005). *Criminal Profiling and Insider Cyber Crime*, Digital Investigation 2, no. 4, 261-267.

нешто што је забрањено и чини њихов живот довољно емотивним и атрактивним. Остали су у искушењу способности да манипулишу, доминирају и контролишу треће стране.

— **снажна, иако радикално другачија мотивација**: Генерално гледано, сајбер починиоцу је потребно време, вештине, мотиви и труд. Они су високо мотивисани, мада су извори њихове мотивације сасвим различити: од достизања сопственог задовољства, забаве, финансијских, политичких и других користи за себе или за остале.

У категорији сајбер криминалаца самопроглашени криминалци првенствено укључују младе хакере, који се могу поделити у неколико главних група: они који су узбуђени и привлаче их нове технологије. Они се забављају проучавањем начина на који рачунарски системи и мреже раде поступком суђења и грешке и разумеју хаковање као прилику за изградњу искуства;хакери који немају намеру да оштете рачунарске системе и мреже. Они су тип оних који могу хаковати систем или мрежу за једину сврху – остављање поруке *Био сам овде*;истраживачи чија је сврха приступ местима на која други нису успели; они који виде хаковање као игру у којој се суочавају са сигурносним системима и мотивисани су жељом да превазиђу ове системе.

Први сајбер криминалци у свету су били углавном млађи од 25 година. То су били радознали млади људи који су чинили таква дела да би сазнали више могућео начину њиховог функционисања и њиховим могућностима. [103]

Развојем информационих комуникационих технологија старосна граница се мењала временом. Данас су то појединциизмеђу 25 и 35 година, који се најчешће баве сајбер криминалом ради стицања материјалне користи. Све је више и појединаца између 35 и 45 година, који су врсни познаваоци информационих технологија и који то знање користе за сајбер криминал.

Образовање је веома важно при разумевању мотива за бављењем сајбер криминалом. Већина сајбер криминалаца воли да учи, али не воле сви учење у школи. Они не желе да дају свој максимум на предмете који их не занимају,и

[103] Chiesa R., Ducci S., Ciappi S. (2009). Profiling hackers. The science of criminal profiling as applied to the world of hacking, New York: CRC Press, стр. 90

често напуштају школу јер сматрају да они знају много више него што имшкола нуди.[104]

Сајбер криминалци често сматрају истражне органе неспособне за њихово хватање јер не разумеју техничке аспекте и личне мотиве који их инспиришу дачине ова дела. Ово објашњава њихов отворени пркос према институцијама и органима који се њима баве. Они сматрају да свака власт угрожава човекову слободу, а не неко ко их штити и обезбеђује слободу

Према критеријуму поштовања етике постоје:[105]

White Hat Hackers (Беле капе) – када је у питању ова групација за њих можемо рећи да се придржавају правила хакерске етике. Њихов главни циљ је заштита система и мрежа рачунара. Дакле, као један од циљева је побољшање система како не би долазило до наношења штета приликом провађивања. Они бивају унајмљени од стране компанија како би провалили у рачунар, открили начин на који је обављен сајбер криминалитет, и како би поправили недостатке и о томе обавестили власника.

Black Hat Hackers (Црне капе) –у односу на прве ова групација краде у уништава податке у мрежама и системима. Хакерску етику прилагођавају на начин који њима одговара. Они провађују у туше системе јер се воде принципом да све информације треба да буду слободне, у том принципу налазе оправдање за своје поступке. Током њихових акција дешава се и уништење одређеног дела система. Такође, једна од њихових активности које предузимају је и креирање и ослобађање вируса и црва који наносе штету корисницима рачунара.

Grey Hat Hackers (Сиве капе) –за ову групацију можемо рећи да се налази у средини између поменуте две горње групе. Њихова жеља је да се издвоје од тастера за безбедност неке компаније и да се дистанцирају од негативизма *црних* капа.У својим почецима они су кршили хакерску етику, али су се временом одлучили да стечено знање примењују по свим правилима.

[104] Chiesa R., Ducci S., Ciappi S. (2009). Profiling hackers. The science of criminal profiling as applied to the world of hacking, New York: CRC Press, стр. 98.
[105] Матијашевић Јелена (2013). *Кривичноправна регулатива рачунарског криминалитета*, Нови Сад, Правни факултет за привреду и правосуђе, стр. 88.

Када је у питању класификација хакера према стешену професионалности разликујемо две велике групе. То су аматери и професионалци. Критеријум нивоа познавањарачунарске технологије и озбиљност последица које проузрокују је заправо разлика међу њима. У наставку ћемо дати одређене разлике између њих:[106]

АМАТЕРИ	ПРОФЕСИОНАЛЦИ
Ова група се често упушта у криминалну активност иако имају легално занимање. Ипак, врло брзо буду и откривени за обављање нелегалних радњи. У оквиру ове групе можемо набројати три врсте људи: на првом месту су појединци који су окарактерисани као слаби и подводљиви, они којима је лако манипулисати. Тренутна повољна прилика која им се нуди је основни разлог обављања криминалног акта. Они врло често немају развијену светс о последицама које могу изазвати предузете радње. На злоупотребу рачунарских система их наговарају особе које су склоне манипулацији и уценама. Поред њих у групу аматера спадају порочни људи које имају и приватне проблеме које су последица социо–патолошких понашања. Свој излаз ови појединци виде управо у обављању криминалних радњи. Последњи тип људи су фрустрирани појединци који заправо представљају незадовољне, разочаране и огорчене особе. Унутрашњим осећајем	Како им само име каже, реч је о особама којима је криминал једино занимање. Њихово технолошко знање је на изузетном нивоу, а и такво често надограђују и допуњују. Они имају велики степен мотивације за обављање криминалних радњи, у обављању тих активности су упорни и истрајни. Поред високог нивоа стручности које поседују, они се тешко откривају, а и ако буду откривени, њихова криминална дела се тешко доказују током судског поступка. Њих можемо окарактерисати на следећи начин, то су индивидуални криминалци, мотивисани остваривањем материјалне користи, који немају разрађене дугорочне планове, нити самосталну стратегију деловања. Они често делују као индивидуе и удруживање са другим особама није пракса којој се повинују. Поред појединаца у групу професионалаца спадају и организоване кримогене групе хакера које су

[106] Будимлић Мухамед, Пухарић Предраг (2009). *Компјутерски криминалитет – криминолошки, кривичноправни и сигурносни аспект*, Сарајево, Факултет за криминалистику, криминологију и сигурносне студије, стр. 33 – 38.

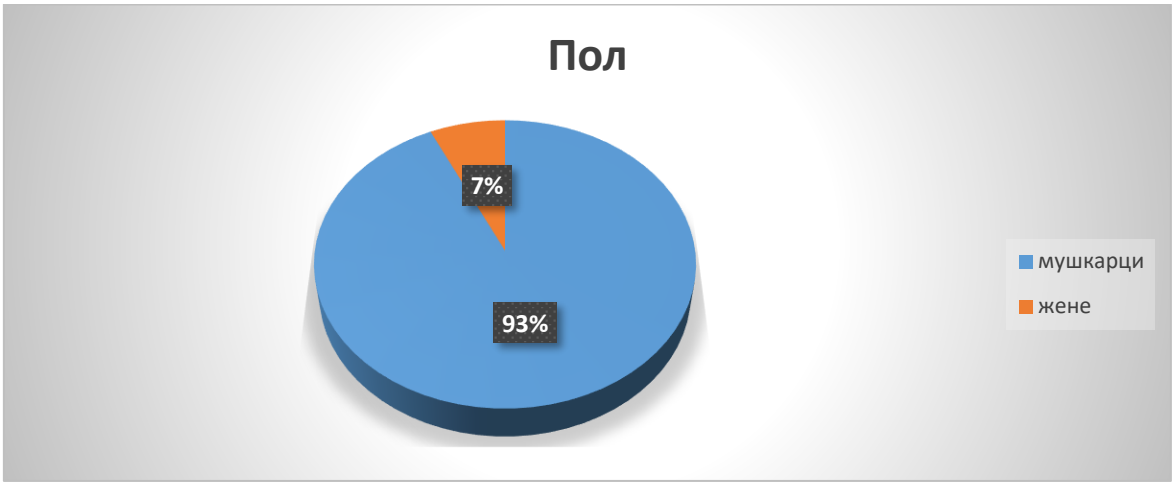
оне правдају чин криминалног понашања јер сматрају да су нпр. преварене и неправедно злостављане.	састављене од појединаца који заједничким снагама делују ради остварења заједничких интереса. Чврста организација и хијерархијска уређеност је одлика ових кримогених групација. Бројност и квалитет организације огледа се у резултатима које постижу. Такође, поседују изутетно информатичко знање које користе ради остваривања бројних сајбер криминалних радњи. Самим тим, поред класичних начела деловања организованих криминалниг група, то је оно што их чини професионалним извршиоцима највишег ранга. Уколико бисмо извршили профилисање професионалног сајбер починиоца, рекли бисмо да је реч о *младој и интелигентној, високо мотивисаној, узорној и поверљивој особи мушког пола са чврсто изграђеном логиком и одличном вештином коришћења компјутерских система.*

„Још давне 1975. Паркер Д. је навео карактеристике модерног компјутерског криминалца тог времена, базирајући их на 17 случајева које је он детаљно испитивао: извршиоци су млади(*просечна старост 29 година*), управљачке и професионалне вештине су преовладавајуће (*70% су били руководиоци или високо искусни технички професионалци*), нарушавање професионалног (радног) поверења било је евидентно у 65% случајева. Личне карактеристике: виђен као веома пожељан радник: поуздан, достојан поверења, бистар, паметан, мотивисанм није професионални криминалац који се поноси својом криминалном прошлошћу,

највећи страх су имали од могућности да њихови криминални акти буду откривени и познати породици, пријатељима и колегама са посла."[107]

„Осам година касније (1983. године) Bequail А.демонстрира сличан профил:старост: 15 – 45 година, криминална прошлост: обично раније нису били у сукобу са законом, професионално искуство: од минималног до високо искусних информатичких професионалаца, мада су забележени случајеви да извршиоци нису имали било какво информатичко искуство, личне особине: бистар, мотивисан и спреман да прихвати технички изазов, ангажован радник. Улога: у већини случајева делује самостално, ипак, расте број случакева са конспирацијом два или више криминалаца, понашање: у јавности никад не нарушава важеће (стандардне) друштвене норме понашања, позиција: најчешће је у позицији са које има лак приступ до рачунара."[108]

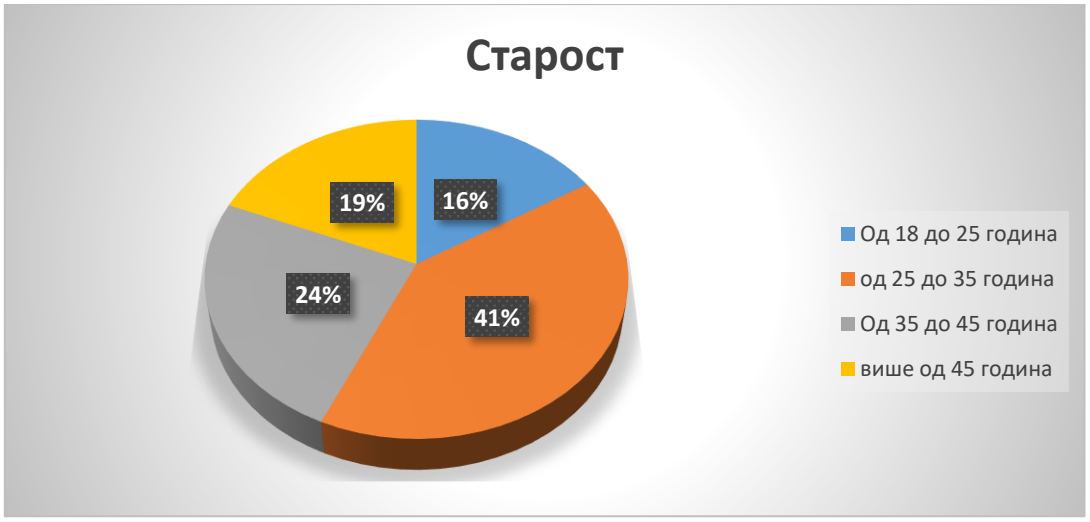
Графички приказ резултата које је спровео Колев са сарадницима[109]:



Полна структура починиоца инкриминисаних дела

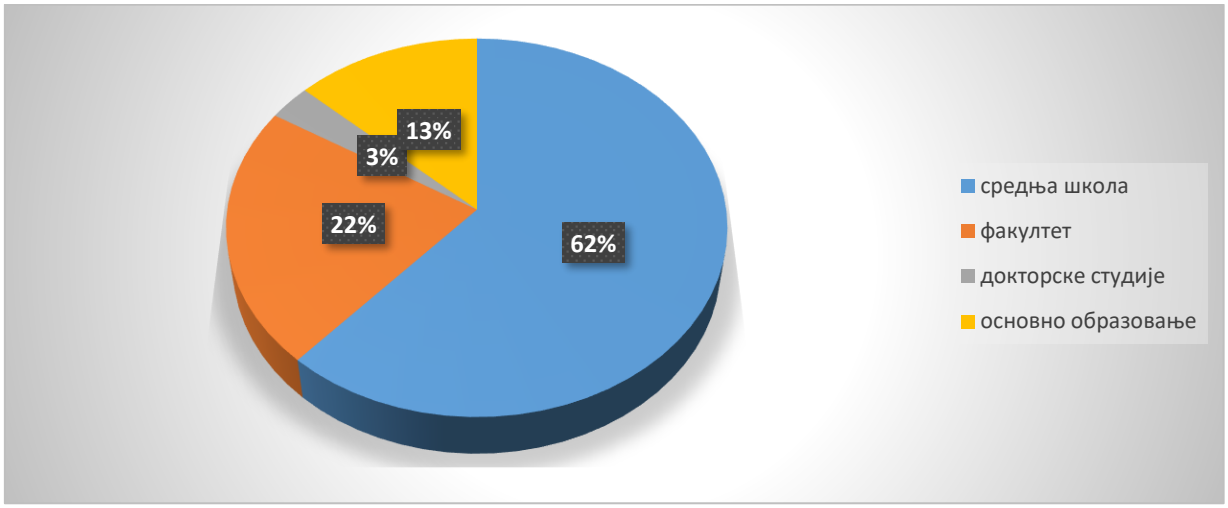
Коментар: *Када је у питању пола структура, већина починиоца је мушког пола. Када су у питању жене оне су су најчешће партнерке или познанице неких одчланова сајбер криминалаца.*

[107]Krauss, L., MacGahan, A. (1989). *Computer fraud and countermeasures*, New Jersey,1979,. стр. 39;I.C. Palmar, G. A. Potter, *Computer security risk management*,London, pp. 117-118
[108] Beaquai A. (1983).*How to prevent computer crime*,John Wiley & Sons, Inc,45-47, стр. 43.
[109]Колев Драган, НастићДраган, Јакуповић Санел (2015). *Социо – демографске карајтеристике починиоца сајбер криминала у Србији,*Моћ комуникације



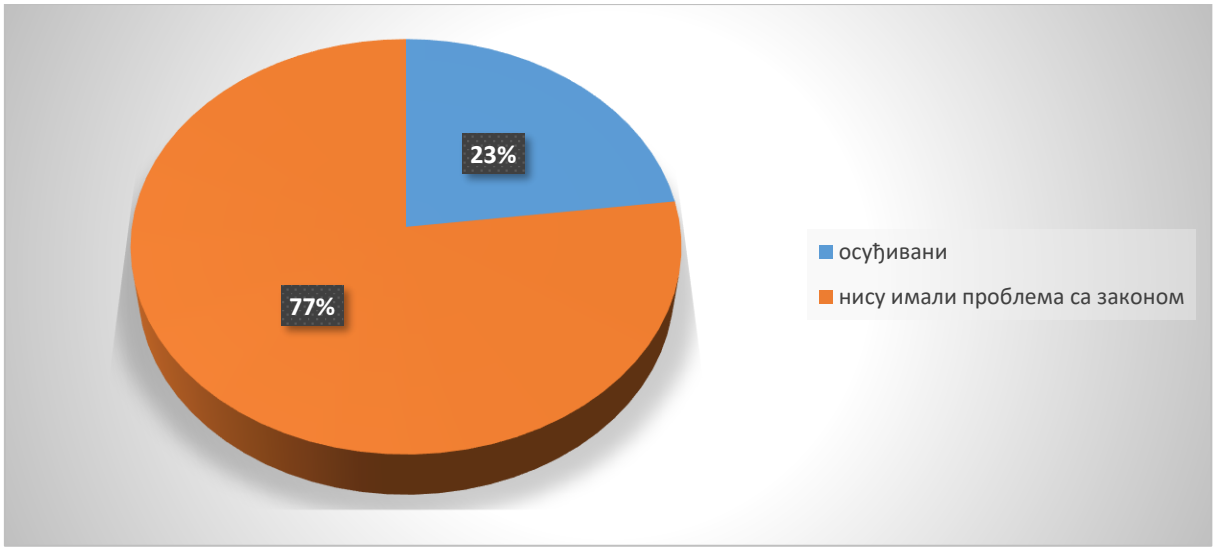
Старосна структура починиоца инкриминисаних дела

Коментар: *Највећи проценат осуђиванихпочиниоца сајбер криминала има од 25 до 35 година старости, а најмање је оних који имају између18 и 25. година.*



Образовна структура починиоца инкриминисаних дела

Коментар: *Највећи проценат починилаца има завршену средњу школу.*



Коментар: *Од укупног броја осуђиваних лица више од половине (56%) је било осуђивано само једном док је петина(19%) било осуђивано више пута.*

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 злочини засновани на трансакцијама као што су 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 сајбертероризма 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.

Сајбертероризам 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 сајбертероризма 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. Броји 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 иу професионалном животу, будемо свесни ових и других сајбер криминалитета и да држимо *очи отворене*, посебно у време кризе када се број преступника повећава.

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.

Шта нам профилисање говори о *типичном* сајбер криминалцу – особи која користи рачунаре и мреже за вршење злочина? Увек постоје изузеци, али већина сајбер криминалаца показује неке или већину следећих карактеристика: одређена мера техничког знања (у распону од *скриптних клинаца* који користе туђи злонамерни код до веома талентованих хакера), непоштовање закона или рационализација зашто су одређени закони неважећи или не би требало да се примењују на њих, висока толеранција за ризик или потреба за *фактором узбуђења, control freak природа* илити особа која осећа опсесивну потребу да контролише себе и друге и да преузме команду над сваком ситуацијом, уживање у манипулацији или *надмудривању* других, и на последњем али не најмање важном месту је мотив за извршење кривичног дела – новчана добит, јаке емоције,

политичка или верска уверења, сексуални пориви, па чак и само досада или жеља за *мало забаве.*

ЛИТЕРАТУРА

— Atkinson, S., & Walker, C. (2015). Psychology and the hacker – Psychological Incident. SANS Institute InfoSec Reading Room.

— Bayuk et al. (2012) Bayuk JL, Healey J, Rohmeyer P, Sachs MH, Schmidt J, Weiss J. *Cyber security policy guidebook.* Hoboken: Wiley; 2012. pp. 3–4.

— Beaquai A. (1983). *How to prevent computer crime,* John Wiley & Sons, Inc,45-47

— Biju, Gopal & Prakash (2019) Biju JM, Gopal N, Prakash AJ. *Cyber attacks and its different types.* International Research Journal of Engineering and Technology. 2019;6(3):4849–4852.

— Bongardt Steven (2010). *A Forensic Examiner,* Springfield Vol.19 Iss 3, 20-25

— Breda, Barbosa & Morais (2017) Breda F, Barbosa H, Morais T. *Social engineering and cyber security.* International Technology, Education and Development Conference. 2017;3(3):106–108.

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

— Chiesa R., Ducci S., Ciappi S. (2009). Profiling hackers. The science of criminal profiling as applied to the world of hacking, New York: CRC Press

— Cohen Daniel (2014). *Cyber terrorism*in Cyber Crime and Cyber Terrorism Investigator's Handbook

— Décary-Hétu David & Aldridge Judith, (2015), *Sifting through the Net: Monitoring of Online Offenders by Researchers*, The European Review of Organised Crime, 2(2) 2015, 122-141

— Décary-Hétu David & Morselli, Carlo, (2011), *Gang Presence in Social Network Sites*, International Journal of Cyber Criminology, July- December 2011, Vol. 5 (2), 876-890.

— Fischer (2009) Fischer EA. *Creating a framework for cybersecurity: an analysis of issues and options*. Hauppauge: Nova Science Publishers; 2009.

— Gačić, M. (1982). *Kompjuterski kriminal, inostrana iskustva,*13. maj, br. 5, Zagreb

— Geers, Kenneth (2010).*Sun Tzu and Cyber War*, NATO Cooperative Cyber Defence Centre of Excellence

— Giacomazzo, Bernadette R. (2014). *OpenSSL Heartbleed Computer Virus Fix and Security: How to Protect Yourself from the Latest Internet Bug*.
— Goel (2020) Goel S. *National cyber security strategy and the emergence of strong digital borders.* Connections: The Quarterly Journal. 2020;19(1):73–86.
— Ignjatović, Đ. *Pojmovno određenje kompjuterskogkriminaliteta,* Anali Pravnog fakulteta, 1-3/91
— Jaishankar, K. (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, Boca Raton, FL, USA: CRC Press, Taylor and Francis Group
— Jang-Jaccard & Nepal (2014) Jang-Jaccard J, Nepal S. *A survey of emerging threats in cybersecurity*. Journal of Computer and System Sciences. 2014;80(5):973–993.
— Kirwan, G., & Power, A. (2013). Cybercrime: Psychology of cybercrime. Dublin: Dun Laoghaire Institute of Art, Design and Technology.
— Krauss, L., MacGahan, A. (1989). *Computer fraud and countermeasures*, New Jersey,1979
— Kumar, G., Kaur, A., Sethi, S. (2014). *Computer network attacks–a study*, International Journal of Computer Science and Mobile Applications, vol. 2, no. 11, pp. 24–32
— Kumar, G., Kaur, A., Sethi, S. (2014). *Computer network attacks–a study*, International Journal of Computer Science and Mobile Applications, vol. 2, no. 11, pp. 24–32
— Lickiewicz, J. (2011). *Cyber Crime psychology-proposal of an offender psychological profile*. Problems of forensic sciences, 2(3): 239-252.
— Lickiewicz, J. (2011). Cyber Crime psychology-proposal of an offender psychological profile. Problems of forensic sciences, 2(3): 239-252.
— Liff, Adam P. (2012). Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies 35 no.3
— Luiijf Eric (2014). *Definitions of Cyber Terrorism*in Cyber Crime and Cyber Terrorism Investigator's Handbook

— MacKinnonLachlan, FrangiskatosDimitrios (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.
— Mitnick & Simon (2009) Mitnick KD, Simon WL. *The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers.* Hoboken: John Wiley & Sons; 2009.
— Napier, M., Baker, K. (2005). Criminal personality profiling, objavljeno u: *Forensic science: An introduction to scientificand investigative techniques* (eds. S. James, J. Nordby), Boca Raton, 615
— Nick Nykodym, Robert Taylor, and Julia Vilela (2005). *Criminal Profiling and Insider Cyber Crime*, Digital Investigation 2, no. 4, 261-267.
— Palmar, I.C. Potter G. A. *Computer security risk management*, London, pp. 117-118
— Rantala, RR. (2004). Cybercrime Against Business. Bureau of Justice Statistics.
— Reid & Van Niekerk (2014) Reid R, Van Niekerk J. *From information security to cyber security cultures—information security for South Africa.* Piscataway: IEEE; 2014. pp. 1–7.
— Report of McAfee Labs 2016 Threat Predictions by Intel Security, November 2016.
— Romanus Okeke, Mahmood Shah (2016). *Information Theft Prevention, Theory and Practice*, Routledge
— Romanus Okeke, Mahmood Shah (2016). *Information Theft Prevention, Theory and Practice*, Routledge
— Rushinek, A, Rushinek, SF. (1993). U*sing Experts for Detecting and Litigating Computer Crime*. Managerial Auditing Journal. 19-22.

— Sahingoz et al. (2019) Sahingoz OK, Buber E, Demir O, Diri B. *Machine learning based phishing detection from URLs. Expert Systems with Applications*. 2019;117(4):345–357.
— Saroha, R. (2014). Profiling a Cyber Criminal. International Journal of Information and Computation Technology, 4(3): 253-258.
— 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.
— Sreenivasulu N. S. (2013). *Law Relating to Intellectual Property*, Partridge Publishing, Gurugram, India
— Sreenivasulu N. S. (2013). *Law Relating to Intellectual Property*, Partridge Publishing, Gurugram, India
— Steel, M. Chad, *Idiographic Digital Profiling: Behavioral Analysis Based on Digital Forensics*, Journal of Digital Forensics, Security and Law, Vol. 9(1).
— Stefoff, R. (2011). *Criminal Profiling*, New York, 38–70.
— Tumalavičius, V. 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.
— Turvey, B.E. (1999), *Criminal Profiling: an introduction to Behavioural Evidence analysis*. London: Academic Press.
— Veerasamy Namosha (2020). *Cyberterrorism – the spectre that is the convergence of the physical and virtual worlds* in Emerging Cyber Threats and Cognitive Vulnerabilities
— Wall, D. (2003). *Crime and the Internet*, Routledge, Abingdon, UK
— Yar, M. (2013). *Cybercrime and Society*, SAGE Publications, Thousand Oaks, CA, USA
— Yar, M.(2013). *Cybercrime and Society*, SAGE Publications, Thousand Oaks, CA, USA, 2013.
— Алексић, Ж., Миловановић, З. (1994). *Криминалистика*, Београд, стр. 297.
— Будимлић Мухамед, Пухарић Предраг (2009). *Компјутерски криминалитет – криминолошки, кривичноправни и сигурносни аспект*, Сарајево, Факултет за криминалистику, криминологију и сигурносне студије, стр. 33 – 38.

— Гаћиновић Радослав (2007). *Класификација безбедности,* Наука, безбедност, полиција, 2/07.
— Димовски Дарко, *Компјутерски криминалитет,*Правни факултет Универзитета у Нишу, зборник, LV, стр. 197-214
— Дракулић,Мирјана (1996). *ОсновиКомпјутерскогправа*,ДруштвооперационихистраживачаЈугославије –ДОПИС,Београд
— Ђурђевић З. и сарадници (2012). *Криминалистичко профилисање,* Београд, стр. 6
— Жунић Павловић, Весна, Ковачевић Лепојевић, Марина (2009). *Интерперсонално насиље у cybernпростору*,Истраживањаспецијалнојпедагогији,факултетзаспецијалну едукацијуирехабилитацију,Београд
— Колев Драган, НастићДраган, Јакуповић Санел (2015). *Социо – демографске карајтеристике починиоца сајбер криминала у Србији,*Моћ комуникацицје
— Константиновић-Вилић, Слободанка, Николић-Ристановић, Весна,Костић, Миомира (2012). *Криминологија,* 5. измењено и допуњено издање,Ниш:Правнифакултет,Центарза публикације,стр.178-182.
— Кривокапић, В., Жарковић, М., Симоновић, Б. (2005): *Криминалистичка тактика*, Виша школа унутрашњих послова, Земун, Београд
— Крстић, О. (2009).*Малољетничка делинквенција*, Бања Лука, 2009, стр. 197–199.
— Лазаревић, Љ. (2006). *Коментар кривичног законика Републике Србије,* Савременаадминистрација, Београд
— Матијашевић Јелена (2013). *Кривичноправна регулатива рачунарског криминалитета*, Нови Сад, Правни факултет за привреду и правосуђе, стр. 88.
— Матијевић, М., Бошковић, М. (2007). *Криминалистика оператива*, Бања Лука, стр.
— Прља Драган, Ивановић Звонимир, Рељановић Марио (2011). *Кривична дела високотехнолошког криминала*, Институт за упоредно право. Београд

— Радновић,Бранислав,Илић,Милена,Радовић,Немања (2012).*ЕкономскисајберкриминалуСрбији– аспектзаштитеинтернетпотошача*,Зборникрадова,међународнанаучност ручнаконференција,Сузбијањекриминалаиевропскеинтеграцијесосвртомна вискотехнолошкикриминал
— *Стратегијски преглед одбране Републике Србије*, 2009.
— Тањевић, Наташа (2009). *Компјутерски криминал − правна заштита нанационалном нивоу*, Безбедност - Часопис Министарства унутрашњихпословаРепублике Србије,број1-2/2009,стр.152-166
— Цетинић, М. (1998).*Компјутерска кривична дела и њихови појавни облици*, Правни живот, број 10, Удружење правника Србије

Интернет извори

Check Point Security Report (2020) Check Point Security Report Check point research. 2020. https://research.checkpoint.com/https://research.checkpoint.com/

CISA (2020) CISA Critical infrastructure sectors. 2020. https://www.cisa.gov/critical-infrastructure-sectorshttps://www.cisa.gov/critical-infrastructure-sectors

Department of Justice. Russian Man Sentenced for Hacking into Computers in the United States. http://www.cybercrime.gov/ivanovSent.htm

Gercke Marco, *Understanding cybercrime: Phenomena, challenges and legal response*, September 2012, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Gercke Marco, *Understanding cybercrime: Phenomena, challenges and legal response*, September 2012, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

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

Hemamali Tennakoon, *The need for a comprehensive methodology for profiling cyber-criminals*, Quoting Nykodym et al. (2005), http://www.newsecuritylearning.com/index.php/archive/150-the-need-for-a-comprehensive-methodology-for-profiling-cyber-criminals

http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf

http://searchsecurity.techtarget.com/definition/cyberstalking

http://www.gartner.com/newsroom/id/3165317

https://smartlife.mondo.rs/tech/platforme/a27438/koliko-ljudi-na-svetu-koristi-internet-i-drustvene-mreze.html

https://wearesocial.com/special-reports/digital-in-2017-global-overview

https://www.britannica.com/topic/cybercrime

https://www.mcafee.com/enterprise/en-us/products/total-protection-for-data-loss-prevention.html

https://www.stat.gov.rs/sr-Latn/oblasti/upotreba-ikt/upotreba-ikt-pojedinci

Kagita et al. (2020) Kagita MK, Thilakarathne N, Gadekallu TR, Maddikunta PKR, Singh S. A review on cyber crimes on the Internet of Things. http://arxiv.org/abs/2009.05708arXiv

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

Long, L. (2012). Profiling Hackers. SANS Institute. http://www.sans.org/readingroom/whitepapers/hackers/profiling-hackers-33864

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

Report and Guidance on Privacy in Social Network Services *Rome Memorandum* - 43rdmeeting,3-4March2008, Rome (Italy),http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

Saroha, Rashmi (2014). *Profiling a Cyber Criminal*, International Journal of Information and Computation Technology. Vol 4, No 3, pp. 253-258, http://www.irphouse.com/ijict.htm

Schinder, D. (2010). Profiling and categorizing cybercriminals. http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/handling

Shaw, R., Atkins, A. S. (2007), *Conceptual Analysis of Cybercrime Events in Profiling Business Attacks*, IADIS International Conference e-Society 2007, https://www.researchgate.net/publication/266214930

Shaw, R., Atkins, AS. (2007), *Conceptual Analysis of Cybercrime Events in Profiling Business Attacks*, IADIS International Conference e-Society 2007, https://www.researchgate.net/publication/266214930

Silde, Alice & Dr Angelopoulou, Olga, (2014), *A Digital Forensics Profiling Methodology for the Cyber stalker*, International Conference on Intelligent Networking and Collaborative Systems, 2014 IEEE, https://www.researchgate.net/publication/282275955

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

Wesley Lacson & Beata Jones, The 21st Century DarkNet Market*: Lessons from the Fall of Silk Road*, International Journal of Cyber Criminology Vol 10 Issue 1 January – June 2016, http://www.cybercrimejournal.com/Lacson&Jonesvol10issue1IJCC2016.pdf

Никић,Срђан:*Најчешћеметоденападасуберкриминалацаикакосеодбранити*, http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf

ПРИЛОЗИ

Комисија је 29. јануара 2020. године објавила свој најновији *Евробарометар о ставовима Европљана према сајбер криминалу*.Према истраживању, свест о сајбер криминалу расте.52% испитаника је изјавило да су прилично добро или веома добро информисани о сајбер криминалу, у поређењу са 46% у 2017. Међутим, мање Европљана сматра да се могу довољно заштитити: 59%, што је пад са 71% у 2017. Испитаници су забринути због злоупотребе њихових личних података, преваре, закључавања свог рачунара и присиљавања да плате откуп за приступ сопственим подацима, као и од крађе идентитета. Више од трећине је примило лажне мејлове или телефонске позиве у којима се траже лични подаци у последње три године, 8% је постало жртва *ransomware*– а, а 11% је хаковало налог на друштвеним мрежама или налог е – поште. Ово утиче на њихову спремност да користе онлајн услуге: на пример, 10% каже да је због њихове забринутости мања вероватноћа да ће куповати онлајн.

У извештају 2021. године, утицај пандемије COVID – 19 остаје видљив. Убрзана дигитализација у вези са пандемијом значајно је утицала на развој низа сајбер претњи, укључујући: партнерски програми за *ransomware*омогућавају већој групи криминалаца да нападну велике корпорације и јавне институције претећи им вишеслојним методама изнуде као што суDDoS напади. Малвер за мобилне уређаје еволуира са криминалцима који покушавају да заобиђу додатне безбедносне мере као што је двофакторска аутентификација. Куповина на мрежи довела је до наглог пораста онлајн превара. Експлицитни материјал је све већа брига и такође се дистрибуира ради зараде. Криминалци настављају да злоупотребљавају легитимне услуге као што су VPNs, шифроване комуникационе услуге и криптовалуте.[110]

[110] Internet Organised Crime Threat Assessment (IOCTA) 2021

САЖЕТАК

САЈБЕР КРИМИНАЛИТЕТ И ПРОФИЛИСАЊЕ ПОЧИНИЛАЦА

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.

На средини спектра леже злочини засновани на трансакцијама као што су превара, трговина дечјом порнографијом, дигитална пиратерија, прање новца и фалсификовање. Други део ове врсте криминала укључује појединце унутар корпорација или владиних бирократија.

Сајбер тероризам се фокусира на коришћење Интернета од стране недржавних актера како би се утицало на економску и технолошку инфраструктуру нације. Почини се много више сајбер криминала него што се починиоца открије. Броји привредни субјекти зарада очувања репутације упаде у компјутерске системе не пријављују и јавно не објављују.

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.

SUMMARY

CYBER CRIME AND PROFILING PERPETRATORS

Cybercrime encompasses activities. At one end there are crimes involving fundamental breaches of personal or corporate privacy, such as attacks on the integrity of information stored in digital depots and the use of illegally obtained digital information to blackmail a company or individual.

At the center of the spectrum lie transaction-based crimes such as fraud, child pornography, digital piracy, money laundering and counterfeiting. The other part of this type of crime involves individuals within corporations or government bureaucracies.

Cyberterrorism focuses on the use of the Internet by non-state actors in order to influence the economic and technological infrastructure of the nation. Many cybercrimes are committed than the perpetrator is discovered. A number of business entities do not report and do not publish intrusions into computer systems in order to preserve their reputation.

Key factors in the fight against crime and criminals are identifying the perpetrators of cybercrime and understanding the methods of attack. Detecting and avoiding cyber attacks is a difficult task. The police must therefore keep pace with new technologies, in order to understand the opportunities that are being created by criminals and how they can be used as a tool to fight cybercrime.

БИОГРАФИЈА АУТОРА

Маја Вукман рођена је 03.01.1994. године у Нишу. Средњу школу завршила је у Гимназији „Бора Станковић“ у Нишу 2013-е године. Своје академско образовање стицала је у две образовне установе, на Правном Факултету Универзитета у Нишу и на Универзитету Унион Никола Тесла, на Факултету Константин Велики. Звање Дипломираног правника стекла је 21-ог Септембра 2019-е године са просечном оценом 9. Од страних језика користи енглески и шпански језик кроз конверзацију у писаном и усменом облику. Академско образовање тренутно примењује радећи у Републичком геодетском заводу, тачније, у служби за катастарске непокретности, где је запослена на позицији правник. Положила је све испите прописане планом и програмом и испунила је све услове за одбрану завршног Мастер рада.

ИЗЈАВА О ИСТОВЕТНОСТИ

ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Маја Вукман

Наслов мастер рада: Сајбер криминалитет и профилисање починилаца

Ментор: Професор 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

Вукман Маја

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом Сајбер криминалитет и профилисање починилацапријављен 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: Маја Вукман

У Нишу, _____

Потпис аутора

Vukman Maja