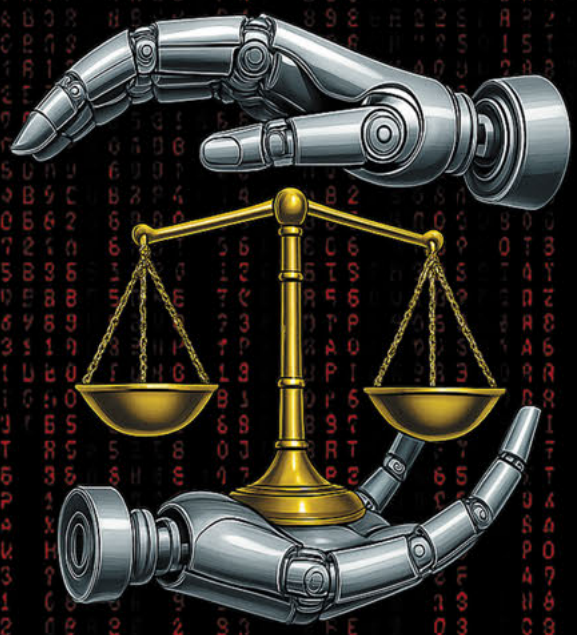
ИНСТИТУТ ЗА УПОРЕДНО ПРАВО
МОНОГРАФИЈА 206

Мина Зиројевић
Звонимир Ивановић



САЈБЕР ЗАКОНОДАВСТВО СРБИЈЕ

– други део –

Београд, 2025

САЈБЕР ЗАКОНОДАВСТВО СРБИЈЕ
– ДРУГИ ДЕО –

ИНСТИТУТ ЗА УПОРЕДНО ПРАВО

МОНОГРАФИЈА 206

Проф. др Мина Зиројевић
Проф. др Звонимир Ивановић

САЈБЕР ЗАКОНОДАВСТВО СРБИЈЕ
– ДРУГИ ДЕО –

Београд, 2025

Проф. др Мина Зиројевић
Проф. др Звонимир Ивановић

САЈБЕР ЗАКОНОДАВСТВО СРБИЈЕ – ДРУГИ ДЕО

Монографија 206

Издавач

Институт за упоредно право, Теразије 41, Београд

За издавача

Проф. др Јелена Ћеранић, директор

Рецензенти

Проф. др Гордана Гасми, редовни професор,
виши научни сарадник, Институт за упоредно право

Проф. Др Хатица Бериша, ванредни професор,
Школа националне одбране, Универзитет одбране

Проф. др Жарко Браковић, ванредни професор,
Факултет за дипломатију и безбедност

Проф. др Дарко Марковић, ванредни професор,
Правни факултет за привреду и правосуђе

Техничка припрема

Бранимир Трошић

Дизајн корица

Проф. др Дарко Марковић

Штампа

Birograf Comp d.o.o., Београд

Тираж

70 примерака

ISBN 978-86-82582-33-5

DOI: 10.56461/M206_25MZ.ZI.

Монографија је настала као резултат научноистраживачког рада Института за упоредно право који финансира Министарство науке, технолошког развоја и иновација Републике Србије према Уговору о реализацији и финансирању научноистраживачког рада НИО у 2025. години (евиденциони број: 451-03-136/2025-03/200049 од 4. 2. 2025. године).

Издавање ове монографије финансијски је помогло Министарство науке, технолошког развоја и иновација Републике Србије.

Садржај

1. Историја мрачног веба

Излазак *Freeneta* 2000. године се често наводи као почетак мрачног веба. Пројекат тезе Иана Кларка (Ian Clarke), студента Универзитета у Единбургу у Шкотској, *Freenet* је био замишљен као начин анонимне комуникације, размене датотека и интеракције на мрежи.[1]

Године 2002. утицај мрачног веба је значајно порастао када су истраживачи уз подршку америчке поморске истраживачке лабораторије изградили и пустили Тор мрежу. У то време, интернет је још био млад, корисника је било мало, а праћење људи је било лако, уз поштовање анонимности. Тор мрежа је створена да отвори безбедне канале комуникације за политичке дисиденте и америчке обавештајне оперативце широм света.

Касније је Торов основни код објављен под бесплатном лиценцом и формирана је непрофитна организација под називом Тор Пројекат (*Tor Project*). Године 2008. објављен је претраживач Тор, који је свима олакшао приступ мрачном вебу.

1.1. Дефиниција тамног веба (Dark Web)

Мрачни веб је скривени скуп интернет сајтова којима се може приступити само уз помоћ специјализованих мрежних (web) претраживача. За разлику од површинског претраживача, на мрачном вебу постоји скоро потпуна анонимност и приватност интернет активности, што може бити од корисно за коришћење легалних и илегалних апликација. Док га неки користе да би избегли владину цензуру и/или обезбедили себи потпуну анонимност, други га користе за различите илегалне активности.

1.1.1. Шта је мрачна мрежа, дубока мрежа и површинска мрежа?

Интернет је огроман простор са милионима веб страница, базама података и сервера који раде 24 сата дневно. Али такозвани „видљиви" Интернет (познат и као површински или отворени веб - *surface web*) је само врх леденог брега. Број страница, информација и услуга који се могу пронаћи помоћу претраживача као што су Гоогле и *Yahoo* су кап у мору у односу на мрачну мрежу (види слику 1.).

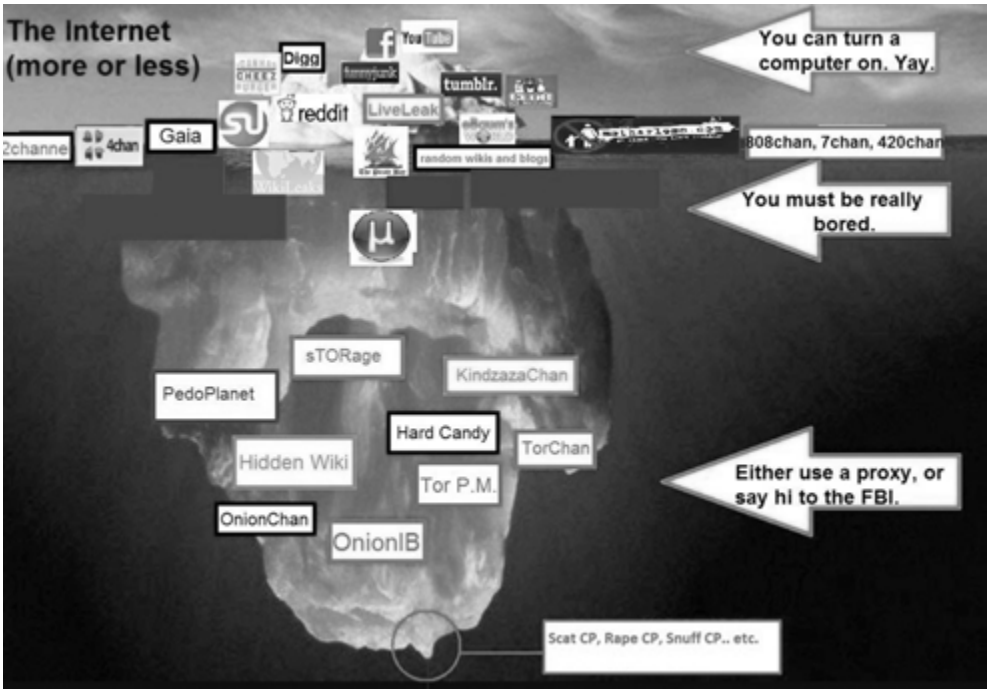
Постоји неколико појмова који окружују невидљиви Веб, али вреди знати у чему се разликују ако планирате да истражите нове стазе.

---

[1] Стална интернет адреса: https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web

1.1.2. Површинска мрежа или отворена мрежа (clear net)

Отворена мрежа, или површинска мрежа, је „видљиви" површински слој. Ако наставимо да визуализујемо целу мрежу као ледени брег, отворена мрежа би била горњи део који је изнад воде. Са статистичке тачке гледишта, овај скуп веб сајтова и података чини мање од 5% укупног интернета.



Слика бр. 1. Сликовити приказ Интернета (Извор: https://i0.wp.com/pcpress.rs/wp-content/uploads/2017/04/Intermex.jpg?ssl=1)

Овде су садржане све веб локације које су обично јавне, којима се приступа преко традиционалних претраживача као што су *Google Chrome*, Интернет *Explorer* и *Firefox*. Веб локације су обично означене операторима регистратора као што су ".com" и ".org" и могу се лако пронаћи помоћу популарних претраживача.

Лоцирање површинских веб (мрежних) локација је могуће, јер претраживачи могу да индексирају веб преко видљивих веза (процес који се назива „пузање" због тога што претраживач путује мрежом попут паука).[2]

[2] Пузање (Crowling) је начин на који Веб пописивач, који се понекад назива паук или спидербот, систематски прегледава светску мрежу и којим обично управљају претраживачи у сврху веб индексирања како би се информације брзо вратиле.

1.1.3. Дубока мрежа (Deep web)

Дубока мрежа лежи испод површине и чини око 90% свих мрежних локација. Ово би био део леденог брега испод воде, много већи од површинске мреже. У ствари, ова скривена мрежа је толико велика да је немогуће открити тачно колико је страница или мрежних локација активно у било ком тренутку.

Настављајући аналогију, велики претраживачи би се могли сматрати рибарским чамцима који могу само да „хватају" мрежне странице близу површине. Све остало, од академских часописа до приватних база података и још недозвољеног садржаја, је ван домашаја. Ова дубока мрежа такође укључује део који познајемо као мрачна мрежа.

Док многе новинске куће користе „дубоку мрежу" и „тамну мрежу" наизменично, већи део дубоког дела у целини је савршено легалан и безбедан. Неки од највећих делова дубоке мреже укључују:

Базе података: и јавне и приватно заштићене колекције датотека које нису повезане са другим деловима мреже, како би се претраживале унутар саме базе података.

Интранети: интерне мреже за предузећа, владе и образовне установе које се користе за приватно комуницирање и контролу аспеката унутар њихових организација.

У случају да се питате како да приступите дубокој мрежи, велике су шансе да га већ користите свакодневно. Термин „дубока мрежа" односи се на све мрежне странице које претраживачи не могу идентификовати. Дубоке мрежне странице могу бити скривене иза лозинки или других сигурносних зидова, док други једноставно говоре претраживачима да туда не „пузе". Без видљивих веза, ове странице су скривеније из разних разлога.

На већем обиму дубоке мреже, њен „скривени" садржај је генерално чистији и сигурнији. Све, од постова на блогу у прегледу и редизајна веб страница на чекању, до страница којима приступате на мрежи, део је дубоке мреже. Штавише, они не представљају претњу вашем рачунару или безбедности уопште. Већина ових страница је скривена од отворене мреже ради заштите корисничких информација и приватности, као што су: финансијски рачуни, налози е-поште и криптоване поруке, базе података приватних предузећа, друге осетљиве информације као што је медицинска документација или правни досијеи.

Ако наставимо да пливамо у океану дубоке мреже онда се светлост смањује. За неке кориснике, делови дубоке мреже нуде могућност да заобиђу локална ограничења и приступе ТВ или филмским услугама које

можда нису доступне у њиховим локалним областима. Други иду нешто дубље да би преузели пиратску музику или украли филмове који још нису у биоскопима.

На мрачном крају мреже до које се може доћи уз помоћ Тор претраживача, ћете наћи опаснији садржај и активности. На Тор-у можете да унесете било коју УРЛ адресу коју желите да посетите, укључујући .onion домене.

Претраживачи отворене мреже не могу да приступе мрачном вебу, али специјализовани претраживачи за тамну мрежу могу вам помоћи да пронађете оно што тражите. *DuckDuckGo* је популаран претраживач фокусиран на приватност који вас не прати на вебу када га користите. Када са *DuckDuckGo* претраживачем лутате мрачном мрежом он индексира странице, али мораћете да га отворите помоћу Тор претраживача.

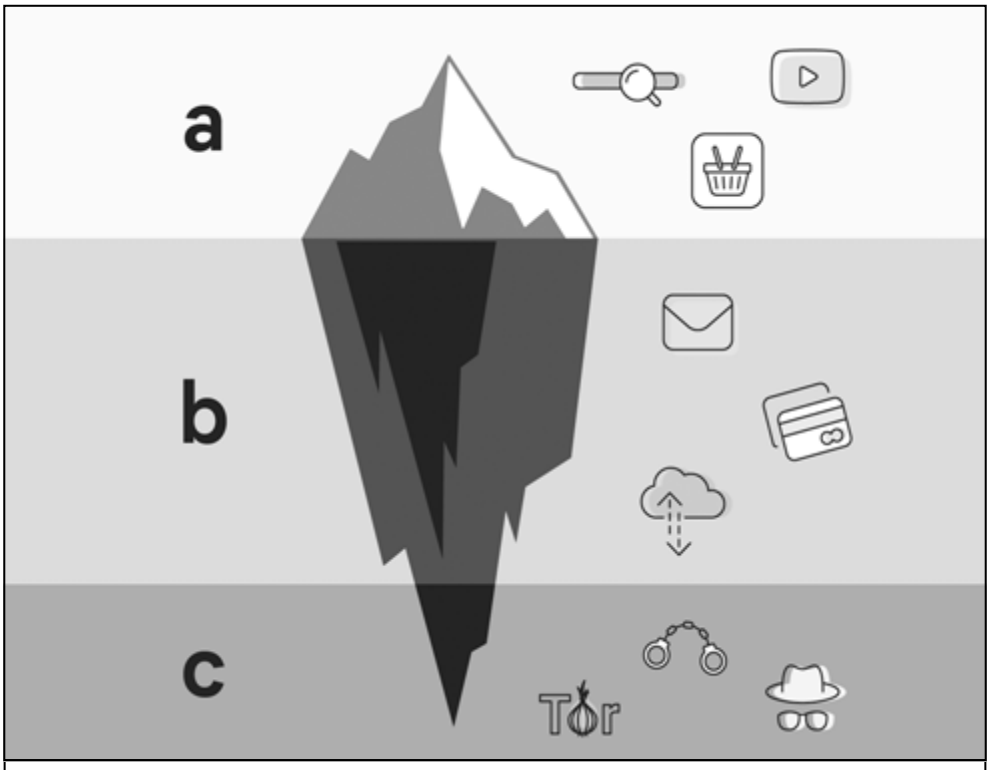
Слика бр. 2. Претраживачи мрачног веба.

Остали претраживачи мрачног веба укључују *Not Evil, Torch, Haistack* и *Ahmia* (Види слику бр. 2). Subreddit r/deepweb је добра полазна тачка за постављање питања искуснијим корисницима о томе како да претражују тамни и дубоки веб за садржај који желите. На крају, Скривена Вики је колекција мрачних веб веза — али везе можда неће радити и могу довести до опасних веб локација.

За просечног корисника мреже обезбеђење дубоке мреже је релевантнија од безбедности тамне мреже, јер можете случајно да завршите у опасним областима: многим деловима дубоке мреже се и даље може приступити са нормалним интернет претраживачима. Ово је начин на који корисници могу путовати кроз довољно тангенцијалних путева и завршити на сајту пиратерије, политички радикалном форуму или гледајући узнемирујуће насилан садржај.

1.2. Darkweb (mračna mreža)

Мрачна мрежа се односи на интернет адресе који нису индексирани и доступни само преко специјализованих мрежних прегледача. Знатно мања од површинске мреже, тамна мрежа се сматра делом дубоке мреже. Користећи наш визуелни приказ океана и леденог брега, тамна мрежа би била доњи врх потопљеног леденог брега (Слика бр. 1 и слика бр. 3).



a: Површинска мрежа укључује локације које се могу јавно претраживати (блогови, сајтови за куповину, сајтови са вестима, *YouTube*).
b: Дубока мрежа се састоји од електронских адреса за које је потребна пријава за приступ (е-пошта, банкарски портали, услуге претплате).
c: Мрачна мрежа захтева посебне алате за приступ, као што је Tor претраживач, и претраживачи га не индексирају.

Слика бр. 3. Приказ слојева екрипције у TOP мрежи
(Извор: https://www.avast.com/c-dark-web#topic-1)

Мрачна мрежа је, међутим, веома скривени део дубоке мреже са којим ће мало ко икада ступити у интеракцију или чак видети. Другим речима, дубока мрежа покрива све испод површине што је увек доступно са правим софтвером, укључујући мрачну мрежу.

Шта утиче на анонимност мрачне мреже?

- Нема индексирања веб страница од стране површинских претраживача. Гоогле и друге популарне алатке за претрагу не могу да открију или прикажу резултате за странице унутар мрачне мреже.
- „Виртуелни саобраћајни тунели“ воде преко насумичне мрежне инфраструктуре.
- Мрежа је недоступна традиционалним претраживачима због свог јединственог оператора регистра. Такође, додатно је скривена разним безбедносним мерама мреже као што су заштитни зидови и шифровање.

Репутација мрачне мреже се често повезивала са криминалном намером или незаконитим садржајем и „трговинским“ сајтовима на којима корисници могу да купе недозвољену робу или услуге.

1.2.1. Колико је тржиште дарквеба?

Тржишта мрачног веба нуде низ легалних и недозвољених добара. У табели 1. можемо видети цене неколико илегалних артикала које можете да купите на овој мрежи.

Табела 1. Цене нелегалних артикала на мрачној мрежи
(Извор: https://www.privacyaffairs.com/dark-web-price-index-2023/)

Ставке на мрачном вебу	**Цена**
Клонирана Visa или MasterCard картица са ПИН-ом	$25
Украдена пријава за онлајн банкарство, минимални износ од $ 2.000	$120
Хакован Coinbase налог (верификован)	$250
Хакован Фејсбук налог	$25
Фалсификовани пасош ЕУ	$3,000
Злонамерни софтвер за Андроид, 1000 инстанци	$650
ДДоС напад на незаштићену веб локацију	$35 (по 1 сату) до $750 (за месец)

Злоупотреба података је често присутна на мрачном вебу. Када су брокери података хаковани, украдени подаци могу укључивати компромитоване кредитне картице, бројеве социјалног осигурања и друге податке, у зависности од тога шта је откривено у кршењу. Ово је уобичајен начин за крађу идентитета и нападе доксирања.

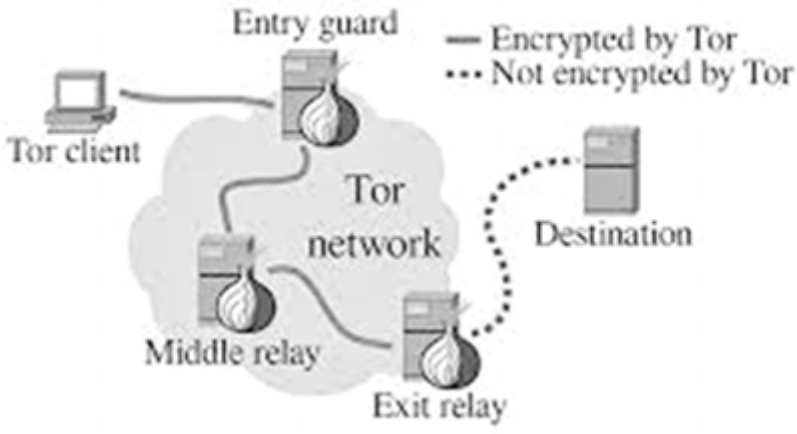
Ако постанете жртва, пријавите крађу идентитета што је пре могуће. И запамтите да постоје бољи (и безбеднији) начини да спречите крађу идентитета него да будете приморани да откупите своје податке са мрачног веба.

1.2.2. Како приступити мрачном вебу

Мрачна мрежа је некада била област само за хакере, службенике за спровођење закона и сајбер криминалаца. Међутим, нова технологија као што је шифровање и софтвер претраживача за анонимизацију, Tor, сада омогућава свакоме да зарони у мрак ако је заинтересован.

Мрежни претраживач Tor („The Onion Routing“ пројекат) омогућава корисницима приступ да посете веб-сајтове и са “.luk“ оператер регистра. Овај претраживач је услуга која је првобитно развијена крајем 1990-их од стране Лабораторије за истраживање морнарице Сједињених Држава.

Схватајући да природа интернета значи недостатак приватности, створена је рана верзија Tor-а како би се сакрила шпијунска комуникација. На крају, оквир је преиначен и од тада је објављен у облику претраживача какав данас познајемо. Свако може да је преузме бесплатно.



Слика бр. 4. Како Tor ради
(Извор: https://privacy.net/what-is-tor/)

Замислите Tor као мрежни претраживач попут Google Chrome или Firefox. Tor уместо најдиректнијег пута између вашег рачунара и дубоких делова мреже, користи насумични пут шифрованих сервера познатих као „чворови“. Ово омогућава корисницима да се повежу на дубоку мреже без страха од праћења њихових радњи или откривања историје прегледача (Слика бр. 4).

Сајтови на дубокој мрежи користе Tor (или сличан софтвер као што је И2П, „Невидљиви интернет пројекат“) како би остали анонимни, што значи да нећете моћи да сазнате ко их покреће или где се хостују.

1.2.3. Да ли је илегално ићи на мрачну мрежу?

Једноставно речено, не, није незаконит приступ мрачном вебу. У ствари, неке употребе су савршено легалне и подржавају вредност „тамног веба".

Што се тиче софтвера, употреба Тор и других анонимних претраживача није строго незаконита. У ствари, ови претраживачи „тамне мреже" нису везани искључиво за овај део интернета. Многи корисници сада користе Тор да приватно прегледају и јавни Интернет и дубље делове мреже.

Приватност коју нуди претраживач Тор је важна у садашњем дигиталном добу. Корпорације и управљачка тела тренутно учествују у неовлашћеном надзору активности на мрежи. Неки једноставно не желе да владине агенције или чак интернет провајдери (ИСП) знају шта гледају на мрежи, док други немају много избора. Корисницима у земљама са строгим приступом и корисничким законима често је онемогућен приступ чак и јавним сајтовима, осим ако не користе Тор клијенте и виртуелне приватне мреже (ВПН). На крају мреже, тамни веб је мало више сива зона. Коришћење мрачне мреже обично значи да покушавате да се укључите у активност коју иначе не бисте могли да обавите у јавности.

Ако предузимате незаконите радње унутар Тор-а онда без обзира на легалност употребе самог претраживача те радње би вас могле инкриминисати. Наравно да је кажњиво ако користите Тор у покушају да копирате садржај заштићен ауторским правима са дубоке мреже, делите илегалну порнографију или учествујете у сајбер тероризму .

Да закључимо, једноставно прегледавање ових простора није противзаконито, али може бити проблем за вас. Сама посета није противзаконита, али вас може изложити непотребним ризицима. Дакле, за шта се користи мрачни веб када се користи за илегалне активности?

1.3. Врсте претњи на мрачној мрежи

Уобичајене претње са којима се можете суочити током прегледања мрачне мреже су заражени програми, преваре или могућност да постанете особа од интереса обавештајних кругова.

Злонамерни софтвер (malware) је присутан широм мрачне мреже. Постоје алати да се ово предупреди, али и поред тога опасност од тога да будете заражени је већа него на површинској мрежи.

На мрачној мрежи не постоји толика законска заштита којом се штите корисници као на осталом делу мреже. Као такви, корисници могу бити редовно изложени неким врстама злонамерних софтвера као што су: Keyloggers, Botnet malware, Ransomware, Phishing malware.

Ако одлучите да истражите било коју веб локацију на мрачном вебу, излажете се ризику да будете издвојени и циљани као мета хакера и још много тога.

Заштита од злонамерних софтвера и вируса подједнако је кључна за спречавање штета на мрежама. Мрачна мрежа је препуна крађе информација од корисника заражених малвером. Нападачи могу да користе алатке као што су keiloggeri за прикупљање ваших података и могу се инфилтрирати у ваш систем на било ком делу мреже.

Такође, анонимност која се повезује са Тором и мрачном мрежом није апсолутна. Свака активност на мрежи може донети мрвице вашег идентитета ако неко копа довољно далеко. Крађа података се често појављују на мрачном вебу. Украдени подаци могу укључивати компромитоване кредитне картице, бројеве социјалног осигурања и друге податке, у зависности од тога шта је откривено у кршењу. Ово је уобичајен начин за крађу идентитета и нападе доксирања.[3]

Пошто су многе адресе засноване на Тор-у обележене (таговане) од стране полицијских власти широм света, постоји јасна опасност да постану мете владе због посета интернет страници на мрачној мрежи.

Илегалне пијаце дроге попут Пута свиле биле су гашене услед полицијског надзора у прошлости. Коришћењем прилагођеног софтвера за инфилтрирање и анализу активности, ово је омогућило службеницима закона да открију корисничке идентитете како корисника тако и посматрача. Чак и ако никада не обавите куповину, касније у животу можете бити посматрани и инкриминисани за друге активности.

Инфилтрације вас могу изложити ризику праћења и других врста активности. Избегавање владиних ограничења у циљу ширења нових политичких идеологија може бити затворски прекршај у неким земљама. Кина користи оно што је познато као „Велики заштитни зид" и ограничава приступ популарним сајтовима управо из овог разлога. Ризик да будете посетилац овог садржаја може да доведе до стављања на листу за посматрање или до тренутног служења затворске казне.

Ако постанете жртва, пријавите крађу идентитета што је пре могуће. И запамтите да постоје бољи (и безбеднији) начини да спречите крађу идентитета него да будете приморани да откупите своје податке са мрачног веба.

---

[3] Доксирање (енг. *Doking*) је термин којим се описује активност која би се могла уврстити у категорију сајбер малтретирања, која се састоји од објављивање приватних и личних података других корисника на мрежи, без њихове дозволе, са намером да их застраши или осрамоти.

1.4. Преваре

Неке наводне услуге попут професионалних „убица“ могу бити само преваре дизајниране да профитирају од вољних купаца. Извештаји сугеришу да мрачна мрежа нуди многе нелегалне услуге, од плаћених атентата до трговине за секс и оружје. Те услуге могу да буду праве, а могу и да буду параван за преваре како би криминалци на основу тога изнудили велике суме новца. Такође, преваре као на пример крађе идентитета су честе.

Без обзира на то да ли сте предузеће, родитељ или било који други корисник веба, пожелећете да предузмете мере предострожности да своје информације и приватни живот држите ван тамног веба.

Праћење крађе идентитета је кључно ако желите да заштитите своје приватне информације од злоупотребе. Све врсте личних података могу се дистрибуирати на мрежи за профит. Лозинке, физичке адресе, бројеви банковних рачуна и бројеви социјалног осигурања круже мрачном мрежом сво време.

2. Оперативна безбедност – Анонимност корисника

На овом најдубљем делу мреже услуге и сајтови се практично не могу пратити и постоји могућност предузимања незаконитих радњи и за кориснике и за провајдере.

Као такав, дарк веб је привукао многе странке које би иначе биле угрожене откривањем свог идентитета на мрежи. Жртве злостављања и прогона, узбуњивачи и политички дисиденти били су чести корисници ових скривених сајтова. Али наравно, ове погодности се лако могу проширити на оне који желе да делују ван ограничења закона на друге експлицитно незаконите радње.

Када се посматра кроз овај објектив, законитост мрачног веба заснива се на томе како се ви као корисник бавите њиме.

Оперативна безбедност (ОПСЕК) приликом предузимања оперативних активности у мрежном окружењу јесте обезбеђење минималних мера и метода у циљу заштите оперативаца и њихових активности током њих. Без обзира на то колико смо одговорни и пажљиви у овом мрежном окружењу ми самим присуством у виртуелном смислу остављамо низ трагова, на различитим нивоима. Адекватно предузете мере на обезбеђењу активности приликом предузимања оперативних мера онлајн подразумева поступање по правилима и смерницама ОПСЕК – а. Међутим, ни придржавање по свим правилима и смерницама на једном нивоу не обезбеђује апсолутну сигурност да се на другим нивоима неће угрозити анонимности оперативаца. Нивои о којима је реч су следећи:

1. мрежни ниво (*network level*)
2. ниво домаћина (*host level*)
3. ниво датотека (*file level*)
4. ниво корисника (*actor level*)

У погледу заштите на првом мрежном нивоу треба разумети да се приликом коришћења интернета свако од корисника пријављује на мрежи кроз одређене унапред дефинисане стандарде и протоколе, од којих је за нас интересантан интернет протокол (ИП). Како би се избегло директно дефинисање корисника преко ових адресних протокола у циљу прикривања користе се два веома интересантна софтверска решења за приступ мрежи, који прикривају моменат и место приступа корисника одређеној мрежи.

- Први приступ укључује пројекат TOP (The Onion Project – TOR), а који провлачи (рутује) саобраћај преко неколико посредничких домаћина

који се јављају као чворови са којих се иницира комуникација и на тај начин прикрива ИП адреса правог корисника.
- Други метод је И2П и он подразумева анонимизацију комуникационог саобраћаја унутар И2П мреже, али такође верно одражава интернет странице (вебсајтове) које се налазе на вебу, како би они били приступачни и на местима која су везана за дубоку (*deep*) или тамну (даркнет) мрежу.
- ВПН (Virtual Private Network - VPN) подразумева још један облик или метод прикривања ИП адреса корисника. Овај метод омогућава слање и примање података преко различитих мрежа кроз креирање безбедног канала комуникације кроз интернет - www. Систем интернет уобичајеног приступа одређеним подацима, а слање и пријем података се врши тако што се корисник преко свог рутера (приступног уређаја за жични и бежични интернет) повезује на интернет. У том смислу услуга ВПН представља следећи корак, где се корисник својом приступном ИП адресом пријављује ВПН-у, а овај пружа други канал приступа који представља потпуно нову ИП адресу коју и обезбеђује ВПН. Ова адреса је доступна једино лицима која прате комуникацију корисника (а она је везана за ВПН), а реална адреса корисника позната је једино провајдеру ВПН услуге.

Најчешћи начин прикривања трагова приступа у комуникационом саобраћају јесте комбинацијом ТОР–а и ВПН. Корисник мора да буде свестан да обе услуге пружају релативно добру заштиту, и том приликом прво се везује за ВПН пружаоца (провардера) услуга, да би се након крајњег чвора ВПН–а са ИП адресом ВПН провајдера прикључио на ТОР мрежу, путем које приступа циљаном сајту. Тада се поред ВПН заштите користи заштитом и ТОР мреже. Основна поука коју треба имати у виду приликом обављања оперативних активности на нету односи се на то да се не користи персонална ИП адреса приликом приступања јавној мрежи – WiFi, GPRS и сл.

У погледу заштите од значаја је посебно и коришћење адреса електронске поште преко којих је могуће препознати или идентификовати корисника. Наиме, ради коришћења већине услуга на интернету неопходно је да се корисник региструје путем свог налога електронске поште како би, на пример, могао отворити рачуне на Даркнет маркетима и сл. Приликом разматрања и планирања ОПСЕК активности од изузетног је значај избор правог добављача (провајдера), ово представља једну врсту постулата који се код ОПСЕК мора поштовати. Неке од опција које су се добро показале у пракси:

- Протон мејл (www.protonmail.com) базиран у Швајцарској има приступ и површинском нету и даркнету поседује и енкрипцију комуникације са краја на крај (*end-to-end*), не захтева никакве приватне и личне податке за регистрацију односно за креирање налога, ИП адресе и логови се не похрањују на њиховим серверима о корисницима.
- Маил.цх/маил.цом (mail.ch/mail.com) са седиштем у Немачкој, има приступ и површинском и даркнету, надограђен на ИП стрипингу[4], анонимне регистрације, поред значајних погодности пружа могућности плаћања у биткоинима (БТЦ).
- Торбокс (*TorBox*) има само приступ даркнету, ограничен на пружање услуга корисницима само дарк веб мејл услуга. Комуникације никада не напуштају ТОР мрежу, делови (партиције) сервера су шифроване – енкриптоване.
- Маил2Тор (Mail2Tor) има приступ само са даркнет, веома минималистички, са веома оскудним интерфејсом и врло просто направљен имејл клијент[5], а који не захтева никакве личне (персоналне) податке без ССЛ/ТЛС (SSL/TLS) подршке, такође не приказује ИП детаље у заглављу (хедеру) електронске поруке.

У вези са коришћењем имејл адреса треба напоменути да су неке потребне за регистрацију на даркнету и даркнет маркетима, у циљу креирања рачуна на маркетима односно на БТЦ провајдерима и сл. Избор правог имејл клијента који омогућава безбедно регистровање и не пружа могућност праћења и утврђивања идентитета јесте део ОПСЕК – а.

2.1. Ниво домаћина (хоста)

У циљу што прецизнијег и потпунијег разумевања ОПСЕК – а неопходно је поновити више пута да безбедност и сигурност, у оперативном смислу, криминалистичким полицајцима придржавање смерница ОПСЕК – а само на једном нивоу не гарантује анонимност. Неопходно је придржавати се више правила и смерница на свим нивоима. Чак ни тада не постоје апсолутне гаранције, обзиром да се у овом свету веома брзо све мења.

На нивоу домаћина (хоста), неопходно је разумети да сваки оперативни систем има својства које се могу искористити како би се повредила анонимност корисника система. Сваки систем скупља податке о

[4] https://community.cisco.com/t5/other-network-architecture-subjects/lan-switching-routing-ip-mac-stripping/td-p/534743 последњи пут приступљено 08.06.2024. год.

[5] https://www.tech-lifestyle.com/top-5-lista-najbolji/top-5-najbolji-imejl-klijent-za-android-u-2021-godini/

кориснику, адресе на које иде, који претраживач користи, уобичајене поставке појединих софтвера, специфичне софтвере за коришћење и сл. У циљу заштите анонимности неопходно је користити живе оперативне системе који се подижу (бутују) на другом систему и представљају врсту гаранције с`обзиром на њихове претходно подешене параметре – један од њих је:

- Тејлс (Tails) – он представља жив оперативни систем, који се може инсталирати и подизати са скоро било ког оперативног система. Овај систем за циљ има заштиту приватности и анонимности корисника. Све интернет конекције и комуникације остварују се преко TOP-a. Свуда је обезбеђено да се хттпс аутоматски користи, као уобичајено подешавање. Овај оперативни систем нема трајно складиште података, нема диск који похрањује податке о систему, кориснику и интеракцијама ова два.
- Хуникс (Whonix) представља оперативни систем инсталиран као верну копију виртуелне машине. Дакле овај систем се подиже у оквиру виртуелне машине и оперише у систему сендбокса[6] – систематике у којој овај систем не оставља трагове ни на систему који контактира ни на систему на ком је подигнут. Циљ му је заштита приватности и анонимности корисника и сва се комуникација одвија у оквиру заштићене TOP мреже, поседује трајни диск за похрањивање података. Овај систем поседује и облике заштите против ДНС/ИП (DNS/IP) адресних / локацијских цурења. Систем поседује заштиту од цурења информација о лоцирању корисника преко ИП адреса и ДНС лоцирања. Хардверске информације код овог система су сакривене од непозваних и неовлашћених лица.
- Кјубес (QUBES) јесте оперативни систем који садржи изоловане апликације, чија основна функција бива првенствено заштита анонимности и приватности корисника. Ове апликације су такве да се изоловано активирају потпуно независно од система и одрађују своје задатке у заштићеном окружењу. Корисници могу одредити нивое безбедности коришћене унутар оперативног система и додељује им се адекватна боја у складу са безбедносним нивоом. Кјубе има безбедносни домен, који представља основу безбедности корисника и апликација које сам иницира.

[6] Простор који представља сигурно место за експериментисање, парадигма дечијег игралишта у песку.

2.2. Ниво датотека (метаподатака)

Метаподаци, настају на нивоу датотека и служе за описивање карактеристика које се везују за такву датотеку, најчешће су то лаичком оку невидљиви подаци. У њих спадају следеће категорије података:

- EXIF (Exchangeable Image File Format) подаци подразумевају податке које по уобичајеним подешавањима настају приликом прављења фотографије од стране система. Ови подаци обично садрже карактеристике камере, отвор бленде у датом тренутку, експозицију, али и неке друге, нпр. гпс локацијске податке, податке о уређају који је генерисао слику и сл.
- Временске ознаке (Timestamps) у смислу датума и тачног времена (према времену уређаја) генерисања фотографије
- Геолокацијске податке (Geolocations)
- Података о носиоцу комерцијалних ауторских права (Copyright)
- Податке о датотеци (File info)
- Податке о музичкој датотеци – извођачу и нумери, као нпр. и албуму, години издања и сл. (ID3 music info)
- Заглавља протокола (Protocol headers)

Приказане информације могу пружити значајну количину података о кориснику, шта више оне могу бити значајна помоћ при идентификацији корисника. Ово никако не желимо за оперативне активности, нарочито за оперативца који је инфилтриран у одређену средину и прикупља податке од значаја за могућност покретања истраге односно за документовање кривичних дела и учинилаца и њихових веза.

Оруђа која се могу користити у овом смислу да се метаподаци могу прочитати и постати видљиви чак и лаичком оку су различита. Већина их је софтвера отвореног кода, али има и комерцијалних. Они су:

- Ексифтул (Exiftool) представља библиотечки тип софтвера који поседује капацитете читања и похрањивања метаподатака у широком дијапазону датотека. Његова командна линија може представљати старт у анализи метаподатака различитих типова датотека, али најчешће фотографија. Видљива резултанта овог софтвера је садржина метаподатака у виду груписаних карактеристика нпр. уређаја који је генерисао фотографију, карактеристика камере, величина креиране датотеке, карактеристике фотографије висина резолуције, отвор бленде и сл.
- Метагуфил (Metagoofil) представља оруђе за прикупљање података које је дизајнирано за извлачење (екстраховање) метаподатака из јавних докумената који припадају мети – субјекту чији се подаци желе прибавити оперативним путем.

2.3. Ниво корисника

Корисници на интернету морају бити опрезни у погледу свог идентитета и својих афинитета, а као показатељ опасности које вребају јавља се свакодневна количина пропагандних порука које стижу сваком просечном кориснику, након једног дана претраживања без икакве заштите. Оперативци приликом предузимања радњи оперативне природе на нету морају вишеструко бити свесни и на опрезу када прикупљају податке и информације, из много разлога. Основна смисао јесте да мета прикупљања информација не буде упозорена на активности припадника органа гоњења. Наравно, поред упозоравања мете, субјекта који је циљ операције, не треба упозоравати ни оне мете које су само тангентно везане за оперативно прикупљање података и информација, а које могу бити од великог значаја за оперативно поступање и истрагу, уопште. Поред описаних момената, некада је у случајевима прикривених активности у циљу прикупљања обавештења и доказног материјала неопходно да се обезбеди оперативац од несмотреног остављања трагова који могу бити показатељ криминалцима да их неко прати, прислушкује и евидентира њихове активности на мрежи. Генерално, неопходно је да оперативни радници евидентирају сопствене радње и документују активности које предузимају у циљу откривања и расветљавања кривичних дела и учинилаца али од круцијалног је значаја да њихове активности ипак остану тајна за друге учеснике у комуникационом саобраћају до момента када се реализује оперативна активност у лишењу слободе и хапшењу лица умешаних у криминалне активности које су надзиране тим путем. Са друге стране сваки учесник на даркнету, без обзира да ли је купац или продавац, користиће најразличитије методе прикривања сопственог идентитета и своје личности, шта више већина ће их имати лажне идентитете и врло често ће их користити вишекратно. Креирање лажне личности – идентитета на интернету обухвата више елемената: име, евентуално презиме, електронску адресу, датум рођења, локацију, шифре и стил писања. У том циљу на интернету постоје апликације које омогућавају брзо креирање оваквих лажних личности (идентитета) и то без бојазни да ће се открити да је у питању лажна личност. Ове апликације иду толико далеко да креирају лажну историју и присуство на интернету лажних личности. Неке од њих су https://www.fakenamegenerator.com/ или https://randomuser.me/ а свака од њих је са својим специфичностима и карактеристикама, те се очекује од оперативца да према својим афинитетима изаберу своју омиљену апликацију и лажну личност. Овде се поставља питање поновног, или вишеструког коришћења одређене личности зато што одређена лажна персона коју користимо може направити

добру репутацију на даркнет маркетима, али са друге стране може бити и „провољена“, откривена, – па тиме и токсична за друге кориснике. У сваком случају вишеструко коришћење једне лажне персоне проблематично је са аспекта анонимности.

- Са аспекта анонимности од круцијалне је важности користити у оперативним активностима искуства криминалних миљеа. У сврху очувања анонимности веома је важно користити криптовалуте приликом плаћања или наплаћивања услуга, али се и том приликом треба водити претходним искуствима и мудро користити оне валуте које су стварно заштићене и стварно анонимне – искључујући биткоин – БТЦ. Биткоин се као криптовалута најчешће користи у трансакцијама везаним за даркнет маркете и купопродају роба и услуга на њима, али ова валута је само псеудоанонимна – она пружа делимичну заштиту корисника, њу је могуће пратити, односно могуће је пратити трансакције корисника. Разлог овоме јавно присуство у пулу трансакција, јавности блокчејна трансакција које су свима доступне и могуће је пратити износе и трансакције и кориснике посредно кроз овако постављен систем. Са друге стране Монеро (XMR) је много заштићенија криптовалута фокусирана на анонимност корисника, са приватним блокчејном и анонимним (прикривеним) трансакцијама. Наравно, осим биткоина нуди се могућност трговине и путем стабилнијих валута Рипла (Ripple XRP) и Етера (Ether ETH) (Слика бр. 5).

Слика бр. 5. Виртуелне валуте Рипле, Етера, Биткоин и Монтеро.

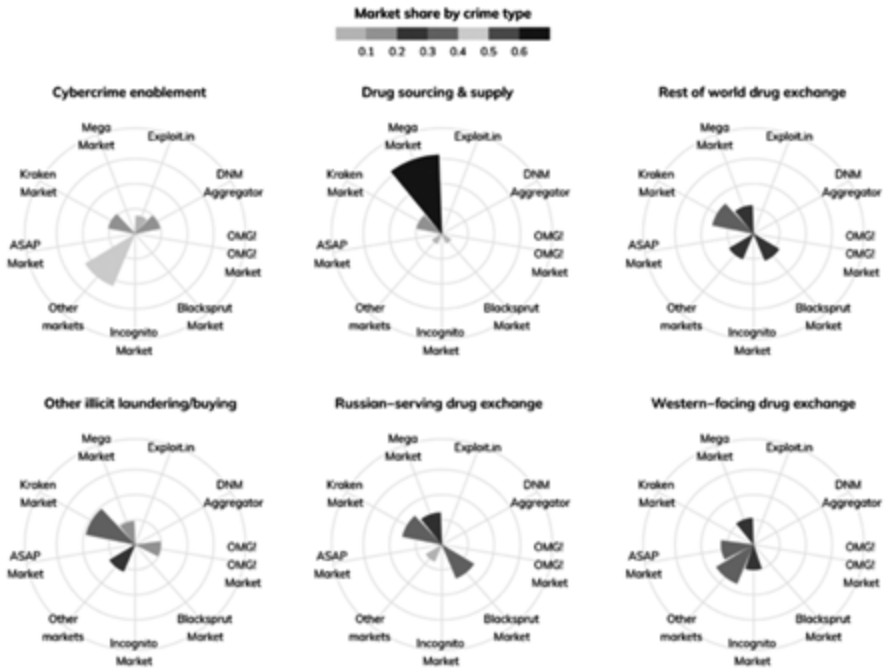
Поред самог избора криптовалуте од непроцењивог значаја је и начин на који се прибављају криптосредства, као и на који начин их конвертовати у „фијат“ (реалне) валуте као што су УСД или ЕУР. Такође је овде значајно указати и на могућности коришћења различитих услуга на даркнету у виду миксера, тамблера или других облика „перача“ ових криптовалута.

На нивоу корисника од великог значаја је у циљу анонимности користити различите облике верификације (аутентификације) за комуникациони саобраћај који се са другима остварује. ПГП (*Pretty Good Privacy* – PGP) јесте техника шифровања (енкрипције) која се користи за обезбеђивање како приватности тако и потврду - аутентификацију комуникационог

саобраћаја подацима. Применом ПГП појединац може потписати, шифровати и дешифровати поруку, користећи криптографску технику која обухвата пар кључева у виду јавни/приватни кључ.

Још један моменат је од значаја за очување идентитета, а односи се на физичко преузимање предмета и поштанских пошиљки поручених преко интернета – сам пријем истих од стране поштанских и курирских предузећа. Први моменат о којем треба водити рачуна односи се на сам контакт ових служби са лицем које преузима пошиљку. Неће се у великом броју случајева корисник одлучити да у овом кораку поставља мулу која преузима пошиљку, али је и то могуће, међутим, код оперативаца треба и о овом моменту водити рачуна. Са друге стране у циљу проналажења продаваца на даркнет маркетима може се узети у обзир приликом планирања праћења да они морају:

- Куповати амбалажу за продукте које шаљу путем курира или поште – кутије, станиолске фолије, целофан и сл. (лоцирање, идентификација)
- Куповати маркице или наручивати курире (лоцирање, идентификација)
- Паковати пакете (ДНК, отисци папиларних линија)
- Достава (указује на локацију – регион)



Слика бр. 6. Преовлађујућа криминална даркнет тржишта у 2023. (Извор: https://www.chainalysis.com/blog/darknet-revenue-2023/)

У циљу прикривања идентитета извршиоци у већини случајева прибегавају различитим методама које иду ка избегавању могућности цурења информација ка лицима која их могу искористити у циљу праћења. На пример већ објашњавано слање мула у циљу преузимања пошиљака, се може користити и у циљу прикривања идентитета код преузимања исплата на банкоматима криптовалута. Са друге стране могуће је користити различита средства за антифорензичку заштиту у моментима паковања, у виду заштитних рукавица, заштитних одела у циљу спречавања трансфера ДНК материјала у пошиљке. Куповина маркица или наручивање курирских услуга такође је могуће избећи, на пример преко услуга: *Stampnik*, за које се УСПС маркице могу купити преко интернета за биткоине (БТЦ).

Примери из реалног живота указују на примене различитих техника и њихов утицај на заштиту анонимности и идентитета корисника интернета.

Први пример је из 2013. год. током завршних испита на Харвардском универзитету када је студент користио TOR и герила мејл (Guerilla mail) сервис електронске поште који је потрошан – и који не задржава много података о кориснику, али није фокусиран на анонимност. Заглавље (Хедер) као део мета-података мејла је открио да је корисник – пошиљалац мејла користио TOR, а такође је показао временске одреднице. У том периоду на том простору само један студент је користио TOR мрежу на универзитетској бежичној (WiFi) мрежи. Наравно када је ухваћен он је и признао слање електронског писма и активност. Овај корисник није користио заштиту на два нивоа заштите – на корисничком и хостовом нивоу. Он је користио заштиту на нивоу датотека и мрежном нивоу.

Други пример је Рос Улбрихт (*Ross Ulbricht*) оснивач Пута свиле (*Silk Road*). Он је још у 2011.год. на биткоин форуму рекламирао под надимком *алтоид* свој вебсајт, који је представљао први организовани облик даркнет маркета. *Алтоид* је поставио оглас за потребом за запошљавањем ИТ професионалца и да се заинтересоване стране могу њему обратити на имејл rossulbricht@gmail.com. На основу судске наредбе о откривању идентитета корисника електронске адресе дошло се до оптужнице и пресуде најозлоглашенијем оснивачу пута свиле. Он је предузео мере заштите на три од четири објашњена нивоа – на мрежном, датотечном и хостовом нивоу, али је успео да подбаци на корисничком нивоу.

Трећи пример је Хозе Порас (Jose Porras) који је био продавац на даркнет маркету и који је продавао премијум марихуану и друге наркотике. У циљу приказа квалитета робе конкретно марихуане, он је поставио сопсвене фотографије на којима држи примерке робе у руци на фото

услужној софтверској платформи Имгур (*Imgur*) не размишљајући да ће на тај начин приказати сопствене папиларне линије и учинити их доступним свима. То је и искористио припадник ХС (хомеланд секјурити) у САД и скинуо (даунлоадовао) његову фотографију и упоредио отиске прстију са постојећим у бази података и утврдио идентитет продавца – Хозеа. Овај корисник је успео да пропусти заштиту на нивоу датотеке.

ОПСЕК мере обухватају четири већ приказана нивоа заштите, међутим оперативци морају имати реалне процене и морају се придржавати мера заштите на свим нивоима заштите. На мрежном нивоу неопходно је користити ТОР/И2П/ВПН, као и приватношћу оријентисаним имејл услугама. На хост нивоу обавезно користити оперативне лајв системе као што су Тејлс, Хуникс и Кјубес (о чему је раније говорено). На нивоу датотека водити рачуна о метаподацима на датотекама, али и о садржајима на датотекама. На нивоу корисника – креирати лажне личности, користити ПГП и заштитити се у вези са достављачима.

2.4. Тор – Tor

The Onion Router – ТОР представља специфичан облик усмеравања комуникационог саобраћаја, од стране система преусмеравања комуникација, на такав начин да се корисничка ИП адреса прикрива приказујући један од излазних чворишта овог система као ИП адресу корисника. Друга дефиниција је да је у питању анонимизирајући комуникациони сервис оријентисан на конекцију. Корисници користе путању везану за извор кроз велики број комуникационих чворишта и бирају „виртуелно коло" кроз мрежу, у којем сваки чвор зна свог претходника и наследника, а међусобно не знају све остале. Трећи облик дефиниције је да ТОР омогућава дистрибуирану мрежу сервера (луковичастих преусмеривача) у којој корисници одбијају своје ТЦП стримове – веб саобраћај, фајл трансвер протоколе ФТП, ССХ и сл. око преусмеривача, прималаца сопствених информација, посматрача чак и самих преусмеравајућих чворова, који имају проблем да прате овакве облике усмерених комуникација. Овај облик идеје за луковичасти облик преусмеравања комуникације зачета је још средином 1990-тих година. Циљ свих ангажованих на ТОР пројекту јесте да корисници интернета требало би да имају приватан приступ нецензурисаној мрежи (вебу)[7]. Деведесетих година 20 – тог века сигурност корисника интернета бивала све више проблематична па су се 1995.године, Дејвид Голдшлаг (David Goldschlag), Мајк Рид (Mike Reed), и Пол Сајверсон (Paul Syverson) из САД Лабораторије за морнаричка

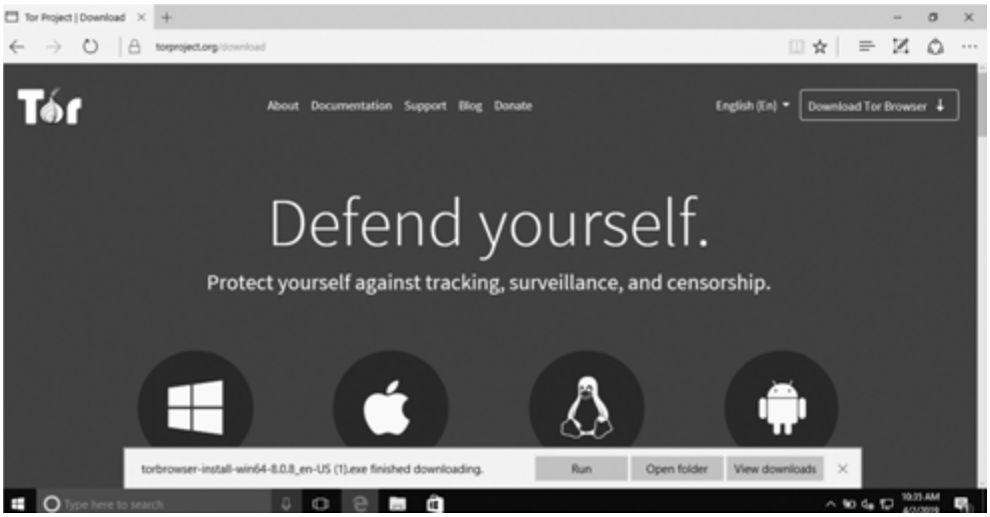
[7] https://www.torproject.org/about/history/ последњи пут приступљено 24.10.2022.год.

истраживања (U.S. Naval Research Lab - NRL) досетили су се да креирају прве истраживачке дизајне и прототипове луковичастог усмеравања комуникација (TOP)[8]. Циљ им је био да TOP омогући коришћење корисницима интернета са највећом могућом приватношћу уз идеју да се комуникациони саобраћај усмери кроз велики број сервера и да се шифрује проток комуникација приликом сваког корака на том путу података. Прави назив TOP, који се одржао до данашњег дана наденуо му је Пол Сајверсон, који је наставио заједно са дипломцем МИТ (Massachusetts Institute of Technology - MIT) Роџером Дингледајном (Roger Dingledine) и Ником Метјусоном (Nick Mathewson) са МИТ, са истраживањима и развојем пројекта током 2000-тих година XXI века. Основа TOP-а је од зачетка била заснована на децентрализованој мрежи, која је морала бити таква да функционише на ентитетима са различитим интересима и претпоставкама у виду поверења, а софтвер је морао бити бесплатан и отвореног кода како би максимизовао транспарентност и децентрализацију. Већ октобра 2002.год. приликом првог постављања система пуштен је софтвер отвореног кода и до краја 2003. године мрежа система је имала преко 10 волонтерских чворова највише у САД, а један у Немачкој. Већ 2007. године мрежа је почела са развојем премошћавања у циљу избегавања цензуре, као на пример у сврху заобилажења заштитних зидова (фајерволова) појединих владиних сајтова у циљу приступа корисницима TOP-а отвореној мрежи. Развој TOP Браузера започет је 2008. године. Веома значајну улогу TOP мрежа са тор браузером је одиграла у Северноафричком пролећу 2010. године чиме су не само заштићени идентитети лица која су учествовала у овим активностима, већ им је тим путем била доступна велика количина материјала која је била изван домашаја њихових влада. Потреба за оруђем које онемогућава масовни надзор комуникација јавила се као мејнстрим активност и насушна потреба у 2013.години, захваљујући Едварду Сноудену, а све око те афере указало је директно на TOP мрежу као једину непробојну у том тренутку. Данас ова мрежа има преко хиљаде релејних чворова, које покрећу волонтери, и има милионе корисника широм света.

---

[8] Финансирање развоја TOP–а током времена се мењало од одбрамбене индустрије САД, до донација грађана:

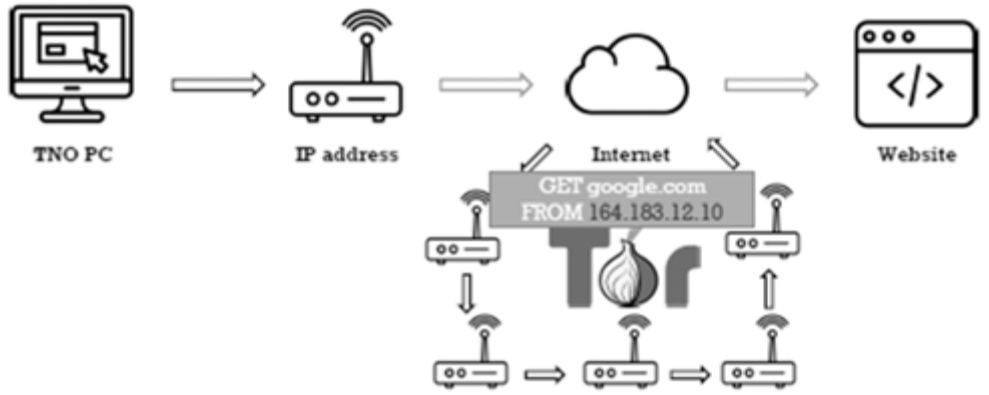
- Defense Advanced Research Projects Agency (DARPA) (2001-2006)
- Naval Research Lab (2006-2010)
- National Science Foundation (2006-present)
- Private citizen donations (2006-present).



Слика бр. 7. Изглед торовог претраживача (Извор: https://ssd.eff.org/files/ssd/wysiwyg/pictures/170/content_run_tor.png)

Мрачна мрежа може изгледати велика, али она то заправо није. Истраживачи из *Recorded Future* процењују да иако постоји више од 55.000 постојећих домена лука, само 8.400 (или отприлике 15%) ових сајтова је било активно. То значи да је укупна мрежа живих тамних веб локација само око 0,005% величине површинског веба.

Тамни веб домени су обично недоследни — нови се појављују, а други нестају, што има смисла јер неки од ових сајтова могу да нуде сумњиву или нелегалну робу и услуге.



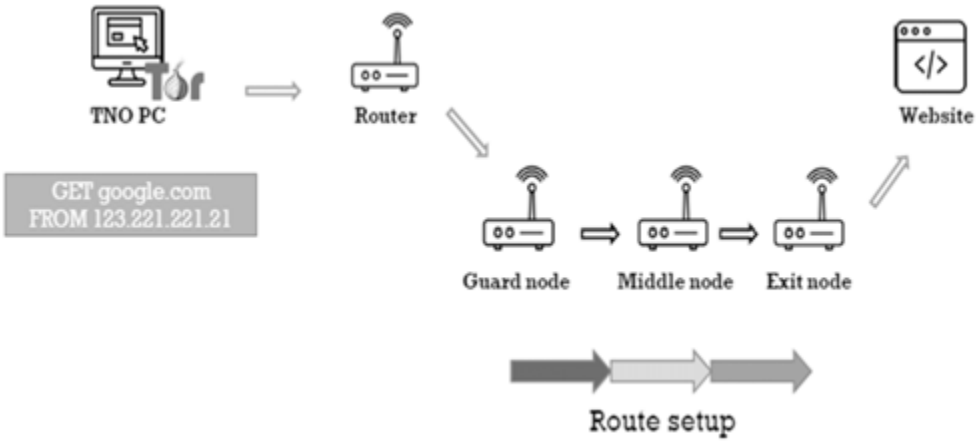
Слика бр. 8. Функционисање TOP-а (Извор: www.torproject.org)

Пројекат Тор каже да од 2 милиона људи који свакодневно користе Тор, само 1,5% њих приступа скривеним или тамним веб локацијама. И

већина веб-сајтова на мрачном вебу је на енглеском — према једној процени, невероватних 78% информација на мрачном вебу је на енглеском.

Како ради TOR? TOR представља мрежу виртуалних тунела који омогућавају корисницима унапређивање сопствене приватности и безбедности на интернету. TOR функционише на такав начин што преусмерава комуникациони саобраћај корисника преко случајно изабраних сервера, који се називају релеји, у оквиру TOR мреже (Слике 8 и 9). Последњи релеј у мрежи назива се излазни релеј и он усмерава саобраћај корисника на јавни интернет. Tor браузер користи TOR мрежу како би заштитио приватност корисника и анонимност. Коришћење TOR мреже има две најзначајније карактеристике:

- Интеренет провајдер услуга (ИСП) као и било ко други ко врши надзор над комуникацијама неће бити у могућности да прати активност корисника TOR мреже, укључујући имена и адресе вебсајтова које корисник посећује
- Администратори вебсајтова и услуге које корисници користе као и било ко ко их надзире биће у прилици да виде конекцију која долази из TOR мреже, уместо ИП адресе корисника и неће бити у могућности да утврде идентитет осим уколико се корисник сам не идентификује.



Слика бр. 9. Начин организације комуникације у TOR мрежи (Извор: https://www.torproject.org/)

Такође, треба напоменути да је TOR браузер дизајниран на начин да онемогућава вебсајтове да идентификују кориснике на основу конфигурације софтвера за крстарење интернетом – браузера. Он је по уобичајеним карактеристикама подешен да не задржава историју претрага и посета на интернету. Колачићи (*cookies*) су валидни само за једну сесију

коришћења на интернету (док се не напусти TOP браузер и захтева нови идентитет при следећој сесији). У суштини TOP онемогућава лица да сазнају локацију корисника и њихове навике приликом коришћења интернета, које сајтове посећују, утврђивање њихове физичке локације. Он је намењен веб браузерима, инстант месицингу, удаљеним логовима, и многим другим активностима интернет корисника. Он представља бесплатан и отворен код за све облике оперативних система корисника (Windouz, Linuks/Juniks, Android и сл.). У почетку TOP је за циљ имао да обезбеди ефективну оперативну комуникацију првенствено припадницима министарства одбране САД у непријатељском окружењу, а данас се њиме користе најразличитији обични људи, пословни људи, новинари, грађани, полицајци, припадници медија, активисти, али и војска и обавештајне службе. Групе просечних корисника интернета представљају следећу групу, који користе TOP у циљу сопствене заштите, своје деце, као и сопственог достојанства приликом коришћења интернета. Пословни људи користе TOP како би надзирали представнике своје конкуренције, такође и како би очували и сачували сопствене пословне тајне, односно у циљу очувања унутрашње (у оквиру фирме) одговорности и поузданости. Медији и припадници медија – новинари користе TOP да би заштитили сопствено истраживачко новинарство и своје изворе информација. Војска и припадници органа гоњења користе TOP у циљу заштите сопствених комуникационих канала, истрага и обавештајних података и информација.

Некада се може десити да ИСП блокира директан приступ TOP мрежи, а некада и органи државе у којој корисник има приступ. TOP претраживач има неке алатке које помажу у заобилажењу оваквих блокада. Ове алатке називају се транспортни прикључци „*pluggable transports*“. У овом тренутку (новембар 2022.год.) постоје три овакве алатке бфс4, меек и Пахуља.

Табела 2. Прикључни транспортери TOP браузера

bfs4	bfs4 чини TOP саобраћај таквим да изгледа као случаја а такође онемогућава цензоре у проналажењу премошћавања кроз интернет скенирање
meek	meek транспортери чине да изгледа као да корисник претражује главне вебсајтове уместо да користи TOP мрежу . meek-azure чини да изгледа као да се користи Мајкрософтов (Microsoft) вебсајт.
Snowflake	Snowflake је унапређење флешпроксија (Flashproxy). Шаље комуникациони саобраћај кроз WebRTC, peer-to-peer protocol са уграђеним NAT punching.

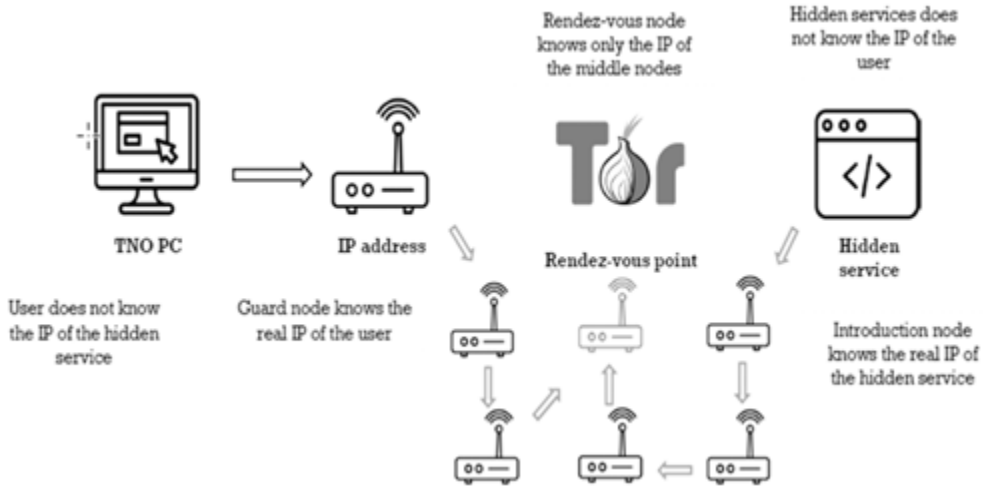
Сваки од приказаних користи се у специфичним ситуацијама, сваки од њих функционише на различитим концептима и њихова ефективност зависи од индивидуалних околности у којима се корисник налази. Уколико се покушава заобићи блокирана конекција по први пут неопходно је пробати сваки од прикључних транспортера, а ако ни један не профункционише онда корисник мора да захтева премошћавање или да мануелним путем унесе адресу премошћавања. Начин на који се прибављају ове адресе је везан за лично захтевање, а то може бити на следеће начине:

- Приступити https://bridges.torproject.org/ и пратити инструкције
- Послати имејл на bridges@torproject.org са Gmail, или Riseup имејл налога
- Користити MOAT како би унутар TOP браузера прибавили премошћавање
- Послати поруку @GetBridgesBot на телеграму са процедуром: куцати Start или /bridges у чету. Копирати адресе премошћавања и на:

• TOP браузеру (на десктопу) кликнути на „Settings“ на хамбургер менију (≡) затим на „Connection“ у сајдбару. У оквиру секције премошћавања („Bridges") у опцији „унети адресу премошћавања коју већ знате“ (Enter a bridge address you already know") кликнути на „додати премошћавање мануелно“ („Add a Bridge Manually") и унети свако премошћавање у посебној линији.

• TOP браузеру (на андроид уређајима) кликнути на подешавања 'Settings' (⚙) затим на „конфигурација премошћавања“ ('Config Bridge'.) подесити „користити премошћавање“ ('Use a Bridge') и изабрати обезбедити премошћавање које је познато ('Provide a Bridge I know').
  - Могуће је и преко MOAT-а директно уносити премошћавање
  - Такође могуће је и на основу QR кода.

Треба посебно указати на то да постоје и тзв. Скривене услуге TOP-а, а које најчешће бивају коришћене на даркнету. Сакривени сервиси су вебсајтови који не напуштају TOP мрежу. Они обично обухватају адресе које се завршавају на *.onion* врхунске нивое домена (*Top Level Domain* - ТЛД). V.2: подразумевају 16 карактера случајно генерисаних засновано на приватном кључу а V3:56 карактера случајно генерисаних засновано на приватном кључу. Овако функционише дарквеб.

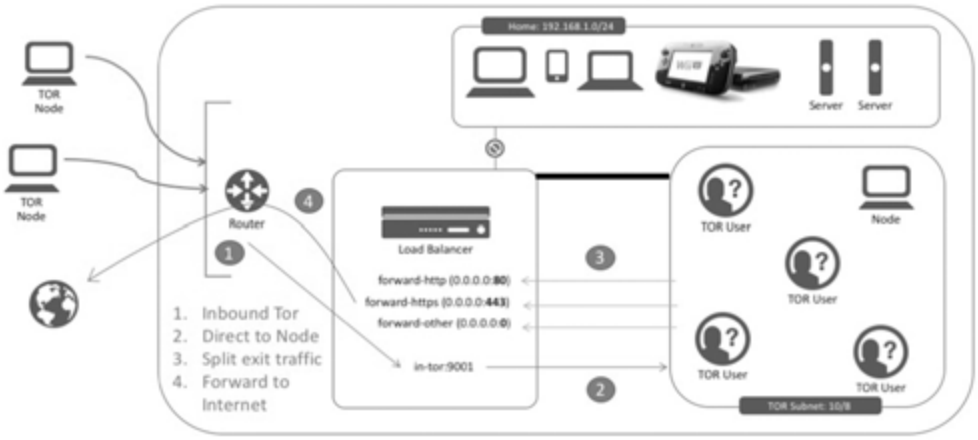


Слика бр. 10. Начин функционисања сакривених сервиса TOR мреже (Извор: https://www.torproject.org/)

У погледу капацитета у сврху доказивања и доказног поступка, као и предистражног и истражног поступка, TOR и поступања како корисника TOR мреже тако и органа гоњења веома је значајно разумети све елементе система као и начин како систем функционише, те улоге појединих елемената система (Слика бр. 10). Првенствено треба разумети систем са аспекта органа гоњења у циљу разумевања стадијума, стања и поступака у циљу расветљавања и документовања активности на расветљавању и доказивању кривичног дела и приписивању учиниоцу. Секундарно са аспекта корисника од значаја је код разумевања поступака у циљу јасног раздвајања свесног од несвесног поступања и законитог и незаконитог домена активности на даркнету. У погледу расветљавања кривичних дела, са аспекта органа гоњења дигитално окружење и дигитални трагови имају овде примат, као и познавање природе и начина настанка и евентуалног проналажења сакривених дигиталних трагова, те њиховог изазивања и чувања и похрањивања. Но то не значи да класичан оперативни полицијски рад овде изостаје или класични облици материјалних трагова и све везано за њих. Управо супротно, у целини активности припадника полиције обе ове сфере имају узајамно повезане улоге и значај. Дакле докази у материјалном смислу су и овде веома присутни, папирни (и физички усмени) захтеви према одређеним субјектима у поступку морају бити присутни (захтеви за хитно задржавање података, пружање обавештења, увида и извода из евиденција корисника, ИП адресе, подаци о времену и датумима

приступа и сл.). Адекватне процедуре контактирања правних лица у циљу прикупљања обавештења нпр. о корисницима услуга и њиховим адресама и контактима и сл. Посебно, везано за прибављање наредаба за претресање уређаја и привремено одузимање предмета и сл.

У овом моменту веома је битно напоменути да TOP не може решити питања и проблеме који се везују за анонимност, мрежа и браузер се фокусирају на заштиту транспорта комуникационих података. Анонимност захтева примену додатних специфичних софтвера који чине подршку TOP мрежи и браузеру. На пример, може се користити TOP дугме на браузеру док крстари интернетом како би се прикриле одређене информације о конфигурацији рачунара који се том приликом користи. Наравно корисници морају бити довољно стручни како би заштитили и очували сопствену анонимност. У том смислу никако не треба нудити сопствене личне податке или друге информације о себи приликом попуњавања одређених формулара на интернету. Сваки корисник мора бити свестан да као и друге анонимизирајуће мреже које су довољно брзе за крстарење по нету TOP мрежа не обезбеђује подршку од временских напада на крајње тачке комуникационе конекције. Уколико нападач има начин да прати саобраћај који долази са корисниковог рачунара, као и саобраћај на дестинацији коју је корисник изабрао, он може применом статистичке анализе открити да ови облици комуникације јесу део истог комуникационог кола.[9]



Слика бр. 11. Анализа мрежног саобраћаја корисника (Извор: https://www.f5.com/labs/articles/threat-intelligence/snooping-on-tor-from-your-load-balancer)

[9] Zirojević Mina, Ivanović Zvonimir; Cyber law – Serbia, Institut za uporedno pravo, 2022.

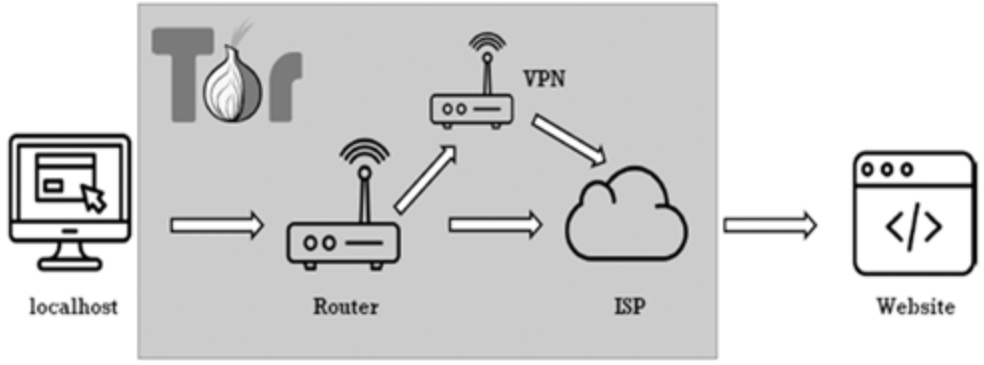
Постоје напади који за циљ имају подривање TOP мреже и она сама није имуна на такве нападе. Напади обухватају следеће видове:

- Нападе на TOP мрежу – мета ових напада обухвата целокупну мрежу, најчешће путем великог броја малициозних TOP чворова
- Напади на скривене сервисе – ове услуге се циљају са намером да се идентификују
- На TOP клијент – мета је браузер у циљу откривања идентитета корисника
- На корисника – где се циља конкретан корисник

Могуће је циљати препознавање TOP саобраћаја кроз анализу мрежног саобраћаја, на пример коришћењем *Wireshark* софтвера. Овај саобраћај се може посматрати на различитим местима.

Када се разматрају напади на TOP мрежу, они се могу груписати у следеће категорије:

- Корелациони напади
- Конгестиони (комуникационо-загушујући) напади
- Временски напади
- Напади „отисака прстију“
- ДОС – напади ускраћивања сервиса (*Denial of Service Attacks*)
- Напади подршке
- Напади откривања сакривених услуга



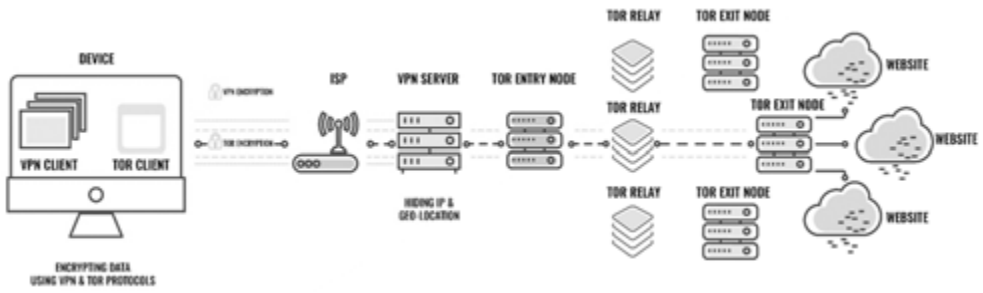
Source IP.	Port.		Dest IP.	Port	Protocol
12.23.34.56	65738	→	23.34.56.78	80	HTTP
12.23.34.56	65738	→	23.34.56.78	443	HTTPS / TOR
12.23.34.56	65738	→	23.34.56.78	9001	TOR

Слика бр. 12. Анализа мрежног саобраћаја корисника
(Извор: www.torproject.org)

У погледу коришћења различитих услуга којима се корисници на интернету могу прикривати у циљу заштите своје приватности, анонимности и прикривања места приступа и идентитета (као корисника) у употреби је велики број оруђа и алатки. Неки од њих су прокси сервиси, анонимизатори, прокси мреже: FreeNet, I2P, JAP, TOP (The Onion Router - TOR) и у оквиру ње TOR hidden services.

Шта су проксији и анонимизатори? Ове алатке подразумевају друге рачунаре, преко којих се преусмерава комуникациони саобраћај. Дакле они су други уређаји, по правилу рачунари, који се користе да преусмере комуникациони саобраћај корисника који их ангажују. Понекада се они одређују као капије (Gateway) или тунелни проксији (Tunneling proxy). Они у основи представљају услужне алате који уместо да приказују адресу корисника приказују адресу прокси сервера приликом приступа одређеним сервисима – вебсајтовима, услугама и сл, Дакле приказују адресу посредничког уређаја, а не адресу уређаја који је корисник користио за приступ мрежи.

Циљеви и разлози примене проксија (посредничког уређаја)[10] се своде на то да се уређај који се користи услугом посредничког уређаја не открије директно већ да се његов дигитални траг прикрије приликом комуникације. Поред овога циљ може бити и убрзање приступа одређеним групама корисника – када је у питању кешинг прокси (Caching proxy), може се такође применити и у случајевима када администратор мреже примењује посебну политику приступа одређеном садржају – где се филтрира приступ одређеном садржају, исто код случајева логовања интернет коришћења, али и код скенирања малвера који улази у облику комуникационог саобраћаја и спречавање цурења информација у облику излазног комуникационог саобраћаја.



Слика бр. 13. Функционисање мреже на Дарквебу
(Извор: https://www.comparitech.com/blog/vpn-privacy/ultimate-guide-to-tor/)

[10] Proxy – у енглеском језику долази од procuracy, а у свакодневном језику подразумева опуномоћење да се друго лице представља или заступа у одређеним пословима – дакле у име и за рачун другог лица.

Начини прибављања проксија и прокси сервера су веома прости, али се треба руководити добром праксом са аспекта органа гоњења, и само они који су вишеструко доказани као сигурни и безбедни требају се користити. Већина оних који су комерцијални су уједно и они који испуњавају ове услове, као што су:

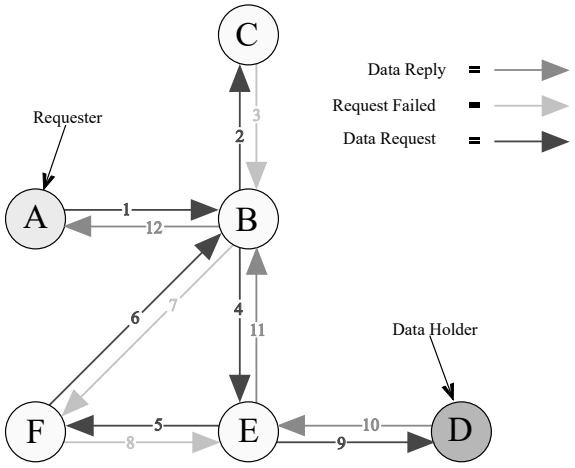
– Behidden.com
– Hide-my-ip.com
– TheSafeProxy.com
– ProxySwitcher.com

Бесплатни којих има на хиљаде, а који нису увек тако поуздани су:

– Безбедни прокси (SafeProxy)
– Протон ВПН protonmail.com, protonVPN
– Freeproxy.ca

Поред ових постоје и тзв. Напредне прокси мреже, које подразумевају да је њихово мрежно окружење – цела мрежа потпуно анонимна. Такве мреже су:

- Слободна мрежа – FreeNet – Fuquid, Frost
- Невидљиви Интернет Пројекат - I2P: Invisible Internet Project
- ЈАП – JAP: Java Anon Proxy
- ТОР – The Onion Router (TOR) који у оквиру сопствене мреже нуди и
  – ТОР скривене сервисе – TOR hidden services
  – ТОР ту веб - Tor2web



Слика бр. 14. Типичан низ захтева. Захтев се креће кроз мрежу од чвора до чвора, повлачећи се из ћорсокака (корак 3) и петље (корак 7) пре лоцирања жељене датотеке. (Извор: https://en.wikipedia.org/wiki/Freenet)

Слободна мрежа – FreeNet јесте бесплатни софтвер који омогућава корисницима анонимно дељење датотека, сурфовање и објављивање слободних сајтова (сајтови – веб странице којима се може приступити само преко слободне мреже), као и четовање – размењивање комуникационих порука без страха од цензуре.или надзора[11]. Ова мрежа је децентрализована у циљу оснаживања исте на могуће нападе, чиме је мање рањива за познате нападе, а уколико се користи у „даркнет" моду, у којем се корисници повезују само са познатим и пријатељским конекцијама чини је веома тешком за инфилтрацију и идентификацију корисника. Комуникација међу чворовима слободне мреже је шифрована (енкриптована) и преусмеравана је преко других чворова како би отежала утврђивање тога ко захтева информацију и који је њен садржај. Корисници доприносе мрежи на начин што препуштају свој део комуникационог снопа комуникационих канала (бендвит – простим речима део свог интернета - комуникационог спектра, који користе) као и свој физички простор на чврстом диску – за похрањивање података (назива се „продавница - депо података"). Датотеке се аутоматски памте – похрањују или бришу у зависности од тога колико су популарне, где мање популарне бивају одбачене у циљу прављења места за друге популарније. Датотеке су шифроване (енкриптоване) тако да их корисник на чијем физичком простору се налазе не може лако открити садржај и тиме „фактички" не може сносити одговорност за њих (поседовање или дистрибуцију). Међутим, самим пристанком на такве активности може се говорити о посредној одговорности да се учествује у нелегалним активностима, тако да су границе могуће неодговорности за последице ипак веома порозне у овим случајевима. Форуми за чет – причаонице, вебсајтови, као и функционалност претрага сви су надограђени на овом дистрибуираном облик продавнице – депоу података. Најважнији скорашњи облик развоја ове мреже јесте оно што је успело веома малом броју мрежа ове врсте – а то је „даркнет". Само кроз повезивање лица која међусобно једни другима верују, корисници могу смањити своје рањивости и изложеност надзору, а уз то повезивање на глобалну мрежу преко „пријатељевих пријатеља" омогућава коришћење слободне мреже и на местима где је она нелегална, а то чини скоро немогућом ову мрежу за обарање или блокирање, од стране влада држава које је бране. Програми слободне мреже су:

– Фрост – Frost: табла за размену порука (са групама) - Message Board (Newsgroups)
– Thaw/Frost/Fuqid: (P2P file sharing) – П2П размена датотека
– Странице слободне мреже Freenet pages: (Web pages)
– Чет слободне мреже – Freenet Chat: (Instant Messaging)

[11] https://freenetproject.org/pages/about.html последњи пут приступљено 26.10.2022.год.

У циљу примене различитих мера за заштиту сопствених података и идентитета на мрежи постоји велики број различитих пројеката чија сврха је блиски овом циљу. Неки од њих су нпр. тејлс (Tails), Орбот (Orbot), Арм (Arm), Атлас (Atlas), Стем (Stem), као и већ помињани TOP транспортни прикључци као и TOP облак.

Тејлс (*Tails*) представља бесплатан оперативни систем који се подиже као живи ДВД/УСБ оперативни систем који је дизајниран на начин да не оставља податке о рачунару са којег се приступа као и навикама корисника, а долази унапред конфигурисан за коришћење TOP мреже безбедно[12]. Уз њега долазе и алатке неопходне за адекватно поступање на интернету без бојазни да ће се одређени подаци „офирати" онима који надзиру комуникациони саобраћај, осим у случајевима неопрезности корисника. Значајно је напоменути да овај систем не оставља трагове на рачунару са којег се подиже и користи, осим уколико корисник то експлицитно не захтева од самог система. На овом систему се користе најмодерније и најефикасније криптографске алатке за енкрипцију датотека, имејлова и инстант порука.

Tails Orbot Arm Atlas Stem

Слика бр. 15. Програми слободне мреже

Орбот је софтвер отвореног кода, бесплатан је и чини га TOP виртуелна приватна мрежа (ВПН)[13] која се подиже услужно за кориснике андроид оперативних система, који тренутно имају највећи удео у мобилним уређајима за телекомуникације као облик функционалних оперативних система (преко 70% актуелног светског тржишта)[14]. Сам Орбот штити

[12] https://tails.boum.org/ последњи пут приступљено 28.10.2022.год.

[13] VPN – Виртуелна Приватна Мрежа као термин означава остваривање заштићене комуникационе мреже повезаности приликом коришћења јавне комуникационе мреже. ВПН шифрује кориснички интернет комуникациони саобраћај и прикрива онлајн идентитет корисника. Ова метода омогућава корисницима погодности које отежавају трећим странама могућност њиховог праћења и крађе њихових података. Упоредити са https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn или https://www.avast.com/c-what-is-a-vpn последњи пут приступљено 27.10.2022.год.

[14] https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/ последњи пут приступљено 27.10.2022.год.

и деблокира специфичне апликације, а пружа брз и безбедан приступ популарним луковичастим услугама.

Арм представља апликацију која садржи командну линију – терминал као интерфејс путем којег корисник може надзирати и вршити додатне дораде у конфигурисању TOP мреже и њених функционалности. Овим се избегавају аутоматизовани облици конфигурисања мреже и напредним корисницима омогућава значајно управљање системом и заштитом.

Атлас је сајт који омогућава претраге TOP мреже – нуди три опције претраге – просту, напредну и комбиновану (агрегирану), а могуће је претраживање по надимку сајта, ИП адреси (192.0.0.2) и отисцима прстију сајта (9695DFC3) или комбиновано. Могуће је користити и локализаторе приликом претрага, а и са специфичним контактима или посебним елементима претрага (flag:Authority). Ако се претражује премошћење онда је кориснику неопходно да претражује преко хешираног отиска сајта (отисак који подразумева примену математичке функције на сајт како би представљао аутентични облик у сваком тренутку провере приликом примене исте функције на резултат).

Стем[15] је база података која садржи библиотеку скрипти и апликација које се користе у TOP мрежи а које служе смањеном оптерећењу програмера и преузимању скрипти у циљу потпунијег, бржег и ефикаснијег приступа мрежи и надограђивању постојећих заштита и оруђа у борби против надзора и праћења комуникација.

TOP облак (cloud) је кориснички пријатан и употребљив начин примене премошћавања комуникација који помаже корисницима у приступу нецензурисаном вебу.

TOP чине три веома специфичне компоненте:

- Мрежа
- Браузер пакет (бандл – *bundle*)
- Сервиси

Тор мрежу чине тор чворишта – којима управљају (оперишу) по правилу волонтери и ентузијасти. Они се јављају у више видова од којих су најзначајнији: излазни, релејни и чуварски[16]. Ови чворови су којима се верује, који

[15] https://stem.torproject.org/faq.html последњи пут приступљено 27.10.2022.год.

[16] Чуварски су они чворови којима је дозвољено да наступају као први облици чворишта у колу, излазни чвор служи као последњи облик чворишта у колу (поред ових постоје лоши излазни чворови за које се верује да су бескорисни обзиром да су цензурисани), брзи/стабилни чворови су погодни за брзе бендвит везе и кола, Ауторитетни представљају чворове који генеришу мрежне статусне документације, ХСДир јесте

имају специфично конфигурисање и посебну регистрацију, а везани су за корпорације. Начин на који мрежа функционише је следећи: Корисник мора имати ТОР клијент који по правилу представља одређени за то посебно конфигурисан интернет претраживач (браузер) који се назива ТОР интернет претраживач. Преко овог клијента контактира се ТОР мрежа и увезује се комуникација клијента на мрежу чиме се случајном путањом остварује конекција са адресом коју је корисник хтео да види (односно са којом је желео да оствари комуникацију). Први чвор који се овим путем контактира у мрежи назива се чуварски чвор. Ова комуникација од клијента ка Мрежи остварује се путем АЕС енкриптованог захтева ка и од ТОР мреже, дакле шифрованим комуникационим каналом. Даље комуникације у мрежи су преко неенкриптованих линкова – дакле без шифроване комуникације. Након првог контакта са чуварским чвором остварује се преусмеравање и премошћавање путем великог броја релејних чворома ТОР мреже при чему ни један у том дугом низу није свестан даљих чворова од оног који му шаље и ка којем иде комуникациони саобраћај. На крају последњи чвор кроз који пролази комуникациони саобраћај у ТОР мрежи је излазни чвор. По правилу су ови излазни чворови опште познати или се могу утврдити, а саобраћај од њих ка дестинацији је у облику неенкриптованих хттп пакета ка јавним серверима.

Тор обезбеђује прикривене услуге које омогућавају корисницима да поставе веб базиране сервисе познате као „прикривени сервиси“ или „тачке за сусрете“ у виду:

- Веб сајтова
- ССХ
- ФТП сајтова и
- Форуме

У овако обезбеђеним прикривеним сервисима по правилу се организују најразличитији облици илегалних активности а неки од њих (најчешће заступљени) су:

- Наркотици – психоактивне супстанце купопродаја
- Сексуална експлоатација деце и малолетних лица
- Клониране физичке кредитне и дебитне платне картице и бројеви
- Сервиси: хакерски, крекерски и малвер
- Биотоксини, кријумчарена и фалсификована роба оружје и друго

директоријум скривених услуга за в.2 луковичасте (онијон) адресеу ДХТ-у и он мора бити присутан олајн за најмањи тренутак времена.

С обзиром да не постоји централни регистар – не постоји репозиторијум свих луковичастих (онијон) сајтова, нема могућности да сви буду познати једном кориснику. О многима од њих мора се добити информација од других ТОР корисника, како би им се приступило. Наравно ипак на мрежи постоји неколико места са којих се може започети пут у дарк и дип нет. Њих је наравно неопходно отворити путем ТОР браузера:

https://dark.fail/
https://thehiddenwiki.org/
http://wikileaks.org
https://www.reddit.com/r/TOR/comments/8zofda/how_to_use_tor_safely/

Генерално на интернету постоје туторијали, а посебно на даркнету о томе како корисници треба да конфигуришу своје системи како треба да користе различита оруђа и софтвере како не би били ухваћени или препознати од оних који надзиру комуникације. Један од веома еклатантних примера је сајт „дечје порнографије“ (за размену ЦСАМ односно материјала којима се искоришћавају малолетна лица у порнографске сврхе) хард кенди („hard candy“) који предлаже да се пре прикључивања на мрежу провери или обезбеди да:

- Браузер не одаје информације – да је подешен на такве активности којима прикрива податке о кориснику
- Да ће на сајту наићи на дискусије које укључују разматрање секса са малолетним лицима млађим од 18 година, као и да ће се наилазити на материјале који подразумевају обнажене фотографије и видео записе овакве садржине који су легални за дистрибуцију, према прописима САД.
- Корисници не дозволе да им излети било који податак док сте анонимни о свом идентитету, односно да не дозволе повезивање сопственог и псеудонимног идентитета. Начини остваривања – цурења информација о идентитету су излистани на линку понуђеном код једног од наведених појмова, уз упозорење да се овакво одавање информација може више компромитовати кориснике од цурења информација кроз браузер, а да се то може догодити да корисник и не буде у потпуности свестан да се исто десило.
- Корисници треба да буду свесни да одређени сајтови користе јава скрипте (*java script*) и неки ТОР релеји и да у одређеним ситуацијама овакве инјектују увезане јава скрипте како би пратили кориснике који су им приступили. Генерално, добра пракса јесте да се искључе сви облици скриптовања приликом сурфовања интернетом и да се искључе колачићи (*cookies*), као и да се искључе сви ифрејмови (*iframes*) и непотребни прикључци (*plugins*) на браузерима.

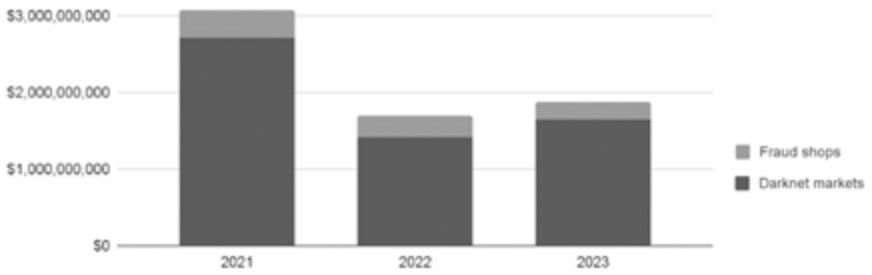
- Уколико корисници имају идеју да сопствене материјале постављају на сајтове, да свим материјалима скину метаподатке који би их могли компромитовати. Многе дигиталне камере остављају податке на дигиталним фотографијама о камери, локацији и сличним подацима који могу указати на идентитет, а многи рачунарски програми такође похрањују метаподатке о систему коришћеном приликом израде дигиталне датотеке и кориснику, локацији и слично, о чему посебно треба водити рачуна.

ТОР ИП адресе могуће је анализирати и утврдити која је функција којих ТОР чворова на више различитих сајтова:
- https://circleid.com/posts/20201129-a-look-into-tor-nodes-locations-and-isps-with-ip-intelligence/
- https://metrics.torproject.org/
- https://support.heimdalsecurity.com/hc/en-us/articles/360006539077-TOR-node-list

ТОР коло (као остварена веза путем ТОР браузера – преко чворова који са директним приступом крајњем сајту излазном чвору) траје по правилу неких 10 минута, односно у случајевима када коло функционише како треба а уколико то изостане, прави се ново коло и раније.

Начини на које се може супротставити анонимизирајућим техникама су разноврсни и могу се сублимирати у следеће:
- Прављење профила извршилаца кроз анализирање шаблона које они користе
- Тражење грешака у коришћењу анонимизирајућих оруђа и техника
- Путем коришћења историјских база података
- Наредбе за тајни надзор комуникације којима се фокусира на ИП шаблоне којом приликом се идентификују они који немају везе са инкриминисаним активностима и конкретизују налози са којих је инкриминисани саобраћај остваривaн
- Претраживати активности које нису криминалне, а притом није коришћена анонимизација

Профилисање обухвата утврђивање додатних података и информација: имејл адреса, других вебсајтова – конкретних интересовања мете, анализу флуентности енглеског језика или другог језика који је корисник користио, анализа колоквијализама коришћених од стране корисника, као и интересовања у виду спорта, кладионица, географији, политици и сл.



Слика бр. 16. Годишњи приход на даркнет тржишту 2021/2023 (Извор: https://www.chainalysis.com/wp-content/uploads/2024/03/darknet-market-and-fraud-shop-revenue-1200x753.png)

Идентификација грешака обухвата ситуације у којима корисници не користе проксије (веома ретке, али могуће) ове ситуације су веома корисне за анализу идентитета особе, ситуације у којима корисници користи онемогућавање проксија за „легалне" активности, неки сајтови одбијају приступ корисницима који користе проксије или TOP чворове (или нодове) као нпр. Microsoft live. У овом смислу класично ОСИНТ претраживање може дати значајне резултате – претрага у било ком интернет претраживачу google, bing, yahoo, duckduckgo може дати изузетне резултате – у вези имена презимена, имејл адресе или других сајтова, а посебно претраге социјалних мрежа за корисничким именима и имејл налога коришћених за ове или претраге самих имејл налога који се користе са којим корисничким именима.

Наредбе везане за тајни надзор комуникације већином случајева обухватају откривање и анализу података о: другим имејл налозима које одређено лице користи, другим сајтовима који интересују лице од интереса, такође и друга лица од значаја за конкретну истрагу или друге истраге. Анализа ИП логова о комуникацији – може открити ситуацију у којој можда нису коришћени проксији када су се регистровали, идентификацију инстанци када проксији нису коришћени и у циљу претрага шаблона путовања (подаци о хотелима које је извршилац користио).

Остале активности на које се наилази на TOP мрежи су:

- Наркотици, нове психоактивне суппстанце,
- Мејлови
- Четови
- Порнографија
- Хаковање
- Крековање шифара
- Украдене платне картице и подаци о њима
- Фишинг.

3. E-Banking

Једна од првих дефиниција *E bankinga* дала је компанија *IBM*[17]: „*E banking* је трансформација кључних пословних процеса употребом интернет технологија". Поред трансформације кључних пословних процеса, дошло је и до трансформације средстава која учествују у трансакцијама.[18]

3.1. Електронски новац

Дигитална валута је свака валута, новац или имовина налик новцу којом се првенствено управља, чува или размењује на дигиталним рачунарским системима, посебно преко интернета. Врсте дигиталних валута укључују криптовалуте, виртуелну валуту и дигиталну валуту централне банке.[19]

Криптовалута (*cryptocurrency, crypto-currency, crypto*) је дигитална валута дизајнирана да ради као средство размене преко рачунарске мреже која се не ослања ни на један централни орган, као што је влада или банка, који би је одржавао или одржавао.[20]

Виртуелна валута, или виртуелни новац, (*Virtual currency, virtual money)* је дигитална валута која је углавном нерегулисана и коју издају и контролишу њени програмери и која се користи електронски међу члановима одређене виртуелне заједнице.[21]

Дигитална валута централне банке (ЦБДЦ) (која се назива и дигитална фиат валута[22] или дигитални основни новац)[23] је дигитална валута коју издаје централна, а не комерцијална банка.[24]

---

[17] https://www.ibm.com/ibm/history/ibm100/us/en/icons/ebusiness/transform/ последњи пут приступљено 10.07.2022.

[18] Zirojević Mina, Ivanović Zvonimir Cyber law – Serbia, Institut za uporedno pravo, 2022.

[19] Al-Laham, Mohamad; Al-Tarawneh, Haroon; Abdallat, Najwan (2009). „Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy" (PDF). *Issues in Informing Science and Information Technology*. 6: 339–349. последњи пут приступљено 12.05.2021.

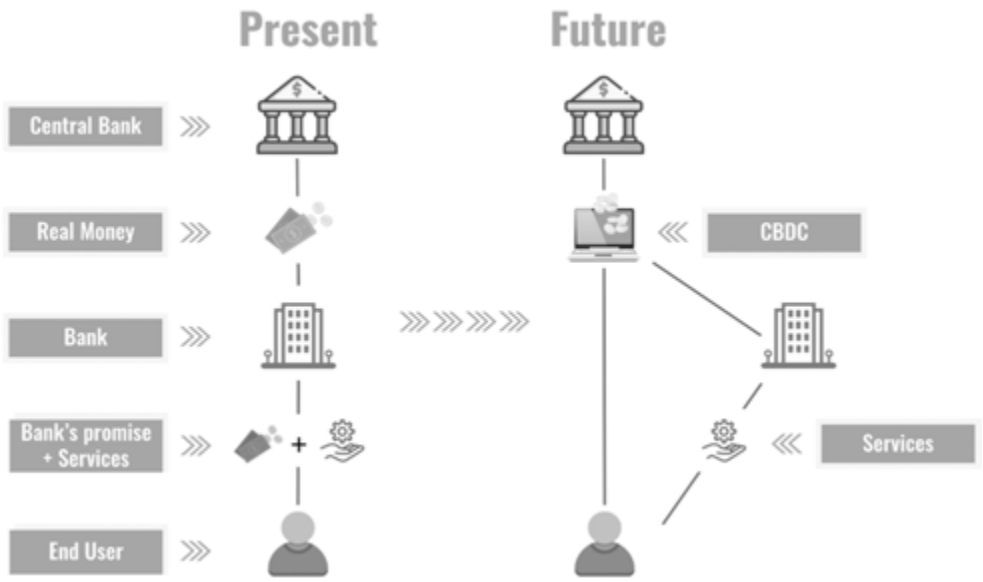
[20] Milutinović, Monia (2018). „Cryptocurrency". *Ekonomika*. 64 (1): 105–122.

[21] European Central Bank (October 2012). „1". *Virtual Currency Schemes* (PDF). Frankfurt am Main: European Central Bank. p. 5. . последњи пут приступљено 19 June 2021.

[22] Focus Group on Digital Currency including Digital Fiat Currency". *ITU*. http://www.itu.int/en/ITU-T/focusgroups/dfc/Pages/default.aspx. последњи пут приступљено 19 June 2021.

[23] Mersch, Yves (16 January 2017). *Digital Base Money: an assessment from the ECB's perspective* (Speech). Farewell ceremony for Pentti Hakkarainen, Deputy Governor of Suomen Pankki – Finlands Bank. Helsinki: European Central Bank. последњи пут приступљено 19.06.2021.

[24] Davoodalhosseini, M., Rivadeneyra, F., & Zhu, Y. (2020). CBDC and monetary policy (No. 2020-4). Bank of Canada. https://www.banqueducanada.ca/2020/02/note-analytique-personnel-2020-4/. последњи пут приступљено 12 May 2022.



Слика бр. 17. ЦБДЦ у односу на конвенционалну валуту (Извор: https://coinloan.io/blog/guide-to-central-bank-digital-currency-cbdc/)

Развојем информационе и телекомуникационе технологије створени су услови за глобализацију пословања. Развој Интернета и умрежавање појединаца, компанија и јавне управе воде до значајних промена у начину и ефикасности пословних система.

Савремено пословање поставило је као императив повезивање клијената и протока информација на начин да то буде што је брже могуће и ефикасније, без обзира на географску удаљеност. Са развојем електронског преноса средстава финансијски инструменти и пословне технологије су се значајно променили. Финансијске трансакције у реалном времену се преносе неограничено на даљину преко постојећих интернет комуникационих мрежа, без традиционалне припреме налога и пратеће документације. Електронско банкарство, безготовинско плаћање и модерно пословање на берзи су сегменти који су се од класичног начина рада и пословне сарадње трансформисали у електронско пословање и дигиталну економију.

Утицај интернета на банкарство огледа се кроз електронско банкарство, кућно банкарство, мобилно банкарство, банкомати и ПОС терминали. Електронско банкарство односи се на услуге које банке пружају својим клијентима - пословним субјектима, првенствено на пољу домаћег и страног платног промета. На даљи развој електронског банкарства утиче комбинација раста употребе Интернета и *online* технологија са трендовима економске глобализације и концентрације финансијских услуга.

Ови „нови“ облици пословања нису остали имуни на продор криминалних понашања у њихове структуре. И не само то, појавили су се нови облици и актери тог криминалног деловања у дигиталном свету. Средства која користе су нужно везана за интернет као највећу глобалну мрежу, што значи да морају бити „повезани на мрежу“.

3.2. Превара

Заштитни објект кривичног дела преваре јесте имовина у целини, а не само неки њени облици (као на пример, покретна ствар код крађе и утаје). Радња извршења основног облика састоји се у навођењу (у намери прибављања противправне имовинске користи) неког лица да учини или не учини на штету своје или туђе имовине. То значи да се радњом извршења не проузрокује непосредна штета на имовину, већ се пасивни субјект наводи да он сам, чињењем или не чињењем, то учини са својој или туђој имовини. Навођење се врши на два начина: довођењем у заблуду лица лажним приказивањем или прикривањем чињеница или одржавањем у заблуди на исти начин. Довођење у заблуду представља стварање погрешне слике о неким чињеницама, тако што се постојећа чињеница лажно приказују као другачија него што стварно јесте или тако што се прикрива постојање неке чињенице. Заблуда је погрешна представа о чињеницама, што значи да постоји таква представа о некој чињеници која не одговара стварности. Само одсуство представе о истинитој чињеници није довољно за постојање заблуде.[25]

Главна карактеристика преваре јесте довођење друге стране у заблуду ради прибављања незаконите имовинске користи. Она се у основи своди или на лажно изношење чињеница или на њихово прикривање.

Кривични законик Републике Србије предвиђа основни облик преваре који подразумева постојање намере за остваривање противправне имовинске користи која настаје као последица нанесене штете на имовини пасивног субјеката или туђој имовини уз обавезно навођене на ту радњу у виду довођења у заблуду. Поред овог основног КЗ предвиђа још три облика, један лакши и два тежа. Лакши облик представља изостанак намере за противправном имовинском коришћу и постојање намере да се субјекат оштети. Два тежа облика се огледају у новчаној вредности нанесене штете, први тежи облик се јавља када је нанесена материјална штета већа од четиристопедесет хиљада динара, док се други тежи облик јавља у случају када је нанешена материјална штета већа од милион и петсто хиљада динара.

[25] Стојановић З., Делић Н., (2013): *Кривично право посебни део,* Правни факултет универзитета у Београду, стр. 152.

Исти закон прописује превару у обављању привредне делатности (чл.223 КЗ РС), и каже ко у обављању привредне делатности, у намери да себи или другом прибави противправну имовинску корист, доведе кога лажним приказивањем или прикривањем чињеница у заблуду или га одржава у заблуди и тиме га наведе да нешто учини или не учини на штету имовине субјекта привредног пословања за које или у којем ради или другог правног лица. [26]

Из дефиниције овог кривичног дела закључује се да свако може бити учинилац овог кривичног дела. Међутим, то свако има један услов која се огледа „у обављању привредне делатности". Ово је у суштини кривично дело против привреде које као начин извршења има преварну радњу.

Разликујемо и финансијску превару као подгрупу из области привредних превара. Финансијска превара јесте намерно, промишљено, нетачно тврђење или изостављање материјалних исказа или рачуноводствених података, који посматрано са осталим информацијама у целини, наводе на то да читалац промени или преуреди своју процену или одлуку.[27] Могу их извршавати различита лица, у различитим одељењима у предузећу, у различитим привредним секторима и могу се установити у предузећима различите величине.

У Међународним стандардима ревизије финансијска превара се дефинише као намерна активност једног или више руководилаца, лица овлашћених за управљање, запослених или трећих страна, која укључује обмањивање ради стицања неприпадајуће или незаконите добити. Амерички институт овлашћених јавних рачуновођа (*AICPA*) наводи две основне категорије финансијских превара: намерно погрешно приказивање финансијских информација и неоправдано присвајање имовине (или крађа)[28]

Online преваром се сматра облик преваре који се врши помоћу рачунара, рачунарских система и межа. Превара је саставни део радњи које се врше у дигиталном свету, са циљем да се неко лице наведе да нешто учини или не учини на штету своје или туђе имовине. Превара и финансијски криминал прилагођавају се догађајима у доменима у којима делују. Појавом дигитализације и аутоматизације у финансијским системима, ови злочини су постали електронски софистицираније и безлични (За поглед

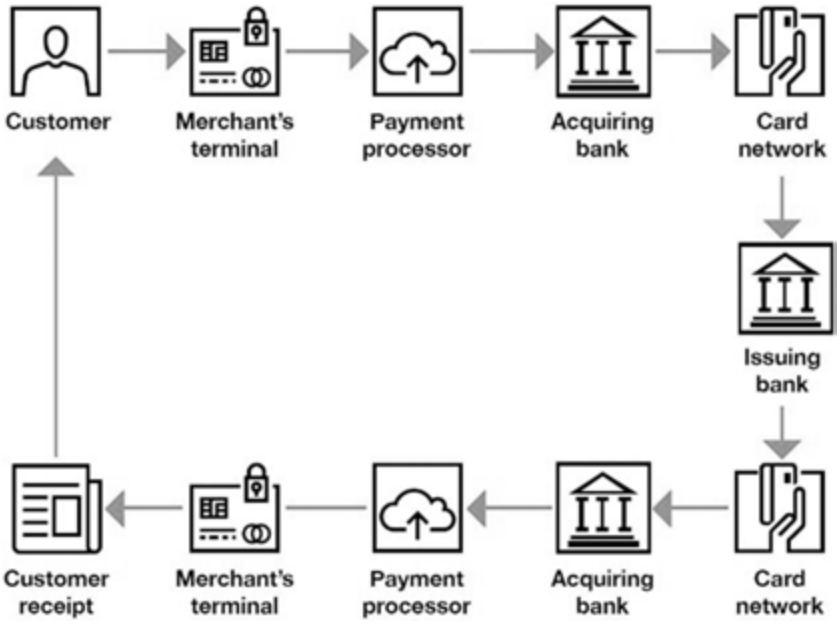
[26] Кривични Законик, *Службени гласник РС,* бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

[27] Rezaee Z., Riley R., (2009); *Financial Statement Fraud: Prevention and Detection,* John Wiley & Sons Publishing, New Jersey, стр. 5.

[28] Сергар Т., Врањеш С., (2013); *Откривање и спречавање финансијских превара у циљу јачања финансијских перформанси предузећа у Републици Српској,* Acta Economica, број 19, стр. 185.

како ради плаћање кредитном картицом види слику 18.). То значи да се преварном радњом не чини директна штета на одређену имовину, већ се пасивни субјекат наводи да својим чињењем или не чињењем доведе до штете на својој или туђој имовини.

Извршиоци се служе погодностима које им пружа интернет, скоро потпуну, анонимност, као и чињеницом да је дигиталне финансијске токове, који обично воде преко више држава, веома тешко пратити и утврдити крајњу дестинацију средстава.[29]

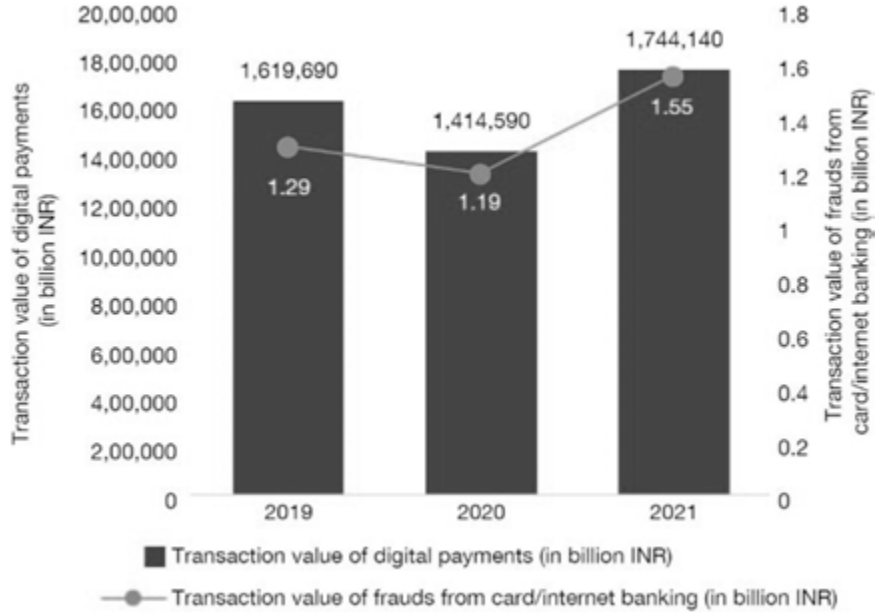


Слика бр. 18. Процесни круг плаћања кредитном картицом (Извор: Стабилна интерент адреса https://www.pwc.in/industries/financial-services/fintech/dp/combating-fraud-in-the-era-of-digital-payments.html)

У Великој Британији губици од финансијских превара на платним картицама, е - банкарства и чекова износили су 844,8 милиона фунти у 2018. години, што је пораст од 16 процената у односу на 2017. Године 2018. су спречене преваре у вредности од 1,66 милијарди фунти. То је еквивалентно односу у коме је на сваки покушај преваре у вредности од 3 фунте, спречено деловање у вредности од 2 фунте.[30]

[29] Урошевић В., Ивановић З., Уљанов С., (2012), *Mač u world wide web-u, izazovi visokotehnološkog kriminala,* Enternal mix, Београд, стр. 94.

[30] https://www.paccsresearch.org.uk/wp-content/uploads/2019/06/WEIS_2019_paper_25.pdf последњи пут приступљено 05.08.2022.



Слика бр. 19. Вредност превара у односу на трансакције дигиталног плаћања (картице и интернет банкарство)
(Извор: https://www.pwc.in/industries/financial-services/fintech/dp/combating-fraud-in-the-era-of-digital-payments.html)

У земљама где су преваре и финансијски криминали широко распрострањени, грађани често морају да плаћају мито за јавне услуге, по неким проценама један од четири појединца у глобалу учествује у таквим радњама. Иако је ово искуство на појединачном нивоу, то често може да се одрази на виши ниво, унутар влада и организација приватног сектора. Вреди напоменути да они који су умешани у превару и финансијски криминал не морају увек бити „лоши људи" у конвенционалном смислу. У случају преваре, недостатак знања, укорењени обичај и пракса или одсуство потребних оквира управљања може резултирати да људи несвесно злоупотребе или буду злоупотребљени.[31]

Подмићивање, корупција, проневера и прање новца спадају у међународне оквире непоштовања закона. Конвенција Уједињених нација против корупције (UNCAC)[32] и Радна група за финансијске акције (FATF)[33]

[31] https://www.iksi.ac.rs/izdanja/finansijski_kriminalitet_2018.pdf; приступљено 06.08.2022.

[32] https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf пут приступљено 05.10.2022.

[33] https://www.fatf-gafi.org/ последњи пут приступљено 20.10.2022.год.

две су примарне, међународне институције која постављају стандарде за борбу против преваре и финансијског криминала. Иако су на снази друге антикорупцијске конвенције, већина их је углавном ограничена на одређене регионе или уске манифестације корупције.

Лоше ствари на Интернету најчешће погађају обичне грађане када се на извештају њихове кредитне картице или извештају из банке појави наплата коју нису одобрили, па су преваре у *online* плаћању саставни део свеукупног криминала усмереног према имовини на мрежи.

Земље на светском економском форуму су приметиле да су превара и финансијски криминал индустрија од милијарду долара, пријављујући да су приватне компаније потрошиле око 8,2 милијарде долара на *Anti Money Laundering* (*AML*) контролу само у 2017, а 60 % *online* превара се извршава преко мобилних платформи[34]. Злоупотребе у привреди, откривене и неоткривене, постале су многобројније и скупље него икад.

3.3. Дела привредног криминала кроз дигиталну призму

Привредни криминал се као и остатак света прилагођава новонасталим приликама у чијем домену делује. Појавом дигитализације и аутоматизације ови криминални деликти су постали софистицирани и безлични. Привредни криминал у дигиталном добу представља неке посебне нове изазове за законодавство и целокупно друштво. Анонимност, приступачност и одговорност (законодавствена) су најважније „нове" карактеристике привредног криминала.

Анонимност се огледа у томе да криминалци могу прикрити свој идентитет и активности, отварање простора у коме могу досегнути потенцијалне жртве као никада раније. Наше кривично процесно право традиционално, попут већине других држава у континенталној Европи, користи термин оштећени. Оштећени је физичко или правно лице чије је неко лично или имовинско право извршењем кривичног дела повређено или угрожено. То је веома широка дефиниција, која је знатно шира од уобичајеног појма жртве у криминолошком и делом кривичноправном смислу, односно пасивног субјекта у смислу кривичног материјалног права.[35]

Многе криптовалуте пружају сигурност корисницима својом псеудо-анонимношћу дефинисану дизајном и стварају нову методу за олакшавање плаћања, стварајући нове изазове за креаторе политике, регулаторе,

[34] https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/; приступљено 05.08.2022.

[35] Шкулић М., (2015); *Нормативна анализа: Положај жртве кривичног дела/оштећеног кривичним делом у кривичноправном систему Србије,* Правни факултет, Београд, стр. 2.

стручњаке за ревизију који раде на решавању активности попут прања новца.

Приступачност као карактеристика је довела да је привредни криминал постао приступачнији захваљујући ширењу информација на Интернету, технолошкој револуцији која је омогућила лакоћу комуникације и трансфер новца који прелази међународне границе без да се захтева физичка присутност лица.

Одговорност законодавног тела подразумева да се можда по први пут икада мора постићи права регулаторна равнотежа између људског надзора и ослањања на машину. Другим речима, све је већа потреба света за законским решењима и механизмима који би подржали технолошки напредак у привредном пословању, са једне стране, и омогућила сигурно и несметано дигитално пословање, са друге стране.

У Републици Србији нема доступних информација које говоре о заступљености *online* прања новца, али тренд вршења кривичних дела против привреде помоћу дигиталних технологија је присутан, у прилог томе говоре подаци из следеће табеле.

Табела 3. Представља број кривичних дела против привреде из области високотехнолошког криминала у Републици Србији.

Година	Укупан бр. дела ВТК	Кривична дела против привреде	
		Неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга	Фалсификовање и злоупотреба платних картица
2018	664	219	124
2019	780	232	336

Извор: МУП Републике Србије

Подаци изнесени у табели 3. потврђују заступљеност кривичних дела против привреде у дигиталном простору на територији Републике Србије. У 2018, години укупан број кривичних дела из области високотехнолошког криминала био је 664, а од тога 343 кривична дела против привреде, што износи 51% од укупног броја. У 2019. години укупан број кривичних дела из области високотехнолошког криминала износио је 780, а од тога 568 кривичних дела против привреде, што износи ипозантних 72% од укупног броја. Скоро троструко повећање кривичних дела фалсификовања и злоупотреба платних картица допринело је овом расту кривичних дела против привреде од 21%.

У великом броју финансијских злочина које олакшава интернет, прање новца добија на значају због своје величине и различитих метода које се користе на мрежи за трансформацију нелегално стеченог новца у легалне токове. Кривична пракса прања новца која је извршена у *cyber* простору путем *online* трансакција означена је као *cyber* прање. Перачи новца стално трагају за новим начинима у циљу избегавања законске санкције, а Интернет је отворио велики простор могућности за њих.

Организација за контролу и спречавање прања новца (*Financial Action Task Force – FATF)* је међудржавно тело које има за циљ да развија и унапређује мере у борбу против прања новца и финансирања тероризма на националном и међународном нивоу. *FATF* такође прати напредак који државе чланице постижу у имплементацији ових мера, анализира типологије прања новца и финансирања тероризма, и промовише усвајање и имплементацију одговарајућих препорука на глобалном нивоу. У овим активностима *FATF* сарађује са осталим међународним телима за борбу против прања новца и финансирања тероризма[36]. Оно по чему је *FATF* препознатљив јесу његове препоруке[37] земљама чланицама о конкретним корацима које треба предузети како би се и превентивно и репресивно деловало на појаве прања новца и финансирања тероризма.

Међународна организација која се бави тематиком прања новца у азијско – пацифичкој регији наводи да прање новца у западном свету није ништа ново, те да се тај тренд шири на источни свет. Ова организација у свом годишњем извештају из 2018. године наводи да се посебан фокус прави на прање новца путем Интернета, и додаје да *cyber* превара представља преовлађујућу претњу у азијско – пацифичком региону са повећањем од 35% у поређењу са 2017. годином.[38]

Када говоримо о превари у дигиталном простору, најчешће мислимо о одређеној радњи која претходи самом прању новца, тј. можемо је и назвати припремном радњом у којој се одређено лице доводи у заблуду, која претходи кривичном делу прања новца, радња у којој се од оштећеног лица које је доведено у заблуду на преваран начин прибављају ресурси потребни за извршење кривичног дела прања новца (нпр. лични подаци).

---

[36] Савет Европе, (2016); *Истраīа и īроцесуирање кривичних дела коруīиције идентификованих кроз ревизорске извештаје,* практикум за припаднике правосуђа и полиције, Београд, стр. 9.

[37] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html; приступљено 03.10.2022.

[38] APG Yearly Typologies Report (2018); *Methods and Trends of Money Laundering and Terrorism Financing;* APG Secretariat, New South Wales.

Поред довођења у заблуду превара омогућава извршиоцима да избегну откривање и санкцију од стране надлежних органа.

Овде се може приказати једна пригодна типологија преварног понашања у дигиталном свету које за свој финални циљ имају остварење деликата против привреде:

3.4. Злоупотреба друштвених мрежа

Преваранти користе платформе друштвених мрежа попут *Facebooka* како би упутили средства јавних депозита на своје банковне рачуне. У једном случају, преступник је под окриљем радикалне идеологије инспирисао истомишљенике (корисника друштвених мрежа) да му уплате новац. Други пример, преступник, представљајући се као владин службеник, намамљује људе, пасивне субјекте кривичног дела, тако што им обећава непостојећу финансијску помоћи од владе и тера их да депонују део обећаног износа унапред као обезбеђење. Овако добијен (прљав) новац се најчешће у кратком временском периоду повуче или буде прослеђен на друге банковне рачуне.

Анализом ових типологија можемо закључити да је присутно кривично дело лажног представљања које не спада у кривична дела против привреде, али ако би починиоци ових дела била лица са одређеним службеним положајем и носиоци одређених овлашћења јасно је да би се радило о кривичном делу злоупотреба службеног положаја. У немалом броју случајева присутном у различитим регионима (Јужна Азија, Северна Америка) извршиоци и јесу били припадници државних органа, државни службеници и сл.

Анализом података МУП-а закључујемо да су пријаве за кривично дело злоупотреба службеног положаја најзаступљеније у Републици Србији када говоримо о кривичним делима против привреде (графикон 1). У периоду од 2006 – 2015 најмањи број пријава забележен је 2014. године а највећи 2010. Кривично дело Злоупотреба службеног положаја чини 18,1% од укупног броја пријављених кривичних дела привредног криминалитета у 2006. години, 20,7% у 2007. години, 26,3% у 2008. години, 23,7% у 2009. години, 26,6% у 2010. години, 26,4% у 2011. години, 26 % у 2012. години, 17,1% у 2013. години, 9,1% у 2014. години и 10 % у 2015. години, дакле 20,4 % у просеку за поменути период (графикон 1). Из ових података видимо да ово кривично дело заузима једну петину свих дела против привреде у Републици Србији и ако томе додамо експоненцијални раст превара у дигиталном свету, јасно је да симбиоза ова два кривична дела у дигиталном свету представљају модеран и деструктиван напад на појединца и државу.

Графикон бр. 1. (Извор: МУП Републике Србије)

3.5. Online крађа идентитета

Овде преступници користе име или идентитет жртве да би извршили кривична дела. Подаци о идентификацији особе, укључујући име, национални идентификациони број, финансијске информације (број рачуна и ПИН)[39], добијају се разним методама као што је крађа идентитета путем електронских медија, телефона или платформе за инстант поруке. Информације се затим користе за различите криминалне радње, прекршаје, укључујући преваре са кредитним или АТМ картицама и неовлашћене трансфере помоћу интернет банкарства. Украдени идентитет омогућава криминалцима да извршавају нелегалне радње под легитимним идентитетом. Дигитализација, у којој изостаје моменат визуелно – физичке провере, омогућила је лакшу крађу идентитета али и проширила је могуће поље злоупотребе украдених идентитета. Једна од битних карактеристика *online* крађе идентитета је касно откривање од стране оштећеног који схвати шта се догодили тек након што се његови подаци искористе у сврху неких криминалних радњи. Жртва се сусреће са штетом која може бити директно у вези са њеним средствима, али када говоримо о привредним преступима, крађа идентитета подразумева коришћене података за различите трансфере који су саставни део прања новца. Ови подаци своју употребу проналазе и код *shell* компанија, где се украдени идентитет користи да би се обезбедио фиктивни власник компаније.

[39] У овом случају по нашем Законику (КЗ РС) у питању је кривично дело фалсификовања и злоупотребе платних картица из чл.243. КЗ РС.

3.6. Коцкање на мрежи

Постоје *online* платформе које олакшавају коцкање средствима укључујући покер, коцкарнице и спортско клађење. Многе азијске земље забрањују или ограничавају коцкање на мрежи. Међутим, неки криминалци зарађују путем ових опција и пребацују неовлашћени приход на банковне рачуне како би их учинили легитимним. Оваквим радњама се национални буџет ускраћује за средства која би по закону требала да се уплате на рачун државе и поред тога се та средства пребацују на различите банковне рачуне, чиме долази до прања новца.

У Републици Србији ову област уређује закон о играма на срећу у коме се наводи да приређивач плаћа накнаду за приређивање игара на срећу - клађење преко средстава електронске комуникације месечно у висини од 15% на основицу, а за остале посебне игре на срећу преко средстава електронске комуникације у висини од 10% на основицу, коју чини разлика између укупно остварених уплата и укупно остварених исплата, с тим што укупан износ накнаде не може бити мањи од динарске противвредности 10.000 евра месечно, обрачунате сразмерно броју дана до краја месеца од дана пријема решења о одобрењу.[40]

Поред дефинисане накнаде према држави законодавац је прописао одређене дужности приређивача како би се спречиле злоупотребе у омогућио континуирани надзор пословања.

Приређивач посебних игара на срећу преко средстава електронске комуникације дужан је да користи информационо-комуникациони систем за приређивање игара на срећу преко средстава електронске комуникације, који омогућава чување, архивирање и размену података електронским путем са софтверским решењем Управе (Управа за игре на срећу) у сврху вршења надзора.[41]

3.7. Међународна дигитална превара

То је тренд криминала започет почетком 2012. године када су криминалци хаковали *e-mail* како би банкама жртава послали лажна упутства за пренос средстава на банковне рачуне у другој земљи. У неким случајевима су жртве извршавале пренос средстава по налогу криминалца тако што су биле доведене у заблуду. Сингапур је био једно од истакнутих *off-shore* локација за депоновање таквих криминалних прихода. Банковне рачуне у Сингапуру поседује локално становништво које се спријатељило са члановима

[40] Закон о играма на срећу, *Службени гласник РС*, бр. 18/2020.

[41] Закон о играма на срећу, *Службени гласник РС*, бр. 18/2020.

криминалних синдиката, углавном путем друштвених мрежа. Ови локални власници банковних рачуна познатији и као *money mules,* на захтев криминалног синдиката, сложили су се да примају новац на свој рачун и након тога средства пренесу на друго место, обично на банковне рачуне у иностранству.[42] *Money mules* обично добијају провизију за своје услуге.

У овом облику преваре примећујемо да она претходи отуђивању средстава од жртве и прању новца које врши треће лице (*money mules* – муле за пренос новца). Обједињавањем трансакцијских података из више финансијских институција и извршавањем софистицираних алгоритама могу се идентификовати такозвани *mules accounts*, рачуни у банкама за фантомско преношење новца који се користе за прање новца и друге илегалне активности.[43] Многи од ових рачуна нису директно успостављени од стране криминалаца, већ путем бројних превара, укључујући крађу идентитета кроз *e-mail* или, као што је већ наведено, помоћу трећих лица који нису директни извршиоци.

3.8. Привредна друштва – мете online привредног криминала

Привредна друштва као важни привредни субјекти су честа мета *cyber* нападача. Јасно је да су напади на веће привредне субјекте чешћи и наносе већу материјалну штету која поред непосредно отуђених средстава подразумева и средства која су у том периоду изгубљена (ако привредно друштво није имало могућност пословања због штете нанесене нападом), као и средства која су утрошена на санирање штете.

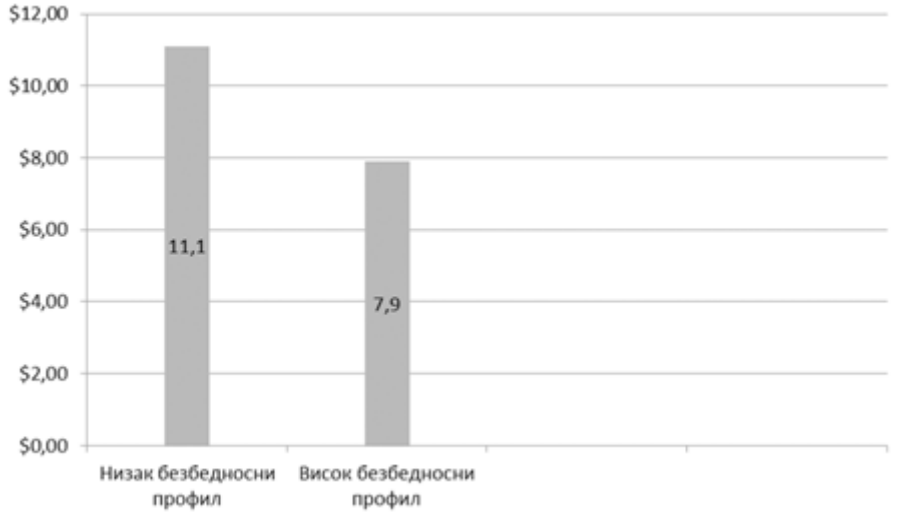
Због лакшег разумевања предстојећег текста, користиће се термин компанија као синоним термину привредно друштво. На узорку од 237 различитих компанија широм света утврђено је да укупни годишњи трошкови везани за *cyber* криминала у 2016. години крећу се од најнижих 0,27 милиона до највиших 74 милиона долара. Средња вредност трошкова је 9,5 милиона долара, док је средња вредност 2015. године износила 7,7 милиона доларана. Укупно 81 компанија представљена у овој студији имала је укупне трошкове изнад просечне вредности од 9,5 милиона долара, а 156 компанија је имало годишњи укупан трошак *cyber* криминала испод средње вредности.[44]

---

[42] https://www.ncpc.org.sg/downloads/mediarelease/22-Nov-2013_Media_Release_on_Money_Mules.pdf; приступљено 23.7.2020.

[43] https://risk.lexisnexis.com/global/en/insights-resources/case-study/financial-institution-uplift-detection-money-mule-accounts; приступљено 23.7.2020.

[44] https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf; приступљено 26.08.2020.



Графикон бр. 2. У ову студију су укључена предузећа чија величина варира о најмање 673 до преко 129.000 запослених који своју делатност обављају на мрежи, са просеком од 9740 запослених по компанији. (Извор: https://www.ponemon.org)

На графикону 2 је приказан однос трошкова које имају компаније са ниским и високим безбедносним системима усмереним против *cyber* криминала.

Налази ове студије су такође показали да висок безбедности профил смањује трошкове *cyber* криминала за компаније. Организације са високим безбедносним профилом доживеле су просечан трошак од стране *cyber* криминала од 7,9 милиона долара, што је испод просека. Насупрот томе, организације са ниским безбедносним профилом имају просечни трошак од 11,1 милион долара. Ови безбедносни профили зависе од броја сигурносних мера и алата које компаније имплеметирају у пословање.

По најновијим истраживањима из 2020. године, *cyber* безбедност у оквиру компанија напредује, у ствари, више од четири од пет испитаника сложило се да су алати за *cyber* безбедност значајно напредовали током последњих неколико година и приметно побољшавају *cyber* отпорност своје компаније. Побољшања у основној безбедносној култури поткрепљују овај налаз. Могућност тачне процене броја *cyber* напада на компанију зависи од њене способности да их открије. С друге стране, нарушавање дигиталне безбедности јесте стварни догађај и вероватно ће бити прецизније забележен. Имајући ово на уму, тимови за *cyber* безбедност из различитих индустрија и географских подручја заслужују признање за побољшани ниво заштите током прошле године (2019). На пример, укупан број *cyber* напада на компаније опао је за 11

проценатa. У просеку, организације се сада суочавају са 22 *online* безбедносна пропуста годишње у поређењу са 30 у претходној години.[45]

3.9. Пореска утаја кроз криптовалуте

Обавеза плаћања пореза и других дажбина предвиђена је Уставом Републике Србије.[46] Плаћање пореза има изузетан значај за сваку државу и њену привреду, због тога државе намећу порезе и дажбине економским обвезницима. Када говоримо о криптовалутама, оне не подлежу опорезивању у нашем законодавству. Због могућности улагања и употребе криптовалута, на глобалном нивоу се све више потеже питање њиховог опорезивања.

У вези с тим, изазов је како категоризирати криптовалуте и посебне активности које их укључују у функцију опорезивања. Ово је првенствено важно због тога да ли се добитак од *Mining* – а или продаје криптовалута категоризира као приход или капитални добитак, што даље одређује одговарајући порески оквир.

Министарство финансија се огласило о пореском аспекту криптовалута, односно *Bitcoina*. У Билтену Министарство финансија даје одговор на питање да ли се на промет дигиталне валуте *Bitcoin* може применити одредба Закона о порезу на додату вредност. Закона прописује: „ПДВ се не плаћа у промету новца и капитала, у случају: пословања и посредовање у пословању по закону, осим за папир и кованице који се не користе као законско средство плаћања или имају нумизматичку вредност".[47]

Министарство је одговорило да се ПДВ не плаћа у промету новца и капитала, и то код пословања и посредовања у пословању законским средствима плаћања, осим папирног и кованог новца који се не користи као законско средство плаћања или има нумизматичку вредност. С тим у вези, а с обзиром да *Bitcoin,* дигитална валута не представља законско средство плаћања у Републици Србији у складу са позитивним прописима, мишљења смо да се на промет *Bitcoin* дигиталне валуте не може применити одредба члана 25. Став 1. Тачка 1) Закона, којом је прописано пореско ослобођење без права на одбитак претходног пореза код пословања и посредовања у пословању законским средствима плаћања.[48]

---

[45] https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf приступљено 01.09.2020.

[46] Устав Републике Србије, *Службени ɪласник РС*, бр. 98/2006, чл. 91.

[47] Закона о порезу на додату вредност члана 25. Став 1. Тачка 1) (*Службени ɪласник РС*, бр. 84/04, 86/04, 61/05 и 61/07).

[48] Министарство финансија Републике Србије (2017); билтен бр. 11; службена објашњења и стручна мишљења за примену финансијских прописа, Београд, стр. 39.

Врховни управни суд Шведске је упутио питања Европском суду правде у вези са Директивом ЕУ о ПДВ – у. Суд је донео одлуку да заједничку директиву о порезу на додату вредност треба тумачити тако да се трансакције, попут оних у главном поступку, које се састоје од замене традиционалних валута јединицама виртуелне валуте *Bitcoin* и обрнуто, обављају плаћањем износа који одговара маржи. С једне стране, цена по којој дотични оператер купује валуту и, с друге стране, цена по којој је продаје својим купцима, чине пружање услуга уз накнаду у смислу те одредбе.

Директиву треба тумачити тако да испоруке услуга, попут оних о којима је реч у главном поступку, састоје се од замене традиционалних валута јединицама виртуелне валуте *Bitcoin* – а и обрнуто, вршећи се плаћањем марже по коме дотични оператер купује валуту и, с друге стране, цена по којој је продаје својим купцима, представљају трансакције ослобођене пореза на додату вредност у смислу те одредбе.[49]

Неке земље су различито категоризирале криптовалуте у пореске сврхе, нпр:

- Израел - опорезоване као имовина
- Бугарска - опорезују се као финансијско средство
- Швајцарска - опорезују се као страна валута
- Аргентина и Шпанија - порез на доходак
- Данска - подложне порезу и губитци се одбијају
- Велика Британија: - корпорације плаћају порез на добит, некорпоративна предузећа плаћају порез на доходак, појединци плаћају порез на капиталну добит.

Углавном због одлуке Европског суда правде из 2015. године, добици од улагања у криптовалуте не подлежу порезу на додату вредност у државама чланицама Европске уније. У већини земаља које су обухваћене овим извештајем и које имају или су у процесу осмишљавања правила о опорезивању, *Mining* криптовалута је такође ослобођен од опорезивања. Међутим, у Русији се *Mining* који премашује одређени праг потрошње енергије опорезује.

У швајцарском кантону *Zug* и општини *Ticino* криптовалуте су прихваћене као средство плаћања чак и од стране владиних институција. *Isle of Man* и Мексико такође дозвољавају употребу криптовалута као начина плаћања заједно са својом националном валутом. Слично као владе широм света које финансирају разне пројекте продајом државних

[49] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=uriserv:OJ.C_.2015.414.01.0006.01.HRV&toc=OJ:C:2015:414:TOC; приступљено 10.09.2020.

обвезница, влада Антигве и Барбуде омогућава финансирање пројеката и добротворних организација путем *ICO*-а које подржава влада.[50]

Економска теорија разликује две врсте утаје пореза која може бити законита и неконита. Избегавање плаћања пореза може бити последица неинформисаност пореских обвезника о пореској обавези, нестручности и неефикасности пореских органа и недостатака у закону.

[50] https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf; приступљено 01.08.2020.

4. Прање новца

Појмовно се одређује као начин да се стечен новац добијен од криминалних и нелегалних радњи легализује. Прање новца често је праћено фалсификовањем финансијске документације и манипулације у систему међубанкарских трансакција.

Стање транзиције, кризе или рата је идеално поднебље за прање новца кроз трговину оружјем, трговину људима и проституцијом, коцкањем и сличним нелегалним делатностима.

Сам термин прање новца дефинисан је на различите начине и потиче из праксе. Најчешће се дефинише као процес којим неко прикрива илегално порекло и употребу новца и на тај начин тежи да га прикаже као легалан. Прање новца као термин има негативну конотацију и саставни је део привредног криминалитета.

Лица која теже да оперу новац превасходно имају за циљ да инвестирају што пре новац, да га на тај начин „прераде" и немају првенствено за циљ профит. Само убризгавање илегално стеченог новца не само што нарушава тржиште, већ може изазвати и веће економске нестабилности као што су нестабилност курса, камата и инфлације.

Перачима новца се сматрају „богаташи" који су нагло постали део високог финансијског сталежа. Процена Међународног монетарног фонда је ипак, да тзв. „бруто криминални производ" у свету износи више од 500 милијарди долара годишње, а по процени Уједињених нација чак 80% наведеног износа остварен је трговином наркотицима.[51]

Перачи новца не плаћају порез, али имају високе трошкове да илегално стечен новац „угурају" у легалне канале пословања

4.1. Фазе прања новца

Прање новца пролази кроз следеће фазе:

- полагање – новац остварен непосредно од криминалног деловања први пут се улаже или у финансијску установу или се њиме купује одређена имовина;
- прикривање – покушава се прикрити или наизглед променити стварно дело или власник средстава;
- интеграција – новац се укључује у легалну економију и финансијске токове.

[51] Опширније на: http://www.imf.org/

У фази улагања тежи се ка увођењу илегалног профита у легални финансијски ситем. Готовина прибављена криминалним пословима уплаћује се на банковне рачуне, обично под изговором неке регуларне делатности што представља фазу улагања.

Фаза прикривања настаје када је готовина претворена у банкарски депозит, следи фаза прикривања, која се остварује пребацивањем средстава с једног рачуна на рачуне разних банака у свету, привидних субјеката као и других финансијских институција, а све ради прикривања оригиналног извора и дестинације почетног криминалног капитала.

Фаза интеграције је последња фаза прања новца којом он поново улази у легалне економске токове је фаза интеграције. Новац се улаже у законите послове или инвестира, после чега се јавља као новац који потиче од законом дозвољене делатности. Популарни метод интеграције новца стеченог криминалом у легалне токове је куповина некретнина, као што су пословне зграде, складишта или станови.[52]

Прање новца се обавља полако и сукцесивно али се може десити да се поједине фазе међусобно преклапају. Јединствен циљ је следећи сакрити порекло и власника новца и што пре извршити легализацију.

Услед масовне појаве прања новца, како на националним нивоима тако и на интернационалним, многе европске и светске организације су реаговале и донеле строге прописе и казне за „перач новца".

Када говоримо прању новца у контексту привредног криминалитета у Србији он је заступљен, а нарочито у фазама рата. Почетак креирања система за борбу против прања новца у Србији везује се за доношење првог *Закона о спречавању прања новца.*

Прањем новца, у смислу закона, сматра се[53]:

- конверзија или пренос имовине стечене извршењем кривичног дела;
- прикривање или нетачно приказивање праве природе, порекла, места налажења, кретања, располагања, власништва или права у вези са имовином која је стечена извршењем кривичног дела;
- стицање, држање или коришћење имовине стечене извршењем кривичног дела

Осим одредби о прању новца, овај закон дефинише и обавезну идентификацију клијената код финансијских институција, пријављивање готовинских и сумњивих трансакција и друго.

---

[52] Стакић, Б., Бараћ, С. (2007): Међународне финансије, ФФМО, друго измењено и допуњено издање, Београд, стр. 354.

[53] Закон о спречавању прања новца и финансирање тероризма, *Службени гласник РС*, бр. 113/2017, 91/19.

4.2. Начин и фазе прања новца у криптовалутама

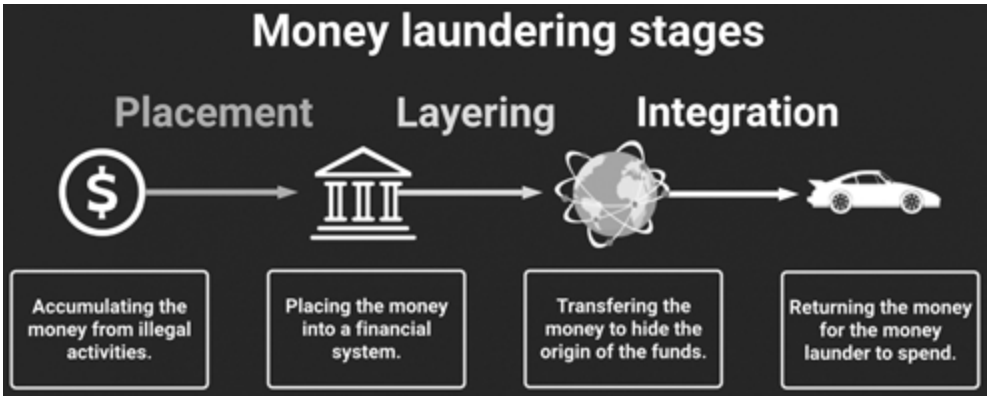
Прва фаза – полагање

У првој фази имплементације (полагања) потребно је прљав новац пренети у криптовалуте, за разлику од традиционалног уплаћивања депозита у банку где је количина готовинског новца једнака оној са којим се располаже на рачуну, са тим да упатилац има могућност избора коју ће криптовалуту купити (заменити готов новац за крипто) и чија се вредност разликује, нпр. један *Bitcoin* има вредност око 10.000 америчких долара, а *Litecoin* око 50 америчких долара. Постоји много начина за размену (куповину и продају) *Bitcoin*-а за готовину без употребе *Bitcoin* банкомата.

Неки користе постојеће мреже традиционалних банкомате у банци где једноставно полажу новац који касније користе за куповину криптовалута. Примећујемо да је овај систем готово идентичан традиционалном системо јер се „перачи новца" суочавају са истим проблемом око износа депонованих средстава који не подлеже додатним контролама од стране банке. Поред тога, овај начин куповине криптовалута је више комплексан јер захтева постојање кривичног дела крађе идентитета или злоупотребе платних картица. На већини сајтова за мењање локалних валута за крипто, потребно је унети личне потатке. Примећује се да је овај начин имплементације готово исти као и код класичног депоновања средстава на рачуне, јер је иницијална проблематика иста, из угла криминалаца.

Други користе трговачке ланце који омогућавају куповину *Bitcoin-a* путем благајне. Овај систем је посебно заступљен у западном свету, могућност куповине криптовалуте у супер маркету сама по себи одаје утисак несигурности и могућности злоупотребе. Као последица ових особина, поставља се питање професионалности и могућности лица које пружа услугу на благајни, таква лица најчешће нису обучена за било какву реакцију у циљу спречавања прања новца.

Broker exchanges су мењачнице које се могу пронаћи на аеродромима. Међутим, уместо размене различитих локалних валута (попут ЕУР у УСД), своју локалну валуту можете заменити за криптовалуте. То је један од најједноставнији начин куповине криптовалуте и зависно од законске регулативе најчешће не захтева посебну аутентификацију података и порекла новца. Али сама куповина захтева дигитално плаћање (дебитна и кредитна картица; *paypal...)* што се опет своди на традиционалан начин извођења прве фазе – полагања.



Слика бр. 20. Извор: What Are The Three Stages Of Money Laundering? (https://brittontime.com/)

АТМ машине за куповину и продају су један од најпопуларнијих система куповине криптовалута у криминалном свету. Овај начин трансакције има низ предности које олакшавају куповину „перачима":

Анонимност – је најважнија из угла криминалаца, у фази имплементације то је најрањивија ставка, и за разлику од других начина куповине који такође обезбеђују анонимност, код куповине преко АТМ она је апсолутна, јер је лице у комуникацији са машином. Искључен је и онај минималан ризик од људског фактора који постоји у односу са делатником нпр. у *Broker exchanges* или благајнама трговачких центара. Постоје АТМ машине које захтевају идентификацију, па чак и отисак прста, али њихов број је доста мањи.

Неограничена могућност куповине – се разликује од државе, региона и провајдера АТМ услуге. Неке од њих дозвољавају неограничен трансфер (куповина и продаја) док су неке ограничиле висину транфера на месечном нивоу. У Републици Србији постоје два провајдера АТМ мењачница са укупно шест машина. Један од њих је ограничио месечни трансфер, уз верификацију броја мобилног телефона, на 30.000 рсд, а за износе преко наведене цифре потребна је идентификација у виду важећег личног документа. Други провајдер омогућава трансакције до 250 ЕУР на дневном нивоу без било какве верификације и идентификације, док за износе веће од наведене цифре захтева испуњавање услова као и претходни провајдер. Поређења ради, у Мађарској одређени провајдери дају могућност дневног трансфера у износу од 2.500.000 ХУФ[54] што је око 7.200 ЕУР и какактеристично је што

[54] https://coinatmradar.com/bitcoin_atm/15150/bitcoin-atm-general-bytes-szeged-change-valutavaltas/ приступљено 10.09.2020.

не постоји могућност трансфера већег од те цифре на дневном нивоу, па чак и уз идентификацију. Другим речима, криминалци имају бесконачну могућност куповине, ако се претпостави да након сваке уплате од 7.200 ЕУР долази до промене крипто новчаника.

Брзина – није најбитнија ставка, али свакако из угла криминалаца представља погодност која смањује ризик од евентуалног откривања. АТМ машине обављају радње у секунди и представљају најбржу платформу за куповину и продају *Bitcoina*. Модел машине такође одређује њену радну брзину. Већина њих обрађује команде за мање од 15 секунди. Кориснику је једноставно потребно да скенира *QR* код, кликне на убаци или повуче рачуне и након притиска на дугме за слање трансакција је завршена.[55]

Поред ових особина које су пресудне за прање новца, АТМ мењачнице приликом трансакција узимају провизију између 5 – 10 %. Из угла посматрања обичног корисника машине, то је износ који није занемарљив и често се одлучују за неки други облик трансакције. Међутим из перспективе особа, које се баве криминалним радњама које си узрок постојања прљавог новца, овај недостатак не представља ману која може да их одврати од употребе АТМ машина. Особе из тог миљеа сматрају да је вредност новца који је имплементиран у легалне токове вишеструко већа од „прљавог", иако је „опраног" новца значајно мање. Другим речима, не маре за висину провизије као ману, већ се фокусирају на предности које АТМ мењачница пружа.

Peer-to-Peer (P2P) куповина и продаја – један од најједноставнијих начина за куповину и продају криптовалута у оквиру кога стране имају могућност договора о условима и начину трговине. С обзиром да је P2P тип мреже у којој ни једна страна нема привилеговани положај и садржај се дели директно ка субјектима комуникације без било каквих посредника (нпр. сервери администратори), веома је погодна за злоупотребе у виду прања новца и других дела против привреде (нпр. примање мита под окриљем крипти размене). Карактеристика овог начина размене је у томе што је веома флексибилна и услови саме реализације зависе од купца и продавца, тј њиховог индивидуалног договора. То значи да у оквиру трансфера ни једна страна не мора приказати документ који потврђује идентитет и само плаћање у виду локалне валуте се може извршити на били који начин који субјектима у овом процесу одговара. Хипотетички гледано, странке овог односа би своју трансакцију могле извршити непосредном разменом физичког новца за вредност криптовалуте која је ускладиштена на хардверски новчаник. У овом облику размене најчешће учествују особе које не желе транспарентност и особе које

[55] https://techbullion.com/how-the-bitcoin-atms-work-and-their-advantages/ приступљено 28.07.2020.

желе да избегну плаћање провизије која у овом начину трговине не постоји. Купци и продавци се проналазе тако што се оглашавају на сајтовима који нуде различите услуге нпр. *Craigslist*.

Из ових начина куповине закључујемо да је могућност злоупотребе веома висока и једноставност самих процеса трансакције олакшава употребу обичним корисницима који не морају имати професионално знање у куповини криптовалута, а самим тим и о првој фази прања новца. „Перачи новца" купују крипто средства на местима која нису усаглашена са *AML* политиком и која не захтевају употребу KYC (*know your client/ customer*) протокола. Права снага криптовалуте неће бити број људи који у њу улажу, већ број људи који с њом обављају трансакције[56].

Друга фаза – Фаза прикривања

Људи користе миксере (претвараче) као покушај да сачувају приватност приликом трансакција са *Bitcoin* –ом и другим криптовалутама тако што прикривају траг свог новца. Ове услуге обично не захтевају провере *Know Your Customer* (KYC) и примарно се користе за анонимно преношење средстава између услуга. Ово би могло довести до логичног закључка да се миксери готово искључиво користе за прање новца или скривање профита од нелегалних активности. Али то није увек случај неки корисници имају политичке разлоге због којих желе остати анонимни.

Ипак, након што појединци пребаце ову „заражену" крипто имовину у регулисане размене или друге финансијске услуге, она ће бити означена од стране институције против прања новца. Ови механизми за оцењивање *AML* политике упозоравају сервис тамо где желе да депонују криптовалуте да су њихова средства пословала са миксером. Другим речима, њихова криптовалута постала је „заражена" придруживањем адреси услуге мешања.

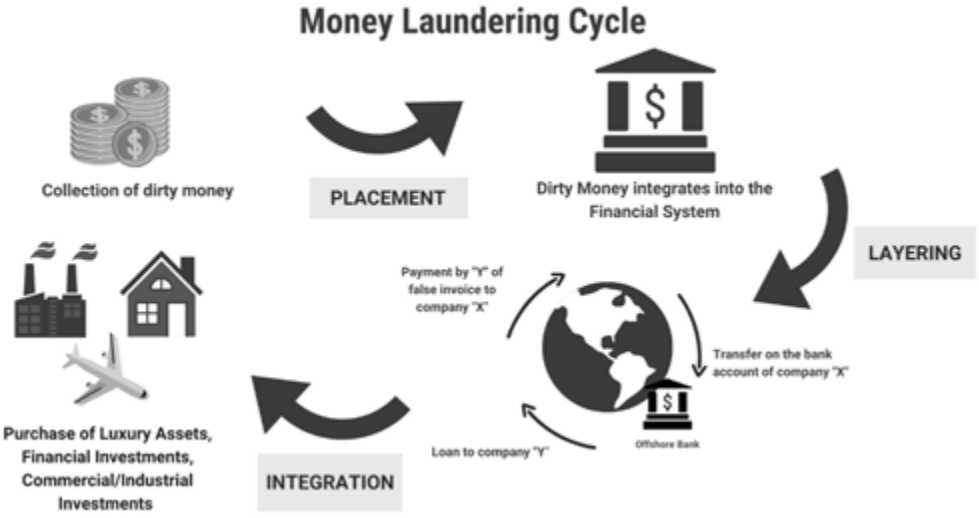
2019. године корисници *Bitcoin* –а су од *BestMixer.io* почели да примају незнатне количине *BTC*-а заједно са промотивном поруком која промовише њихов сервис, која омогућава корисницима да мешају *Bitcoin*, *Litecoin* и *Bitcoin Cash*. Ове ситне трансакције у суштини су представљале масовну рекламну кампању.

Али за разлику од нежељене рекламе, „*crypto dusting*" како су поједини назвали овај феномен, није безазлена. Покретањем злонамерне шеме оглашавања која укључује слање *Bitcoin* на *BTC* адресе, *BestMixer* технички означава ове адресе контаминирајући их да заједно са мешачем

[56] https://www.iaca.int/iaca-alumni/blog-view-magazine/402-cryptocurrency-crime-versus-control-or-the-future-of-money.html приступљено 01.08.2022.

врше трансакцију без њиховог пристанка. Како време напредује у свету криптовалуте, овај облик нежељене поште ускоро би могао постати главна техника криминалних актере и контаминирање законитих корисника у масовним кампањама „запрашивања."

Почетни извештаји погрешно су описали напад „прашине" као напад на приватност. *Bitmixer* очигледно покушава да добије маркетиншку покривеност за њихов миксер.



Слика бр. 21. Извор: Overview (https://www.unodc.org/)

Bitmixer наводи како је главна предност њихове услуге у томе што су сва средства која су враћена корисницима након мешања, верификована на берзи криптовалута са несумњиво позитивном историјом. Додатна поента је да сав новац примате у разним деловима у насумичним временским интервалима и на различите адресе. То је вероватно најбољи алгоритам анонимности до данас.[57]

Неки миксери функционишу тако што укључују велики број корисника који депонују своја средства у заједнички новчаник. Након тога миксери узимају сва средства и враћају их на адресе корисника у износу који су депоновали.

Обично наплаћују до 3-5% по трансакцији, па им је маркетинг услуга прања новца и мешања у најбољем интересу. Ако овакав сервис за мешање може да помеша 100 милиона долара годишње, они зарађују 3-5 милиона долара годишње од рада на малом серверу са седиштм у некој малој острвској земљи која нема механизме ни ресурсе за супротстављање.

[57] https://www.bitmixer.co/ приступљено 15.06.2020.

Према Европолу, постоје знакови пада употребе миксера. Два највећа миксера, *BitMixer* и *Grams Hekix*, угасили су се 2017. У таквој позицији, Европол очекује да ће потреба за миксерима опадати јер ће приватне кованице бити све раширеније.[58]

Криминалци поред миксера користе и једноставан систем слојевитих трансакција које отежавају праћење пре претварања средстава у локалне валуте или друге криптовалуте. Овај систем се назива *chain hopping*[59] и представља дигиталну размену криптовалута из једне у другу, креирајући тако траг новца који је немогуће пратити. Ова врста трансакције није условљена количином средстава која се размењују. Из угла истражитеља који се баве прањем новца, знатно је теже пратити већи број мањих трансакција.

Трећа фаза – интеграција

У трећој фази криминалци покушавају да искористе анонимност како би нелегално стечена средства пребацили у легалне токове. *OTC* (over the counter) брокери олакшавају трговину између појединачних купаца и продаваца који не могу или не желе да раде на отвореној берзи. *OTC* брокери су обично повезани са разменом, али делују независно. Трговци често користе *OTC* брокере ако желе да ликвидирају велику количину криптовалуте за одређену цену по договору. *OTC* брокери су кључни извор ликвидности на тржишту криптовалута. Иако је немогуће знати тачну величину *OTC* тржишта, знамо да је огромна[60].

Проблем код оваквог начине представља легитиман посао који *OTC* брокери воде, а заправо су део криминалне групе која у оквиру својих задужења има задатак претварања крипто средстава у новац. Често се криптовалута прво претвара у неку врсту стабилне посредничке валуте(нпр. *Tether),* затим се уновчава.

Према сајту *Chainalysis*, извршили су анализе трансакција различитих криминалних група и саставили листу од 100 главних *OTC* брокера за које верују да пружају услуге прања новца, засноване на чињеници да су примили велике количине криптовалуте из незаконитих извора. Ово не представља обимну листу *OTC* брокера, пре је то узорак који су сакупили на основу њиховог искуства с прањем новца током времена. Назвали су их „Rogue 100". Седамдесет *OTC* брокера из „Rogue 100" налази се у групи

[58] Европол, *Internet Organised Crime Threat Assessment* 2018, стр. 63.

[59] https://dailyfintech.com/2020/08/10/follow-the-money-crypto-laundering/ приступљено 16.08.2020.

[60] https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019 приступљено 24.05.2020.

Huobi (компаније за размену криптовалута) рачуна који примају *Bitcoin* из недозвољених извора. Њих 32 су у групи од 810 рачуна који примају највише нелегалних *Bitcoin-a*, а 20 њих је у 2019. Години добило милион долара или више у вредности нелегалних *Bitcoin*. Укупно, ових 70 *OTC* брокера је од криминалних субјеката током 2019. године добило 194 милиона долара *Bitcoina*. „Rogue 100" представљају само *OTC* брокере које су ручно идентификовали као „перачи новца" током истрага у име клијената *Chainalysis-a*. [61]

У фази интеграције дигиталних средстава у легалну економији такође се користе АТМ мењачнице. У овој фази није од значаја да ли машине захтевају идентификацију, чак је она и пожељна од стране криминалаца због тога да би се обезбедио траг порекла новца.

Како је већ неколико пута наведено, дигитализација и техничко – технолошки развој друштва су довели до промена у свакодневном животу људи. Због тога се можемо све чешће срести са *online* плаћањем различитих ствари у виду криптовалуте.

Прихватање *Bitcoin-a* као средства плаћања зависи од одлуке одређене компаније. Због тога не постоји посебно тржиште на којем су *Bitcoin-и* универзално прихваћени. Уместо тога, постоје различите компаније у различитим услужним секторима које желе проширити своју базу купаца увођењем дигиталних валута као новог начина плаћања.

Неке од области где се ствари и услуга могу платити *Bitcoin-ом* су: *online* сајт за упознавање, *online* новинске претплате, регистрација домена, видео игре, путовања, угоститељство (барови и ресторани; један сервис нуди могућност поручивања пице *Bitcoin-ом*), донације у криптовалутама, такси служба и друге.[62]

Не треба заборавити да се велики број „опраних" средстава враћа у легалне економске токове преко постојећег банкарског система.

4.3. Законска регулација о прању новца криптовалутама

Почетак се везује са тренутком када су владе приметиле *Bitcoin*, када је постао довољно велик као феномен да су се владе почеле бринути због утицаја који би могао да има и почеле су да разговарају о томе како да реагују на њега. Један од разлога зашто би владе приметиле дигиталну валуту (*Bitcoin)* је тај што законски недефинисана дигитална средства, ако она постоје, могу оборити контролу капитала. Контроле капитала су

[61] https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019; приступљено 15.07.2020.

[62] https://rs.cointelegraph.com/bitcoin-for-beginners/what-can-i-buy-with-bitcoins; приступљено 23.09.2020.

правила или закони које држава доноси и који су осмишљени да спрече проток вредности. Другим речима то је стављање контроле на кретање капиталног богатства у земљи или изван њених граница.

Bitcoin је врло лак начин, у одређеним околностима, да порази контролу капитала, јер неко може једноставно да купи *Bitcoin* са капиталом у земљи, да те *Bitcoin-е* пошаље изван земље електронским путем, а затим да те *Bitcoin-е* прода за капитал или богатство изван земље. Радећи то, омогућује се премештање капитал или богатство изнутра према споља или обрнуто. Пошто се богатство у овом електронском облику може тако лако кретати преко граница и не може га заиста контролисати, влада која жели да примењује контролу капитала у свету, мора покушати прекинути везу са *Bitcoin* –ом.[63]

Неке владе су покушале да ограниче употребу криптовалуте, за коју сматрају да олакшава корупцију, а такође покушавају да користе исту технологију како би финансијски систем постао транспарентнији и отпорнији на преваре.

Постојеће криптовалуте могу се на крају регулисати и контролисати ради спречавања криминалних активности. Слично томе, владе могу да успоставе нове шифроване криптовалуте као легитимну дигиталну валуту. Међутим, како је технолошка иновација по дефиницији неозбиљна, чини се да је тешко зауставити развој нових криптовалута. Потражња за слободним протоком трансакција и независност од централних банкарских система додатно ће подстаћи та кретања.

Можда је најважније напетост између циља владе да учине тржиште ефикаснијим и њихових покушаја да контролишу криптовалуте у политичке и финансијске сврхе.

Тржишна ефикасност сигурно захтева мало интервенције владе, а чини се да технологија *blockchaina* томе доприноси. Ако заиста идемо према времену виртуелне валуте, одговорност централних банака може се променити и њихова независност у одређивању монетарне политике ће требати додатне прегледе и заштиту од јавног надзора и политичких притисака. Могу бити и друге импликације, посебно у контексту антикорупцијске и криминалне активности.

Без обзира на то да ли се ради о непредвидивим интервенцијама владе, одређеним тржиштима која покрећу крипто-вал или расправама у *cyber* заједници о томе како треба да се смањи криптовалута, још увек нису јасни трендови упркос растућој нади оних који се баве криптовалутама.

[63] https://www.coursera.org/specializations/wharton-fintech; последњи пут приступљено 22.06.2022.

Табела 4. Приказ законске регулативе против прања новца и других криминалних радњи у вези са крипто средствима, упоредни приказ.

	ЕУ	Us-FinCEN	Русија	Кина	Велика Британија	Малта	Иран
Крипто – локална валут	РГ	РГ	РУТ	З	РУТ	РГ	З
Крипто - крипто	НР	РГ	РУТ	НР	РУТ	РГ	НР
„Travel rule“	НР	РГ	НР	НР	РУТ	НР	НР
„custody solutions“	РГ	РГ	НР	НР	РУТ	РГ	НР
ICO - „initial coin offering“	РГ	РГ	РГ	З	РУТ	РГ	НР
Мењачнице	РГ	РГ	РУТ	З	РУТ	РГ	РУТ
Новчаници	РГ	РГ	НР	НР	РУТ	РГ	НР
„privacy coins“	НР	РГ	НР	НР	РУТ	НР	НР
„smart contracts“	НР	НР	РГ	НР	НР	РГ	НР
„hedge rules“	НР	НР	НР	НР	НР	РГ	НР
„mining“	НР	НР	РУТ	НР	НР	НР	РУТ

З – забрана РУТ – регулација у току РГ – регулисано законом НР – нерегулисано законом

Извор: https://ciphertrace.com/

Док се криптовалута брзо развија, тренутни статус глобалног финансијског система могао би бити у опасности и прилика да се амерички долар скине са пиједестала светски признате и усвојене валуте, као међународна валута избора за званичне и незваничне трансакције.[64]

Табела 4 приказује веома различите нивое зрелости и опште прихваћености крипто средстава као привредне претње на државу или организацију. Недостатци законских регулатива представљају ризичне путеве које могу искористити „перачи новца“ и терористичке организације. Конкретно, законодавци се недовољно баве ризицима прања новца од крипто – крипто размене, *privacy coins* и осталих анонимних услуга.

Из ове табеле још можемо закључити да већина области, везаних за крипто средства, није регулисано у склопу наведених субјеката. Мењачнице и размена криптовалута у локалну валуту су једине области које су регулисане од стране свих субјеката или су у процесу регулације.

Поред Малте за коју би се могло рећи да је област крипто средстава ставила под законски оквир, Русија је донела закон „О дигиталним правима“. Овај нови закон формално уређује паметне уговоре *(„smart contracts“)* и заштиту крипто жетона у руском грађанском закону. Законодавство дефинише „дигитална права“ као хартије од вредности или скуп уговорних права на која ималац има право. Закон такође описује како корисници

[64] https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf; приступљено 18.07.2020.

могу да користе и преносе та „дигитална права" и налаже да информациони системи буду у стању да идентификују власника дигиталних права као и учеснике трансакције и да омогуће репродукцију услова споразума.[65]

Кинеска централна банка, Народна банка Кине већ три године спроводи истраживање дигиталне валуте и основала је Институт за дигитални новац у оквиру банке. Кинески регулатори не признају виртуалне валуте попут *Bitcoina* као средство за плаћање у малопродаји попут папирних новчаница, кованица или кредитних картица. [66] Банкарски систем не прихвата ниједну виртуалну валуту нити пружа одговарајуће услуге.

Ограничени број земаља регулише *initial coin offering* (*ICO*), који користе криптовалуте као механизам за прикупљање средстава. Међу јурисдикцијама које се баве *ICO*-м, већина се углавном фокусира на њихово регуисање док их неке (углавном Кина, Макао и Пакистан) забрањују у потпуности.

Разлике у категоризацији *ICO*-а зависи од регулација и релевантних регулаторних институција. На пример, на Новом Зеланду се могу применити посебне обавезе у зависности од тога да ли је понуђени токен (*ICO)* категорисан као гаранција дуга, хартија од вредности, управљани инвестициони производ или дериват. Слично томе, у Холандији правила која се примењују на одређени *ICO* зависе од тога да ли се понуђени токен сматра хартијама од вредности или јединицом у колективном улагању.

Регулаторна тела у Кини су упозорили да токени или виртуелне валуте укључене у финансирање *ICO*-а не издају монетарне власти и стога нису прихваћене као легалне понуде, немају једнак правни статус са локалном валутом и не могу и не би требало да циркулишу и користе на тржишту као валута. [67]

Многа упозорења различитих земаља такође говоре о могућности које криптовалуте стварају за илегалне активности, попут прања новца и тероризма. Неке од анкетираних земаља превазилазе просто упозоравање јавности на штетно деловање и проширile су своје законе о прању новца, тероризму и о организованом криминалу на тржиште криптовалута. Оне траже од банака и других финансијских институција које омогућавају таквим тржиштима пословање, да спроведу све потребне захтеве, ревизије и прописе који су у складу са законима.

---

[65] https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/ последњи пут приступљено 02.08.2022.

[66] *Zhou Xiaochuan (*2018*): Future Regulation on Virtual Currency Will Be Dynamic, Imprudent Products Shall Be Stopped for Now,* Xinhuanet.

[67] http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html; приступљено 14.08.2020.

На пример, Аустралија, Канада и *Isle of Man* су донели законе против прања новца и финансирања тероризма којима су обухватили трансакције са криптовалутама и дефинисани су институционални оквири.

Неке су надлежности отишле још даље и наметнуле су ограничења улагања у криптовалуте, чији обим варира од једне до друге надлежности. Неке државе (Алжир, Боливија, Мароко, Непал, Пакистан и Вијетнам) забрањују све активности које укључују криптовалуте.

Катар и Бахреин имају нешто другачији приступ у томе што забрањују својим грађанима да се баве било каквим активностима које укључују криптовалуте локално, али грађанима дозвољавају да то раде ван својих граница.

Постоје и државе које, иако не забрањују својим грађанима да улажу у криптовалуте, намећу индиректна ограничења тако што забрањују финансијским институцијама да унутар својих граница олакшавају трансакције које укључују криптовалуте (Бангладеш, Иран, Тајланд, Литванија, Лесото, Кина и Колумбија).

Нису све земље појаву *blockchain* технологије и криптовалута виделе као претњу. Неке јурисдикције, иако криптовалуте не признају као легално средство плаћања, виде потенцијал у технологији која стоји иза њега и развијају регулаторни режим погодан за криптовалуте као средство за привлачење инвестиција у технологију компанија које имају одличан успех у овом сектору. У ову класу спадају државе попут Шпаније, Белорусије, Кајманских острва и Луксембурга.

Неке јурисдикције желе још више и развијају сопствени систем криптовалута. Ова категорија укључује разноврсну листу земаља, попут Маршалових острва, Венецуеле, држава чланица Централне банке Источних Кариба (*ECCB*) и Литваније.

Индијска влада дуго се бори против употребе нерегулисаних криптовалута, јер се оне често користе за прање новца и други финансијски криминал. Влада тек треба да објави званични предлог закона. Нацртом закона се такође тражи да се уведе званична дигитална валута за Индију, „Дигитална рупија", коју ће влада уско регулисати. [68]

4.4. Симбиоза cyber криминала, привредног криминала и преваре

У водећим финансијским институцијама нагласак је да се уложе заједнички напори против финансијског криминала, превара и *cyber* криминала. *AML* (*anti money loundering*), док се сада углавном гледа као

[68] https://www.bankinfosecurity.asia/government-mulls-banning-cryptocurrencies-a-12628; приступљено 15.08.2020.

регулаторно питање, сматра се следећим хоризонтом за интеграцију. Важни почетни кораци за институције које предузимају интеграционе напоре јесу прецизно дефинисати природу свих повезаних активности управљања ризиком и разјаснити улоге и одговорности у линијама одбране. Ови кораци ће обезбедити потпуну, јасно разграничену покривеност - од стране предузећа и функција предузећа (прва линија одбране) и ризика, укључујући финансијски криминал, преваре и *cyber* деловање (друга линија), истовремено елиминишући дуплирање напора.

Сви ризици повезани са *online* привредним криминалом подразумевају три врсте контрамера[69]:

1. идентификација и аутентификација купца,
2. надзор и откривање аномалија трансакција и понашања,
3. реаговање на ублажавање ризика и проблема.

Контра-мере у случају привредног (финансијског) криминала:

1. Оцена ризика клијента, повећана пажња на дуговања и друштвени статус клијента (нпр. особа на високој политичкој функцији)
2. Надгледање трансакција, праћење имена особа ка којима су трансакције упућене као и праћење тренутних плаћања.
3. Праћење сумњивих активности, оснивање јединице за финансијске истраге, *List management* укључује задатке објављивања података и максимизирање одговора на претњу промотивним напорима.

Контра-мере у случају преваре повезане са привредним криминалом у дигиталном простору:

1. Провера идентитета,укључујући дигитално и недигитално присуство.
2. Надгледање трансакција и доношење одлука о валидности истих, анализа уређаја са којих се врши трансакција и анализа гласа.
3. Оснивање тимова који се баве истрагом и решењем проблема преваре.

Контра-мере у случају *cyber* криминала као средства извршења привредног криминала:

1. Управљање повериоцима,
2. Оснивање сигурносно-оперативних центара и мрежно оперативних центара за котролу и праћење,
3. Оснивање сигурносно-оперативних центара и посебних тимова за решавање претњи, као и посебних форензичких тимова.

[69] https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity; приступљено 11.07.2020.

Свака од ових активности, било да су узете као одговор за превару, кршење *cyber* безбедности или друге финансијске злочине, има подршку у виду података и процеса. Спајање ових извора података са аналитичким материјалом побољшава видљивост, истовремено пружајући много дубљи увид за побољшање могућности откривања. Такође омогућава превентивне напоре. У мултидисциплинарном погледу основних процеса, банке могу да усмере пословање и технолошку архитектура за бољу подршку купцима, побољшано одлучивање о ризицима и веће ефикасности трошкова. Организациона структура може се затим реконструисати по потреби.

Приступ овим областима од стране надлежних институција можемо поделити на три модела:[70]

Колаборативни модел. У овом моделу који за већину банака представља статус кво, свака од области, финансијски криминал, преваре и *cyber* сигурност, одржавају своје независне улоге, одговорности и извештавање. Свака јединица гради свој независни оквир, сарађујући на таксономији ризика и подацима и аналитикама за надгледање трансакција, превара и кршења. Приступ је познат регулаторима, али нуди банкама мало потребне транспарентности за развој обједињеног погледа на ризик финансијског криминала. Додатно, колаборативни модел често доводи до прикривања празнине или долази до преклапања између различитих група и не успевају у постизању сразмерне предности које долазе са већом функционалном интеграцијом. Модел се ослања на мање, дискретне јединице, такође значи да ће банке бити мање способне да привуку најбоље лидерске таленте.

Делимично интегрисани модел за *cyber* сигурност и преваре. Многе институције сада раде према овом моделу, у коме су *cyber* сигурност и превара делимично интегрисане као друга линија одбране. Свака јединица одржава независност у овом моделу, али делује из конзистентног оквира и таксономије, пратећи међусобно прихваћена правила и одговорности. Тако конзистентна (доследна) архитектура за превенцију (као што је и за оверавање аутентичности купца) је усвојена, процеси идентификације и процене ризика (укључујући таксономију) су подељени, и слични процеси забрањивања су развијени (распоређени). Превладавају дубље интегралне предности, укључујући доследност у надгледању и откривању претњи и нижи ризик од пукотина и преклапања. Ипак, приступ остаје доследан постојећој организационој структури и мало омета тренутне операције. Сходно томе, транспарентност се не повећава, будући да се одвојено

[70] https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity приступљено 20.07.2020.

извештавање одржава. Нема користи од сразмерних нагомилавања и са мањим оперативним јединицама које су још увек на месту, модел је мање атрактиван за врхунске таленте.

Унифицирани модел. У овом потпуно интегрисаном приступу, финансијски криминал, преваре и *cyber* сигурност операције су обједињене у јединствену оквир, са заједничким средствима и системима који се користе за управљање ризиком у предузећу. Модел има јединствен поглед на купца и дели аналитику. Конвергенцијом ризика побољшава се транспарентност пријетњи на нивоу цијелог предузећа, што боље открива најважније основне ризике. Унифицирани модел такође обухвата предности сразмерне кључним улогама и на тај начин повећава способност банке да привуче и задржати врхунске таленте. Недостаци овог модела су што укључује значајне организационе промене, чинећи пословање банке мање познато регулаторима. Чак и са организационом променом и конвергенцијом ризика, ризици остају различити.

Путеви криминала се зближавају, замагливши традиционалне разлике између *cyber* преступа, преваре и финансијског криминала. Банке, као најзначајније финансијске институције, теже ка томе да се границе постављене између ових радњи регулишу обједињеним приступом заснованом на истим подацима и процесима.

4.5. Банке – субјекти у ланцу прања новца

Кључни тренд је све већа испреплетеност банкарских и виртуелних средстава. У четвртом тромесечју 2019. године, *CipherTrace* (сајт који се бави дигиталном форензиком криптовалута) је објавио резултате велике студије из које се може видети да су готово свих десет првих америчких малопродајних банака затражиле *MSB*-ове (*MONEY SERVICES BUSINESSES*) у криптовалутама. У то укључујући крипто размене и средства која су пренели на своје мреже плаћања. Анализа даље открива да типично велика америчка банка годишње обрађује милијарде неоткривених трансфера везаних за криптовалуте. Ове прикривене операције стварају ризике поштовања закона, правила и њихову злоупотребу. Криминалци морају пронаћи начине за прање неовлашћено стечених крипто профита, без обзира да ли се тај профит доспео у дигитални свет кроз фазу интеграције прања новца или се прибавио кроз неки од облика *cyber* криминала и преваре.

Распрострањено и често незапажено присуство крипто имовине у финансијским системима излаже банке ризику против прања новца (*AML*) и сузбијању финансирања тероризма (*CTF*). У ствари, *CipherTrace*

истраживање је показало да су банке глобално платиле више од 6,2 милијарди америчких долара новчаних казни у 2019. години.

Придржавање *AML / CTF* није једини ризик повезан са недостатком видљивости крипто имовине на рачунима купаца и платним мрежама. Такође отвара могућнос банкама да извршењем радњи не поштују економске и трговинске санкције наметнуте непослушним земљама као што су Иран и Северна Кореја. Ове санкције се строго примењују према америчком закону Канцеларије за контролу страних средстава (*OFAC*) Министарства финансија[71].

У 2019. години *OFAC* је доживео неке револуционарне извршне акције, попут санкционисања појединих адреса и објављивања имена власника. *OFAC* сматра да кршење поменутог закона представља озбиљан ризик по националну безбедност и могућност изрицања кривичне казне до 20 милиона америчких долара, зависно од кривичног дела, и затворске казне дуге чак 30 година. Грађанске казне за кршење закона могу досећи и до 65 000 америчких долара за сваку повреду[72].

Даркнет тржишта представљају још један вектор претњи банкама. Истраживање *CipherTrace* -а открива да 66% продаваца даркнет тржишта продаје компромитоване банковне рачуне и украдене финансијске производе. Поред тога, даркнет тржишта су омогућила изузетно једноставну куповину софтвера за *ransomware* нападе који је доступан за само 4,99 УСД. Истраживачи су даље открили да је 97% *ransomware* регистрованих напада 2019. године тражило плаћање *у Bitcoinu*.[73]

BTC је веома погодан као платна линија за злочине *ransomware*, јер је то најзаступљенија криптовалута и сходно томе се лакше материјализује у локалну валуту.

„*TRAVEL RULE*" је дизајниран тако да умањи оно што *FATF* види као растућу претњу од прања новца и финансирања тероризма. Нова правила о путовању средстава захтевају од провајдера услуга да размењују и чувају податке о пошиљаоцу (иницијатору) и примаоцу (кориснику) пре обраде трансакција виртуелним средствима. Ово даље захтева од банака да морају поштовати правило о познавању клијената (*KYC*) који су у овом случају провајдери.

---

[71] https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/; приступљено 22.05.2022.

[72] https://www.treasury.gov/about/organizational-structure/offices/pages/office-of-foreign-assets-control.aspx последњи пут приступљено 22.05.2022.

[73] https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/ последњи пут приступљено 22.05.2022.

У заједници виртуалних средстава одмах се појавила забринутост да поштовање правила путовања није само непрактично с обзиром на тренутну технологију *blockchaina*-а, већ је и супротно природи криптовалута.

Провајдери услуга у вези са дигиталним средствима се називају *Virtual asset service provider – VASP,*[74] и представљају било које физичко или правно лице које није обухваћено другим регулативама, а као предузеће обавља једну или више следећих активности или операција за или у име другог физичког или правног лица:

- Размена између виртуелне имовине и локалних валута;
- Размена између једног или више облика виртуелних средстава;
- Пренос виртуелне имовине;
- Чување и / или управљање виртуелном имовином или инструментима који омогућавају контролу над виртуелном имовином; и
- Учешће и пружање финансијских услуга у вези са понудом издаваоца и / или продајом виртуелне имовине.

У овом контексту виртуелне имовине, пренос значи обављање трансакције у име другог физичког или правног лица које виртуелна средства премешта са једне адресе или рачуна на други.

Током 2019. године, размене криптовалута и други *VASP* –ови у 28 држава чланица Европске уније (ЕУ) такође су се суочени са другим великим сетом нових прописа. Пета директива против прања новца, различито названа *5AMLD* и *AMLD5*, ступила је на снагу 10. јануара 2020. године. Делимично потакнути терористичким нападима у Француској, нови прописи представљају тежњу за транспарентнијим трансакцијама између криптовалута, чинећи информације о *AML / CTF* доступним европским финансијским регулаторима. Директива такође укључује строге нове прописе за *VASP*–ове о размени криптовалута и провајдерима *online* новчаника. Неусклађени *VASP* -ови могу се казнити новчаном казном до 200.000е.[75]

Банке несвесно шаљу средства *VASP*–овима, чиме се излажу ризику од прања новца. Како све већи потрошачки и институционални инвеститори прихватају криптовалуте, традиционалним фирмама за финансијске услуге постаје све теже, ако не и немогуће да избегну замке са крипто економијом. На пример, значајни ризици против уговорних страна произилазе из тога што купци остварују ризичне крипто размене.

---

[74] https://www.fatf-gafi.org/glossary/u-z/ последњи пут приступљено 04.10.2020.

[75] https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/; приступљено 22.05.2020.

Остали ризици укључују:

- Слање и примање новца добављачу виртуелних средстава (*VASP*) и од њега, а да то не знате (нпр. *Bitmixer*).
- Хостинг компаније са нелегалним новцем.
- Слање новца субјектима који су на *OFAC*–овој листи санкционисаних, појединцима и *blockchain* адресама.
- Могуће је олакшавање финансирања тероризма.[76]

Банке немају опште прихваћен систем ефикасног и аутоматизованог начина за процену ризичности *VASP*–ова. То за последицу може имати неадекватну процену која би довела до одвраћања потенцијално уносних клијената. Поред тога, оне не намерно ризикују да присиле компаније, које послују у крипто свету, на прикривање трансакција и праву природу свог пословања. На тај начин стварају више милијуонске слепе тачке које спутавају банкарске системе да процене и разумеју изложеност ризику, а као наставак и примену *AML* политике.

Једном када их банке одбију, ове компаније могу се окренути ризичним алтернативама, као што је на пример, панамски процес плаћања . У међувремену, неке банке настоје да побољшају своју способност откривања и реаговања на ризике скривених крипто средстава користећи алате отвореног типа да би прегледали *blockchain*. Али овим алатима често недостаје интелигенција (укључујући оцене ризика за размене криптовалута широм света) неопходна за обављање било чега осим анализе основних ствари. Будуће банке почињу да смањују изложеност *AML/CTF* коришћењем специјализованих алата изграђених за идентификацију ризичних добављача услуга виртуелних валута и других ризика усклађености који произилазе из пословања са крипто имовином.

Као што је већ наглашено, *P2P* тржишта криптовалутама су веома популарна међу онима који желе да задрже анонимност у процесу трансакције. Ова тржишта су посебно дизајнирана да олакшају људима куповину и продају, јасно је да је такав начин трговине подобан за различите злоупотребе. На овим *P2P* тржиштима купцима се саветује да у случају уплаћивања готовине у банкама на пословне рачуне, никако не обавештавају банкарског службеника о куповини криптовалута, већ ће нагласити да се ради о куповини „дигиталних услуга".[77]

Слично томе, код банковних преноса, корисници који желе да купе криптовалуте усмерени су да избегавају спомињање *Bitcoin* у било којој комуникацији.

---

[76] *Ibid.*

[77] https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/ последњи пут приступљено 22.05.2020.

Поред тога што су нерегистровани, многи од ових *P2P* размењивча немају било какав *AML* програм и обављају мало или нимало познавање клијента (*KYC*). Овај недостатак контроле представља огромне ризике против прања новца за банке и друге финансијске институције.

Када банке дизајнирају свој пут према обједињеном оперативном моделу за финансијски криминал, превару и *cyber* сигурност, морају испитати питања о процесима и активностима, људима и организацији, подацима и технологији и управљању. Већина банака креће интегришући јединице за *cyber* сигурност и преваре. Како побољшавају размену информација и координацију, већа ефективност и ефикасност предупређивања ризика постаје могућа. Да би постигле циљно стање које траже, банке редефинишу организационе „линије и оквире" и што је још важније, улоге, одговорности, активности и способности потребне за сваку одбрану.

Водећа америчка банка основала је мултидисциплинарни „центар изврсности" како би се омогућило одлучивање све до краја преко преваре и *cyber* сигурности. Од превенције до истраге и опоравка, банка може указати на значајно повећање ефикасности. Глобална универзална банка прешла је пут, обједињујући све операције у вези са финансијским злочинима, укључујући преваре и *AML* политику, у јединствену глобалну услугу. Банка је постигла холистичкији приказ ризика клијента и смањила трошкове пословања за приближно 100 милиона долара.[78]

Како криминални преступи у сектору финансијских услуга постају све софистицираније и пробијају се традиционалним границама ризика, банке проматрају како различите функције спречавања ризика постају скупље и мање ефикасне. Стога лидери преиспитују своје приступе да би искористили синергију доступну у виду, превара, *cyber* сигурност и *AML* политике које се могу консолидовати по обједињеном приступу заснованом на истим подацима и процесима.

4.6. Политика супротстављања online привредном криминалу

Anty-money laundering политика

Циљ политике против прања новца је спречавање великог протока средстава преко државних граница и кретања између подземне и легитимне економије. За разлику од ове политике неке земље примењују контролу капитала, где само покушавају спречити новац да пређе границе.

[78] https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity; приступљено 25.05.2020.

У неким случајевима земље су у реду с новцем који прелази границе, али желе знати ко, шта, коме пребацује и одакле тај новац долази.

Анти-прање новца има за циљ да покуша да отежа поједине врсте криминала, посебно организованог криминала. Организоване криминалне групе често добијају пуно новца на једном месту и желе га отпремити негде другде, али не желећи да објасне одакле тај новац долази, отуда и жеља да новац пошаљу преко границе. Или сматрају да сами зарађују много новца у подземној економији и желе да тај новац доведу у надземно легитимно власништво како би га могли потрошити на лагодан живот или даље инвестирати у легалне послове. *AML* политика је дизајнирана тако да у почетку одбије покушај прања новца или да допринесу санкционисању криминалаца, а све са циљем отежавања рада организованим криминалним групама.

Само у САД-у се процењује да се трошкови спречавања прања новца (*AML*) износе 23,5 милијарди долара годишње. Европске банке се приближе са 20 милијарди долара потрошених годишње.[79]

На снази је тренутно *5AMLD* директива против прања новца која обухвата и регулисање у односу размене крипто – локална валута, без обзира да ли се пружају путем веб странице или банкомата, постоје докази да неки учесници на тржишту нису сигурни у то и поздравили би изричито појашњење у том смислу од стране регулатора.[80] Извештај радне групе за крипто средства британске владе каже да, примењујући *5AMLD*, влада намерава да се консултује о регулацији „банкомата криптовалута", који би се могли анонимно користити за куповину криптовалута.[81]

Иако су обавезе проширене на виртуалну размену валута испод *5AMLD* једнаке онима које се примењују на друга предузећа, техничке карактеристике виртуалних валута нуде могућности (попут алата за праћење *blockchain*-а) које можда не постоје у другим деловима финансијског сектора. Да би се осигурало најефикасније ублажавање ризика од привредног криминала, супервизори требају објавити и препознати иновативне приступе осмишљене да искористе те могућности.

---

[79] https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/; приступљено 02.06.2020.

[80] https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf; приступљено 04.06.2020.

[81] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf; приступљено 25.07.2020.

5AMLD Директива ће донети преко потребну транспарентност за сектор виртуелних валута широм ЕУ. То ће осигурати пружаоце услуга складиштења (новчаника) и оне размене између виртуелних валута и локалних валуте. Главне особине:

- прикупљање информације о купцима (*KYC)*;
- примењује појачану пажњу према купцима високог ризика;
- надгледање трансакције; и
- означавају нешто са *STR* ознаком, када се сумња у незакониту активност.[82]

Међутим, размене крипто за крипто контроле, нису укључене у *5AMLD*, то представља критичну слабост у ефикасности *5AMLD* да заустави прања новца и финансирања тероризма. Државе чланице ЕУ су ипак слободне да усвоје јаче прописе. Да би биле у складу са Директивом, од држава чланица се тражи да изврше измене у свом националном законодавству ради усаглашавања са ЕУ стандардима. Ако држава чланица не усвоји законе *5AMLD* у своје национално законодавство, Европска комисија може покренути правну тужбу против државе чланице у Европском суду правде.

У ишчекивању примене *5AMLD*, неколико компанија које се баве овом делатношћу већ су затворене. Базен за рударство криптовалута *Simplecoin* и *Bitcoin* платформу за играње *Chopcoin*, које је основао исти појединац, угасили су се у јануару 2020. године, позивајући се на предстојеће *5AMLD* прописе. Обавештење на вебсајту *Simplecoin*-а гласи: „Када закони ступе на снагу, били бисмо приморани да захтевамо од вас, кориснике, да се идентификујете у сврхе против прања новца. Ископавање би требало да буде доступно свима, а ми одбијамо да угрозимо приватност наших корисника. “ [83]

4.6.1. KYC – Know Your Customer

Једно од правила која иде уз прање новца је нешто што се зове познавање вашег купца (*KYC*). Ова правила могу бити мало компликовани, зависе од локалитета примене, али основне идеје *KYC* захтевају од одређене врсте предузећа која баве новцем, пре свега, идентификују и потврде ко су њихови клијенти, да знају ко су ти људи и да добију неку врсту аутентичности да они заиста јесу они за које тврде да јесу, и да ти идентитети одговарају некаквом идентитету у стварном свету.

---

[82] https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf; приступљено 01.08.2020.

[83] https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/; приступљено 22.05.2020.

Особа не може само ушетати у неку финансијску институцију и рећи неко име. Они заправо морају дати идентитет и након провере би се могли бавили одређеним пословима.

Након идентификације и аутентификације клијената, од предузећа се може тражити да процени колико је то ризично, колики је ризик у вези са одређеним клијентом, посебно ако се утврди да се клијент бави сумњивим активностима. Процена се заснива на томе како се клијент понаша, колико дуго траје његов пословни однос са компанијом, колико су познати у заједници и разне друге врсте фактора. Ова правила углавном захтевају неку врсту анализе ризика у односу на поједине клијенте, а захтевају и од компаније која је покривене од стране *KYC* да третира са више пажње клијенте чије активности изгледају ризичније.

Обично постоји захтев да се пази на аномалије у понашању, да се пази на понашање које делује као да указује на криминалне активности или прање новца или друга понашања која одступају од уобичајног. Повезивање овога заједно са проценом ризика је потребно да би се разумело колики је ниво ризика у односу на одређеног купца и на шта треба посебно обратити пажњу у конкретном случају.[84]

KYC подразумева од компаније да прекине пословање са клијентом који не може да потврди легитимитет свога пословања. У Сједињеним Америчким Државама постоје обавезни захтеви, које је вредно споменути. На пример, компаније из различитих сектора морају да извештавају о трансакцијама већим од 10 000 УСД, у обавези су да поднесу нешто што се назива извештај о валутној трансакцији. Тај извештај подразумева саржање одговора на следећа питања:

- Колика је трансакција?
- Шта се преноси (валута)?
- Ко шаље и ко прима?

Обавезно је пријављивање влади и затим извештај доспева у базе података, сагледавањем и анализом извештаја би се могли тражили обрасци понашања који указују на прање новца. Од компанија се такође тражи да пазе на клијенте који се баве структуирањем трансакција како би избегли извештавање. На пример, ако неко учествује у низу трансакција које вреде 9.000 УСД, као начин да се заобиђе правило извештавања о трансакцијама од 10.000 УСД. Такав начин преношења средстава представља структуру на коју компаније морају обратити посебну пажњу.

[84] https://www.coursera.org/learn/cryptocurrency; приступљено 14.08.2020.

Подношење извештаја о сумњивим активностима долази до базе података где анализом може довести до истраге клијента. *KYC* препоруке и регулативе се разликују од државе пословања, широко гледано, грађанска је дужност пријавити надлежним органима када постоји сазнање о кривичном делу. Америчка влада и друге владе врло озбиљно схватају правила против прања новца, што значи да ово нису само препоруке већ законски регулисана правила чије непоштовање захтева репресивно деловање од стране власти. Многе компаније које су пословале са криптовалутама су затворене, а људи су отишли затвор због непоштовања ових правила. Ово је једна од области у којој ће владе широм света енергично спроводити закон и која регулише *Bitcoin* још од тренутка када су приметили да је *Bitcoin* довољно велик да представља ризик од прања новца.

4.7. Последице прања новца на друштво и банкарски систем

Нелегално стечен новац који се враћа у легалну економију изазива незадовољство код друштва које поштује законе, као неприметни резултат криминала, прљави новац се такође користи за финансирање сукоба широм света. Како се супротстављамо прању новца и како ћемо се борити против њега у будућности је од виталног значаја за друштво и економије широм света. Опрани новац представља између два и пет процената глобалног бруто домаћег производа (БДП), наводе УН. То је еквивалент пете највеће економије на свету (Индија, БДП износи око 3 %).

Године 2009. су УН проценили да је 3,6% светског БДП-а повезано са кривичним приходима. Велики део тога је опран: 2,7% БДП-а, што је еквивалент 1,6 билиона долара.[85]

Са глобализацијом и иновацијама у технологији које олакшавају трансфер великих износа брзо и лако, овај проблем свакодневно расте. Прљави новац и зарађени добици се више не скривају у сефовима нити се закопавају, они се већином преносе у дигиталне токове и крећу се кликом миша са било које локације у свету где је могуће приступити мрежи. Ипак, сада је теже него икад пре опрати новац. Од 2001. године уложени су велики напори створени да осигурају да финансијске институције могу уочити, упозорити и поразити прање новца. То је подстакнуто законодавством и тужилаштвом и дало је значајне резултате. 2016. године педесет два процента анкетираних за истраживање финансијског криминала су рекли да очекују да ће се инвестициони буџети за борбу против прања новца (*AML*) повећати током наредне три године[86], што се и догодило. Казне за

[85] Опширније https://www.un.org/en/

[86] https://www.baesystems.com/en/cybersecurity/financial-crime-survey-2016# последњи пут приступљено 21.08.2022.

банке које не препознају и зауставе прање новца су високе. Али, постоје и други трошкови за прекршиоце, понекад ненамерни „knock-up“ ефекти за друштво у целини.

Утицај прања новца протеже се далеко изван пословања, на економију и друштво у целини.

Највећи утицај прљавог новца се може видети у области некретнина, с обзиром да њихова куповина најчешће захтева велику количину новца, тако нпр. цене некретнина у Лондону су „напумпане“ *offshore* криминалним средствима[87], док се у Ирској 60% куповина кућа плаћа у готовини[88].

Појава виртуалних валута значи да ће неки од тренутних механизама одбране против прања новца бити неважећи и биће их немогуће применити у будућности.

Банке постају опрезније и мање је вероватно да ће закључити пословне трансакције које носе већи степен ризика. Ово је допринело опадању кореспондентног банкарства кључном средству за привреде у настајању. За велике банке суочене са тешким питањима о могућностима њихових кореспондентних банака у другим земљама да испуне мере против прање новца и захтеве политички изложених лица, најсигурнија опција је да уклоне ризик и једноставно престану да тргују.

Прва жртва тренутног таласа регулације било је кореспондентно банкарство. Ако банка у једној земљи нема своју испоставу у другој и клијент мора да пренесе средства у ту земљу обратиће се другој банци која јесте у могућности да испоручи или да прикупи средства у његово име. Овај однос и сложеније варијације, некада покретана глобална трговина, осигуравали су радницима могућност слања новца кући и отварали богате економије предузећима са седиштем у сиромашнијим земљама. Систем помаже новцу и роби да лако прелазе између богатих и сиромашних економија, посебно када је рич о земљама у којима велике глобалне банке можда немају спремно присуство, омогућавајући онима у земљама у развоју приступ тржиштима развој економије.

У ризичне трансакције спадају, поред оних где се ризик не може смањити или отклонити, и оне у којима је могуће смањити ризик и отклонити али си ти трошкови превисоки за финансијске институције. Ако је немогуће утврдити извор средстава или крајњег корисника средстава банка је на крају ланца изложена ризику од трансакција прљавим новцем. Централне националне банке су дозволиле криминалцима да перу прљави

[87] http://www.cityam.com/220931/foreign-criminals-launderingmoney-drive-london-house-prices последњи пут приступљено 21.08.2022.

[88] https://www.thejournal.ie/housing-market-ireland-cash-buyers-funds-2-2895200-Jul2016/ последњи пут приступљено 25.08.2022.

новац, као и дозволивши свима другима да се баве законитим послом, и омогућиле су релативно лак пренос средстава проистеклих из кривичног дела, мита, украдених јавних средстава и готовине за терористичке активности у основане, стабилне земље у којима се могу користити. Проблем треба сагледати двострано, улога банака у слабије развијеним земљама је подједнака као и улога банака у земљама развијене економије. Разлике између националних система за борбу против прања новца искористиће перачи новца, које имају тенденцију да се своје мреже преселе у земље и финансијске системе са слабим или неефикасним противмерама.

Локалним банкама у земљама са слабије развијеном економијом можда недостаје исти ниво ресурса, људи, технологија и улагања, које би утрошили на оперативно поштовање прописа као и глобалне банке, тако да није изненађујуће да ће се можда борити да испуне захтеве на које веће институције редовно троше милионе долара. Не испуњавање међународних прописа, а у циљу спречавања прања новца, банке ризикују да њихове земље буду под међународним санкцијама, невезано да ли су то јаке економије или у развоју.

У Републици Србији је предвиђено да министар, на предлог Управе, утврђује листу држава које имају стратешке недостатке, узимајући у обзир листе релевантних међународних институција, као и извештаје о процени националних система за борбу против прања новца и финансирања тероризма од стране међународних институција[89].

Интегритет тржишта банкарских и финансијских услуга у великој мери зависи од перцепције да она функционише у оквиру високих правних, професионалних и етичких стандарда. Једна од најбитнијих ставки за финансијске институције је углед који уживају код клијената у смислу поштивања регулатива, доступности и професионалности. У случају нарушавања интегритета постоји могућност пригушивања страних улагања када се сматра да је трговински и финансијски сектор у земљи под контролом и утицајем организованог криминала. Борба против прања новца и финансирања тероризма је, дакле, део стварања окружења погодног за пословање које је предуслов за трајни економски развој[90].

Ако се средства од криминалних активности могу лако обрађивати кроз одређену институцију, било зато што су подмићени њени запослени или директори или зато што се институција једноставно не улаже довољне напоре да спречи такво пословање, она би могла бити увучена у активну спрегу са криминалцима и постати део саме криминалне мреже.

---

[89] Закон о спречавању прања новца и финансирања тероризма, *Службени гласник РС*, број 91/2019.

[90] https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate); приступљено 28.08.2020.

Докази о таквом саучесништву имаће штетан утицај на ставове осталих финансијских посредника и регулаторних тела, као и обичних клијената.

Што се тиче потенцијалних негативних макроекономских последица неконтролисаног прања новца, може се навести необјашњиве промене у новчаној тражњи, ликвидносни ризици за стабилност банака, контаминација легалних трансакција и повећана осцилација међународних капиталних токова и девизних курсева због непредвиђених прекограничних трансакција трансфери имовине. Пошто унапређује криминал и корупцију, прање новца штети интегритету читаве друштвене заједнице једне земље и дестабилизује демократију и владавину права.

Могући друштвени и политички трошкови прања новца, ако се оставе без надзора или се њиме не ефикасно поступа могу довести до озбиљних дестабилизација друштва. Организовани криминал као, као једна од битних компоненти прања новца, се може инфилтрирати у финансијске институције, стећи контролу над великим секторима економије путем улагања или подмићивањем владајућег друштвеног миљеа.

Економски и политички утицај криминалних организација може ослабити социјалну структуру, колективне етичке стандарде и демократске институције друштва. У земљама које прелазе у демократске системе, овај криминални утицај може нарушити транзицију. Прање новца је увек у нераскидивој вези са криминалним радњама које су га проузроковале, то је узрочно последична веза која се увек изнова понавља.

4.8. Орīанизована криминална īруīа у диīишталном свеш̄у

Појам повезаности организованог криминала и *cyber* криминала одражава динамичну природу и брзину промена транснационалног криминала[91]. Емпиријска истраживања о *cyber* криминалу су још увек оскудна, теоријска сазнања о условима његовог настанка и напредне хипотезе у литератури, дају основ за извођење закључка да интернет трансформише криминал и да *cyber* криминал постаје организован и обиман са све присутнијом поделом послова унутар организоване криминалне групе.[92]

Запошљавање таквих криминалних група се понекад врши у облику пружања легитимног посла, а сама организација је јасно дефинисана улогом сваког члана групе, међу којима су најважнији: програмери и

[91] McCusker, R. (2012). Organised cybercrime: myth or reality, malignant or benign? In S. Manacorda (Ed.) Cybercriminality: finding a balance between freedom and security Milano, Italy:ISPAC, стр. 107.

[92] Ђукић, А. (2018) Организовани високотехнолошки криминал – појам, развој и основне карактеристике, Универзитет у Београду, Факултет безбедности, часопис Безбедност, стр. 130.

програмери одговорни за стварање или модификација постојећег злонамерног софтвера (*malvare*), испитивач одговоран за тестирање злонамерног софтвера, кодери чија се улога огледа у препакивању злонамерног софтвера da га антивирусни софтвер не би препознао, веб дизајнери одговорни за креирање *phishing* страница, особе које су одговорне за контролу, надзор и извлачење новца са компромитованих рачуна – *money mules.* Организатори криминалне групе имају задатак да обезбеде средства неопходна за стварање злонамерних алата који би се користили за извршење кривичног дела. Велике организоване криминалне групе разликују се од осталих криминалних група по томе што њихови напади нису усмерени само на финансијске институције и куповину на мрежи, већ су усредсређени и на нападе на мала и средња предузећа, уз још бољу организацију прикупљања украденог новца коришћењем техника прања новца.

Назив *money mules* јесте тековина традиционалног начина прања новца, потпомогнуте савременим начином трговања на црном интернет тржишту, оне постају софистицираније и олакшано је извршење радње кривичног дела. Овај облик криминала је добио своју унапређену дигиталну верзију, то значи да се скраћује време и трошкови отварања „*shell*" компанија тако што се приступи тржишту које нуди легитимне податке потребне за отварање фиктивне компаније. Модернизација у пословању организованих криминалних група се може поделити на два облика.

Први облик представља само делимичну дигитализацију досадашњих криминалних радњи, тј вршења оног дела радњи које су олакшале традиционално „пословање" у одређеној мери. У овом облику криминалне организације задржавају своје изворно поље криминалног деловања и извора нелегалних прихода, део посла који преносе на „мрежу" зависи од унутрашње организације и „јачине" групе. У овом случају криминалне групе најчешће само перу новац помиђу *online* средстава, а примаран извор нелегалних средстава остаје исти (нпр. трговина наркотицима). Такође, као и већина људи у времену савремених технолошких достигнућа, криминалне групе користе *online* средстава за међусобну комуникацију и организацију.

Велики број истраживача ОКГ у дигиталном свету, као и институција намењених борби против *cyber* криминала, слажу се да традиционалне криминалне групе такође усмеравају своје активности ка Интернету, што им омогућава нове начине извршења злочина. Традиционални концепт организованог криминала, заснован на монолитним, хијерархијским и етнички заснованим групама које желе да зараде ослањајући се на мито

и насиље, може се сматрати застарелим. Дигитална технологија условила је мрежне облике организације и друге врсте колективних акција у *cyber* простору[93]

Други облик представља потпуну дигитализацију организованих криминалних група. У овом случају деловања криминалне групе се одвија искључиво на мрежи, што значи да су средства која је потребно „опрати" прибављена у дигиталном свету као производ *cyber* криминала или преваре. За разлику од првог облика који *online* средства користи у одређеним фазама криминалног деловања, у овом случају групе користе Интернет као средство и као „место" целокупног деловања. За разлику од традиционалних организованих криминалних група, ове организације немају вишегодишње трајање, хијерархију и остала обележја „класичних" криминалних група. С обзиром на не постојање хијерархије, не постоји „дон" који издаје наређења да се неки напад изврши, већ се особе које имају одређена знања из рачунарских технологија окупљају и користе своје вештине за извршење кривичних дела. Зависности од познавања стручне области чланови се групишу ради извршења заједничког циља, чиме остварују ланац деловања у којем је свака карика подједнако важна у испуњавању свог дела посла. Организовањем у криминалну групу ови појединци постају више деструктивни и у таквом систему међузависности унутар организације долазе до одређене врсте добити која је заједнички циљ.

Као што је већ наглашено, црна интернет тржишта си места на којима криминалци продају своје услуге и која остварују *online* криминалну економију у којој владају посебна тржишна правила. Појава ове економије довела је до експанзије броја криминалних група које нуде своје услуге на црним интернет тржиштима и доступне су свима у сваком моменту, без обзира у ком делу света се налазе њени чланови или корисници услуга. Организоване криминалне групе су у дигиталном свету постале флексибилније, софистицираније, делују са већом анонимношћу и не познају никакве националне и географске границе.

Битна карактеристика ових група јесте флексибилност у организацији, често се група формира само ради извршења једног напада, по завршетку се она расформира. За одређени напад се организују лица са потребном знањима и вештинама како би се успешно реализовао и постигла заједничка корист.

Софистицираност представља особину организоване криминалне групе која иде у корак са развојем технике и технологије. Ове групе се труде да буду корак испред регулаторних тела и алата који би потенцијално

[93] Ђукић, А. (2018) Организовани високотехнолошки криминал – појам, развој и основне карактеристике, Универзитет у Београду, Факултет безбедности.

спречили њихово деловање. Усавршавање комплексних криминалних метода и техника и њиховим пласирањем на црном тржишту, криминалци успевају да допринесу све већој појави *cyber* криминала.

Анонимност унутар организованих криминалних група у дигиталном простору је карактеристика која се ослања на претходну, омогућавајући члановима групе деловање без физичког контакт и непосредне комуникације. То посебно олакшава формирање и расформирање криминалних група у заједничком циљу. У *online* круговима, појединци користе псеудониме по којима се препознају и на којима граде своју репутацију од које зависи ангажовање у групи.

Транснационалност је генерална особина Интернета као глобалне мреже, поред тога што је олакшава свакодневно функционисање друштва, она олакшава и деловање криминалних група. Погодан амбијент који транс националност обезбеђује, довео је до тога да сви који су на „мрежи" могу бити угрожени, иако се налазе у некој удаљеној, развијеној и богатој земљи. Научне структуре се мало баве транс националним организованим криминалом у дигиталном свету, тако да поред дефиниције традиционалног облика у Конвенцији из 2000, године, нема пуно научника који се баве ближим одређивањем овог феномена.

Једна од постојећих дефиниција гласи: „Транснационална ОКГ која делује *online* је свака криминална активност коју намерно чине три или више особа са заједничком намером да стекну материјалну корист, стекну моћ или остваре друге нематеријалне интересе, где је почињено више кривичних дела и чланови групе делују заједно дужи временски период; информационо комуникационе технологије се користи као средство, а мета може бити Интернет или уређај повезан са Интернетом, или се Интернет може користити као инструмент за почињење кривичног дела или у вези са две или више држава."[94] Овакво дефинисање овог феномена може бити прихватљиво само ако се изузме сматрање да групе делују дужи временски период. Као што је већ наведено, Интернет као глобална мрежа ствара такав амбијент да групе могу веома лако да се формирају, а затим расформирају по завршетку криминалне радње, чиме знатно отежавају откривање и санкционисање од стране надлежних органа.

„У неким од већих случајева које смо имали,постоји основна група актера који се заиста добро познају, а који затим развијају помоћну мрежу људи које могу користити као *money mules* или за претварање информација које су добили у стварни новац" рекао је Томас Холт, професор универзитета Мичиген. Из овога се види да постоје и случајеви када се

[94] Li, Xianghia. (2015). Transnational Organized Crime in the Context of Internet.; University of Vienna, Vienna.

чланови групе међусобно познају, али због лакшег остваривања заједничког циља ангажују другу мрежу људи са посебним стручним знањима и могућностима. Холт је додао „С обзиром да се ствари премештају на дарк нет и користе криптовалуте и друге начине плаћања, хакерска понашања се мењају и постају све тежа за потпуну идентификацију и постаће све теже разумети нека од ових понашања“ [95]

У криминологији и кривичном праву Интернет заслужује посебну пажњу због својих главних карактеристика као што су глобални карактер, тренутна доступност и неограниченост, дигитални је и омогућава аутоматску обраду података. Ово пружа посебне опције за извршење дела *cyber* криминала у којима су рачунарске мреже циљ и важан алат. Интернет омогућава интеракцију између криминалаца и криминалних организација, а функционисање података о кривичним делима и финансијских података олакшава преваре, крађе и друге криминалне радње.[96] Стварна природа организације *cyber* криминала варира у зависности од нивоа укључености дигиталне и умрежене технологије, начина рада и циљних група жртава, што такође помаже у дефинисању разлика између њих.[97]

Потреба за различитим стручним вештинама на мрежи ће паралелно расти са развојем технике и технологије, то ће захтевати груписање „хакера“ ради остваривања заједничког циља. С обзиром да се све већи број средстава преноси у дигитални свет, логично је за очекивати повећање броја организованих група које ће деструктивно деловати и чије ће се последице осетити у материјалном свету.

Недостатак поузданих емпиријских података о организованом *cyber* криминалу уопште и даље доприноси његовом недовољном разумевању. Овом недостатку увелико доприносе и компаније које се баве продајом антивирус софтвера и других заштитних система. Такође, димензије *cyber* криминала су мало познате, углавном због виртуелности и „невидљивости“ деловања, сложености дигиталних трагова и отежане или немогуће сарадње жртава, као и ограничења спровођења закона у откривању и спречавању.

У уводном делу рада је већ речено да многе државе нису дуго желеле да признају постојање транснационалног организованог криминала, а ту је и проблем око различитог законског регулисања кривичних дела.

---

[95] https://www.sciencedaily.com/releases/2020/01/200116123805.htm приступљено 10.09.2020.

[96] Ђукић, А. (2018) Организовани високотехнолошки криминал – појам, развој и основне карактеристике, Универзитет у Београду, Факултет безбедности.

[97] Wall, D.S. (2017) Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing, University of Leeds, UK.

Исти проблеми у сузбијању овог облик криминала појављују се у његовој дигиталној пројекцији која му је дала могућност међународног прилагођавања, ради избегавања санкција. То значи да криминалне групе имају могућност да делују у сваком месту на свету које је покривено Интернет мрежом, а логично да ће бирати места где закон не одређује дату област, а самим тим смањују ризик од санкције.

4.9. Дарк веб и утицај на привреду

Дарк веб је дом „криминалне" економије и криминалних заједница. То је епицентар организационих ризика и ноћна мора за финансијска одељења широм света.

Да би схватили како опасности дарк веб утичу на привреду и како се одбранити потребно је схватити шта је то и како функционише.

Емили Вилсон, потпредседница истраживачког одељења *Terbium Labs*, наводи како је „дарк веб само још један део интернета. Али технологија која га подржава, омогућава већу анонимност, замагљивање корисника и свих ствари које су веома добре за приватност и сигурност, што такође значи да су веома добре и за криминалце. „

Веб претраживачи не могу да виде и пронађу дарк веб, за шта је потребан посебан анонимни претраживач под називом Tor.

„Број тамних огласа на мрежи који могу наштетити предузећу порастао је за 20% од 2016. године. Од свих огласа (осим оних који продају дрогу), 60% може потенцијално наштетити предузећима".[98] Треба напоменути да је овај проценат изражен према криминалним радњама које директно утичу на предузећа. Екстензивно гледано, јачање „криминалне" привреде директно је пропорцијално слабљењу легалне привреде. У случајевима криминалних радњи, које се одвијају помоћу дарк веба или на њему, када привредни субјекти нису директно нападнути и даље постоји опасност по друштвену привреду у целини.

Вилсон каже да би се две врсте података могле појавити на дарк вебу. Први су финансијски подаци - украдене платне картице, кредитне и дебитне картице, укључујући личне и корпоративне картице. Друга врста су стварни банковни рачуни, који су погодни за прање новца. Наставља да каже: „Ако тражите водич за корак по корак како отворити лажни пословни рачун и потом извршити пореску превару, дарк веб вам може помоћи у томе".[99]

[98] https://www.cimaglobal.com/Members/Insights/The-dark-web-and-finance-The-threat-is-real/ последњи пут приступљено 18.08.2020.

[99] https://www.cimaglobal.com/Members/Insights/The-dark-web-and-finance-The-threat-is-real/ последњи пут приступљено 18.08.2022.

Сбербанк, највећа руска банка, очекује да ће до 2022. године штета за глобалну економију која је изазвана *cyber* нападима износити између 8.000 и 10.000 милијарди долара, рекао је заменик извршног директора банке Станислав Кузњетцов.

Штета за руску економију проузрокована *cyber* нападима у 2018. години износила је 1.300 милијарди рубаља (19.6 милијарди долара), рекао је у Руској кући у Давосу, у оквиру Светског економског форума.

"Какав је тренд у погледу штете коју *cyber* напади наносе глобалној и руској економији? Нажалост, предвиђамо њен даљи раст", рекао је Кузњетцов.[100]

Иако се овде говори о свим *cyber* нападима, мора се разумети да нападачи теже интеграцији тих против правно прибављених средстава кроз различите облике прања новца. Одређена кривична дела извршена уз учешће дарк веба као *online* средства, сама по себи представљају кривична дела против привреде. Док се материјализација средстава проистеклих из *online* криминалних радњи које нису повезане са привредом на крају опет своди на неки облик кривичног дела против привреде.

Извештај водеће аналитичке компаније за крипто плаћања, *chainalysis*, показује да су *Bitcoin* трансакције на дарк вебу порасле са приближно 250 милиона УСД у 2012. години на 872 милиона у 2018. години.

Иако је укупан економски обим нелегалних веб активности и даље релативно мали, многи од најагресивнијих претњи друштву данас делују у сенци мреже Тор и тиме заслужују пажњу међународних регулатора, финансијских институција и агенција за спровођење закона.[101]

На црним интернет тржиштима постоји велики број продаваца који нуде власничке папире заједно са матичним бројем послодавца познатим и као порески идентификациони број. Матични број послодавца је јединствен, деветоцифрени број који се додељује пословним субјектима који послују ради отварања банковног рачуна или подношења пореских пријава.

Један продавац нудио је власничке папире и матични број фирме за око 1.600 америчких долара, док је други продавао матични број фирме и оснивачке акте (статут) за око 800 америчких долара. Под условом да такве информације изгледају или јесу довољно легитимне, *money mules* могу отворити пословне рачуне у банкама, омогућујући им да преносе

[100] http://balkans.aljazeera.net/vijesti/steta-od-cyber-napada-do-2022-godine-10000-milijardi-dolara? последњи пут приступљено 20.08.2022.

[101] https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm последњи пут приступљено 20.08.2022.

веће количине новца на рачун и са рачуна без привлачења нежељене пажње на своје активности[102]

Дигитализација друштва омогућава лакши приступ овим мрежама и олакшава прихватање код све већег броја људи. Поред дигиталне трансформације друштва која је условљена развојом технике и технологије, Дарк веб је један од главних алата који су олакшали дигитализацију великог броја криминалних радњи, и развијања нових кривичних дела.

Неоспорна је чињеница да су организоване криминалне групе (ОКГ) главни организатор и носилац активности илегалних интернетских тржишта, која су све развијенија и организованија и са великим бројем чланова чији је број тешко проценити.[103]

Мушкарац из Њујорка оптужен је да се бави хаковањем рачунара, трговином украдених бројева платних картица и прањем новца.

Виталии Антоненко (28) оптужен је за неовлашћени приступ рачунарским мрежама и промету неовлаштених уређаја за приступ, те за прање новца. У марту 2019. Антоненко је ухапшен и задржан због оптужби за прање новца на њујоршком међународном аеродрому *JFK* након што је тамо стигао из Украјине, носећи рачунаре и друге дигиталне медије на којима су биле стотине хиљада украдених бројева платних картица.

Како се наводи у оптужници, Антоненко и саизвршиоци претраживали су интернет у потрази за рачунарским мрежама са сигурносним рањивостима које би вероватно садржале бројеве рачуна кредитних и дебитних картица, датуме истека и вредносне верификације картице (*CVV*) и друге личне податке . Они су користили технику хаковања познату као напад „*SQL* ињекција" да би приступили тим мрежама без ауторизације, извукли податке о платним картицама и друге личне податке и затим их продавали на дарк веб тржиштима. Једном када је суизвршилац продао податке, Антоненко и други су користили *Bitcoin*, као и традиционалне банкарске и готовинске трансакције за прање прихода, како би прикрили њихову природу, локацију, извор, власништво и контролу.

Оптужба за неовлаштени приступ и промет на уређајима предвиђа казну до пет година затвора и новчану казну у износу од 250 000 долара, реституцију и одузимање. Оптужба о прању новца предвиђа казну до 20 година затвора, новчану казну у износу од 500 000 УСД и реституцију и одузимање.[104]

---

[102] https://www.bankinfosecurity.eu/cybercrime-black-markets-rdp-access-remains-cheap-easy-a-13054?highlight=true последњи пут приступљено 21.08.2022.

[103] Ђукић, А. (2018) Организовани високотехнолошки криминал – појам, развој и основне карактеристике, Универзитет у Београду, Факултет безбедности.

[104] https://www.justice.gov/usao-ma/pr/new-york-city-man-charged-hacking-credit-card-trafficking-and-money-laundering последњи пут приступљено 22.08.2022.

Док је истрага против Антоненка, који је такође добио име „Сабе“, и остала два суизвршиоца вођена између 2015. и 2017., ФБИ сумња да су њих тројица наводно почели да се баве украденим бројевима дебитних и кредитних картица у 2012. години.

Истрага ФБИ-а такође се поклопила са истрагом америчке тајне службе неименованог сајта са дарк веба, који тргује украденим кредитним картицама и другим подацима, наводи се у оптужници.

Између 2015. и 2017. године тајни агенти почели су да купују стотине бројева *American Express and MasterCard*, као и друге податке, које је група наводно продала на овом дарк веб тржишту, наводи се у кривичној пријави. Ове куповине су углавном вршене у *Bitcoin* -у.

Као део истраге, агенти ФБИ-а су такође започели истраге трансакција које су настале и у вези су са дигиталним новчаником који је само идентификован као „новчаник А“, наводи се у кривичној пријави. Између 2013. и 2017. овај дигитални новчаник био је укључен у више од 575.000 засебних *Bitcoin* трансакција у вредности од 23 милиона долара, наводи се у кривичној пријави.

Агенти ФБИ-ја почели су пратити *Bitcoin* трансакције групе између 2015. и 2017. путем *blockchain-a* повезаног с дигиталним новчаником. Истражитељи су на крају утврдили да овај новчаник садржи око 19.000 *Bitcoin* адреса које наводно користи група, наводи се у судском документу.

ФБИ је утврдио да су Антоненко и други користили виртуалну валуту како би сакрили профит од наводних активности украдених података о кредитним картицама, а затим опрали те приходе кроз дигитални новчаник продајом *Bitcoin-a* по ценама од 9% до 10% испод тржишне вредности. Ово је ефективно помогло у прању илегалних добитака, наводи се у кривичној пријави.[105]

У овом случају се јасно види повезаност *cyber* криминала и привредног криминала (прање новца). Сама „*SQL*“ техника не захтева „наивност“ корисника као што је случај са *phising*-ом или *pharming*- ом, због тога је у овом случају изостала „дигитална“ превара иако постоји реална могућност њене употребе за прибављање личних података. Крајњи циљ ове криминалне организације јесте прибављање средстава која су имплементирана у легалне токове новца и њихово даље трошење на лагодан живот. Такође се види да је реч о великом броју трансакција у *Bitcoin*-у које су захтевале ангажовање већег броја људи који су обављали унапред организоване дужности. Субјекти који су куповали *Bitcoin* по нижим ценама од тржине су свесно учествовали у процесу прања новца, јер у „дигиталним“

[105] https://www.bankinfosecurity.eu/suspected-hacker-faces-money-laundering-conspiracy-charges-a-14359?highlight=true; приступљено 26.08.2020.

круговима тако смањена цена јасно означава неку врсту неправилности. У овом случају није могуће утврдити одговорност крајњих купаца, јер је проблем у утврђивању свесног умишљаја у учествовању у тим радњама.

Ова врста криминала је у експанзији и сходно томе се може приметити како се западне владе боре против њега. У овом случају су се у борбу укључиле две високо рангиране владине институције ФБИ и америчка тајна служба као крунска организација за безбедност. Озбиљност приступа овом виду криминала оправдава чињеница да његово откривање захтева одређено дигитално праћење и истрагу у дужем временском периоду ради прибављања доказа. Поред криминолошке природе, отежавајућа околност за истражитеље представља и сама технолохија *blockchain-a* која је дизајнирана тако да обезбеди анонимност.

5. Крипто-валуте

5.1. Појмовна одређења

Криптовалута подразумева „дигиталну или виртуелну валуту која је обезбеђена криптографским путем а што је чини скоро немогућом за фалсификовање или двоструко трошење“[106]. Друга дефиниција је да је Криптовалута облик дигиталне имовине која се користи као средство размене користећи криптографију (криптографија) као начин обезбеђивања сигурности трансакција, контроле стварања додатних новчаних јединица и ради потврде трансфера валуте[107]. Касперски их дефинише као: „било који облике валуте који постоји виртуелно или дигитално, а који користи криптографију у циљу обезбеђења заштите трансакција. Оне немају централно тело које их издаје, нити регулаторно тело које их контролише, већ уместо тога користе децентрализован систем за бележење трансакција и издавање нових јединица валута“[108]. Оне се сматрају обликом вредности за мерило и средство плаћања, међутим не у сваком смислу којим се изједначава са средством плаћања у смислу валута у платном систему, обзиром да се према прописима сваке државе, појединачно, тумачи шта се подразумева или сматра средством плаћања на одређеном простору, територији одређене суверене државе. Технологија иза крипто валута зачета је одавно али представљање у функцији актуелног схватања крипто-валута доживели смо од стране лица под псеудонимом Сатоши Накамото - под којим се може подразумевати одређена група непознатих аутора. Тада је уведен концепт тзв. Блокчејн заснованог уговора [109]. У питању је представљање верзије електронског новца – биткоин, који користи криптографију у циљу омогућавања директног пир-ту-пир (П2П) плаћања – (исплата и уплата) у циљу елиминације посредника у економским трансакцијама. Према другој

[106] LION DC project is funded by the European Union's Interna Security Fund — Police, under LION DC WP4 grant agreement no 822616.

[107] https://sr.m.wikipedia.org/sr-ec/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%83%D1%82%D0%B0 упоредити са https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html?sh=2ab1e3f3353e последњи пут приступљено 05.10.2022.год.

[108] https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency последњи пут приступљено 05.10.2022.год.

[109] Ducas, E., & Wilner, A.S. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. International Journal, 72, pp. 538 - 562. P.544.

дефиницији[110] крипто-валуте представљају сваки облик валуте који постоји дигитално или виртуелно и користи криптографију у циљу обезбеђивања трансакција. Два су термина који се морају дефинисати П2П и криптографија, како би се разумеле претходно приказане дефиниције.

П2П (P2P) односно peer to peer је „модел комуникације путем интернета, пандан клијент/сервер моделу, најчешће у употреби за дељење датотека. P2P је скраћеница од (енгл. peer to peer) што би се могло превести као једнак једнаком (или вршњак вршњаку)“[111]. Дакле у питању је облик комуникације на нивоу истих прерогатива и нивоа. Описано постоји „у случајевима мрежног окружења у којима сваки рачунар може деловати као сервер другима и као клијент омогућавајући тиме приступ свим датотеткама и периферијама без потребе за централним сервером“[112]. „P2P је технологија која је развијена за размену података између корисника путем интернета као мреже. Са P2P клијентима базираним на Gnutella протоколу, корисници са компатибилним софтвером могу креирати фајлове на својим хард-дисковима, конектовати се на P2P сервис, а потом лоцирати, приступити и разменити жељени податак. Сваки вршњак (peer) резервише део својих ресурса (процесор, HDD меморија, пропусни опсег мреже) којима остали вршњаци могу директно приступити. На овај начин се избегава повезивање вршњака преко сервера. Вршњаци су и снабдевачи и потрошачи ресурса, за разлику од класичног клијент-сервер модела где сервери само снабдевају, а клијенти користе ресурсе. Не постоји централизована услуга или хијерархијски унутар саме мреже. Овакве мреже су ефикасније у коришћењу ресурса али су и подложне системским грешкама[113]. Сви вршњаци сви су једнаки у привилегијама и овлашћењима али такође деле и терет одговорности пружања услуга. Ови облици комуникационих мрежа могу бити: централизоване, децентрализоване, структуриране, неструктуриране и хибридне. Овај облик мрежног дељења први пут је представљен јавности 1999 у САД – студент Шон Фанинг (Shawn Fanning) који је тада креирао сервис

[110] https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency последњи пут приступљено 20.09.2022.год.

[111] https://sr.m.wikipedia.org/sr-ec/P2P_%D0%BC%D1%80%D0%B5%D0%B6%D0%B0 последњи пут приступљено 20.09.2022.год.

[112] https://support.google.com/websearch/answer/10106608?hl=en приступљено 20.09.2022.год.

[113] Енциклопедија британика: https://www.britannica.com/technology/P2P последњи пут приступљено 20.09.2022.год. Упоредити и са Ивановић, З. Криминалистички аспекти високотехнолошког криминала, КПУ, Београд, 2021, стр. 165 и 247.

НАПСТЕР. Примена код криптовалута уз ширење различитих типова датотека за дељење у оваквим мрежама и даљу децентрализацију мреже. Протоколи П2П су по својој природи отворени, они позивају према сопственом дизајну свакога да се укључе, у јавним мрежама буквално свакога, у приватним вршњаци су познати али могуће је да има оних који нису добронамерни. Начин за спречавање злоупотреба своди се на прихватање консенсуалних протокола.

Два су општа типа протокола – механизама консензуса, први – Накамото консензус, и други Византијски принцип толеранције грешке (Byzantine Fault Tolerance (BFT)). Први, Накамото подразумева избор насумично изабраног лидера, вође, путем „лутријског", математичког, алгоритма (у којем „мајнери" по принципу математичког погађања, или састављања математичке слагалице, верификују догађај у мрежи) путем[114]:

- Доказа о раду *Proof-of-Work (PoW)* (Bitcoin, Ethereum до скоро -16.09.2022. – прешао на POS)
- Доказа о протеклом времену - *Proof-of-Elapsed-Time (PoET) (Hyperledger Sawtooth)*
- Доказа о учешћу - Proof-of-Stake (Ethereum CASPAR) – најчешће адекватан за оптворене, јавне мреже

Други БФТ подразумева многобројне и вишеструке рунде гласања мешу члановима у циљу постизања консензуса. Пример протокола Tendermint, ли погледати такође и

- Рипл протокол консензуалног алгоритма - Ripple Protocol Consensus Algorithm (RPCA) (Ripple)
- Федеративни византијски споразум *Federated Byzantine Agreement (Stellar)* адекватан за затворене (приватне) мреже

Као мотивација за активност ових учесника одређена је по правилу накнада у виду новокреираних криптовалута – као награда за верификацију која је извршена прецизно и ажурно, други разлог и карактеристика ових активности у циљу верификације и валидације јесте децентрализовани консензус[115].

Једна од тих мрежа, већ помињана, је криптовалута биткоин која нуди децентрализовану мрежу са књиговодственом датотеком – лецером о остваренима трансакцијама.

[114] Philipp Hacker, Chris Thomale: Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law, European Company and Financial Law, 2018, pp. 645-696, p. 653.

[115] *Ibid.*

Криптографија[116] као термин обухвата (из античког - грчког: κρυπτός, романизованог облика: kryptós „сакривен, тајан"; и γράφειν graphein, „писати") примену и проучавање техника обезбеђивања комуникација у присуству непријатеља. Општије она обухвата креирање и анализирање протокола који онемогућавају трећа лица или јавност да се упозна са садржином порука које се преносе путем приватне мреже. Модерна криптографија (или криптологија) представља пресек, заједничку област, научних дисциплина математике, информатичких наука, информационе безбедности, електротехничког инжењерства, процесирања дигиталних сигнала, физике и неких других. Практична примена криптографије је честа у електронској трговини, платним картицама базираним на чиповима, дигиталним или крипто валутама, као и војној комуникацији. Под криптографијом се као релативни синоними јављају и енкрипција – која подразумева шифровање порука претварање читљивих порука у нечитљиви текст (шифровани текст) који се може прочитати само применом реверзибилног процеса – дешифровања (декрипција). Током времена ово се мењало – па се савремена криптографија значајано базира на математичким теоријама и науци о рачунарима – криптографски алгоритми су дизајнирани на претпоставкама рачунарске отпорности[117] чинећи такве алгоритме тешке за провалити практично за било ког противника. Раст криптографских техника и технологије уопште и све већа употреба у реалном животу довела је низа правних питања у савременим друштвима, капацитети криптографије за шпијунске активности довели су до тога да се поједине земље према криптографији одреде према криптографији као оружју или да јој ограниче или чак забране промет. Блокчејн технологија постаје све релевантнија у многим областима људског живота, производњи енергије, здравственим системима, едукацији, јавној државној служби, логистици, транспорту, па, чак, и у одређеним оквирима, предлагана у циљу анализе и надзора дистрибуције лажних вести.

Основне карактеристике блокчејн технологије подразумевају дистрибуирану технологију поделе књиговодственог стања трансакција[118]

[116] Погледати Ивановић, З, opus citatus, стр. 19, 86, 100, 212, 328 и 375.

[117] https://en.wikipedia.org/wiki/Computational_hardness_assumption

[118] Трансакција над базом података се састоји од јединице рада извршене у оквиру система за управљање базама података (или сличног система), такве да се третира на кохерентан и поуздан начин, независна од других трансакција. Трансакције над базама података имају две главне сврхе:

- Да омогуће поуздано извршавање јединица рада код таквих да је могућ опоравак од грешки, и да база података остаје конзистентна чак и у случају системских грешака, када се извршавање прекине (у потпуности или делимично) и многе операције над базом остану недовршене или са нејасним статусом.

(*Distributed Ledger Technology* ДЛТ) на П2П мрежи. Према одређеним мишљењима у оквиру информатичких наука развој информационе технологије ушао је у зрелу фазу у моменту када је омогућено премештање датотеке са једног на два или више рачунара – у питању је тзв. Меткалфов закон (*Metcalfe's law*) по којем је ефекат рачунарске мреже пропорционалан квадрату броја повезаних рачунара – који се одређују као чворови (нодови). Рачунарски нод представља активни електронски уређај повезан на мрежу и омогућава слање информација (података) путем комуникационих канала рачунарској мрежи. Појам ДЛТ први пут је употребљен од стране у извештају британске владе припремљен од стране групе њихових експерата[119].

- Да омогуће изолацију међу програмима који истовремено приступају бази података. Без изолације, резултати програма могу да буду погрешни.

Трансакција над базом података по дефиницији мора да буде атомична (енгл. atomic), конзистентна (енгл. consistent), изолована (енгл. isolated) и трајна (енгл. durable). Скраћеница која означава овај скуп особина је АЦИД (од почетних слова енглеских речи за ове четири особине).

Трансакције функционишу по принципу све или ништа, што значи да ће се јединица рада која чини трансакцију или у потпуности извршити над базом података или неће имати никаквог ефекта. Штавише, систем мора да изолује сваку трансакцију од осталих трансакција, резултати морају да буду у складу са постојећим ограничењима у бази података, и трансакције које су успешно извршене морају да буду забележене у трајној складишној меморији.

Сврха

Базе података и други системи за складиштење података код којих је интегритет података императив често имају могућности да раде са трансакцијама како би очували тај интегритет. Појединачна трансакција се састоји од једне или више независних јединица рада, од којих свака чита и(ли) записује податке у или из базе података (или неко друго складиште података). Када се ово дешава, обично је важно да сва обрада података остави складиште података у конзистентном стању.

Пример који илуструје коришћење трансакција је пренос новца са једног банковног рачуна на други. Приликом преноса новца долази до две одвојене акције:

- Извесна количина новца се уклања са једног рачуна
- Извесна количина новца се додаје на други рачун (не обавезно иста количина новца јер банка може да наплати провизију).

Уколико се догоди да услед неке грешке у систему (прекид везе, софтверска грешка, нестанак струје...) буде извршена само једна од ове две акције, долази до неприхватљиве ситуације. Или ће новац бити уклоњен са првог рачуна а неће лећи на други рачун (клијент на губитку), или ће новац лећи на други рачун а неће бити уклоњен са првог рачуна (банка на губитку). Да би се овакве нежељене ситуације избегле, користи се трансакциони систем који ће се постарати да или обе акције успеју или да ниједна не буде извршена.

[119] UK Government Office for Science (2016): Distributed Ledger Technology: beyond blockchain. A report by the UK Government Chief Scientific Adviser, London, UK, 2016.

Они су га дефинисали као облик базе података која се налази на више различитих локација, земаља или институција а која је, по правилу, јавна база података[120]. Подаци се у њој похрањују један за другим у временским континуалним низовима, нови подаци се похрањују само у оним случајевима када учесници у креирању базе постигну консензус о томе[121]. ДЛТ се везује за модерно схватање појма документ, почетни моменат је следећи: метод и безбедност верификације података представљају већу важност од формалних елемената самог документа - његовог самог садржаја. Приступ информацијама и превенција измене (путем чувања интегритета информација) су више важнији од документа *per se*.

Сама суштина документа јесте:

- Садржај информација које носи је константан и стабилан
- Могуће је репродуковати или пренети (трансферисати) информацију на други медиј (у контексту блокчејн технологије њега представљају други рачунар или мрежа) на такав начин да се његова суштина не промени.

У случају ДЛТ-а верификација или валидација података дешава се кроз информациони систем, аутоматски, заснован на криптографији и заптити података. Информације се одобравају (потврђују) након верификације од стране учесника у мрежи (а то су чворови (нодови), нпр. учесници – популарно прозвани „мајнери“ за рачунарима који конституишу мрежу) који су за верификацију података овлашћени.

Блокчејн јесте кованица од две речи блок (block) што је најприроднија реч коју смо усвојили – блок и чејн (chain) што значи ланац. Ова технологија подразумева концепт заснован на коришћењу криптографски заштићеном ланцу трансакционих блокова. Трансакције су спаковане у блокове а блокови су везани у ланац. Блокови су повезани криптографски путем хеш[122] функције. Криптографска хеш вредност користи се као

[120] *Ibid.*

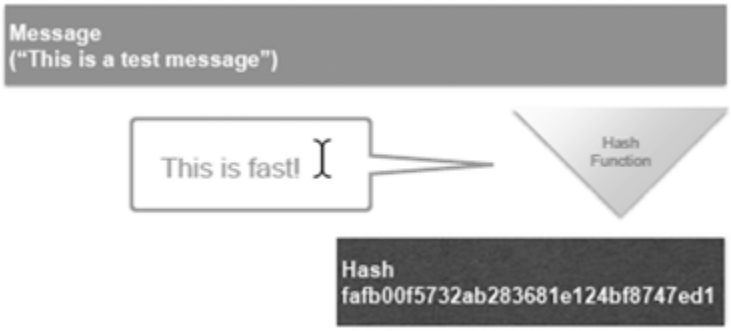
[121] *Ibid.*

[122] Хеш (хеш вредност) представља математичку вредност, која се односи на кратак низ фиксних дужина а који представља скраћени облик дугог низа (чексума). Веома често ово се описује као процес који одговара процесу млевења меса – када са једне стране машине за млевење меса убацујемо парчиће меса продукт не личи ни у ком случају на оригинални извор али се одликује јединственим садржајем, такође није могуће остварити реверзибилни процес. Хеш функције се првенствено користе за генерисање фиксне дужине излазних података који се понашају као референце на оригиналне податке. Хеш функције представљају основни принцип за ПГП алгоритам за валидацију података. Такође се користе да би се убрзало тражење ставки у базама података, детектовање дуплираних или сличних вредности у великом фајлу и проналажење сличних сегмената у ДНК секвенци.

безбедносни механизам у блокчејн технологији. Криптографска хеш функција одређеној поруци (било ком облику података) додаје случајан (произвољан) али коначан број и приказује хеш вредност фиксне величине. Илустрација функције је следећа.

Ф (порука) = Хеш
Ф (бибер, порука)| = Хеш

Погледати и илустрацију бр.1. Добра хеш функција је:
- Лака
- Неповратна (иреверзибилна), и
- Јединствена.



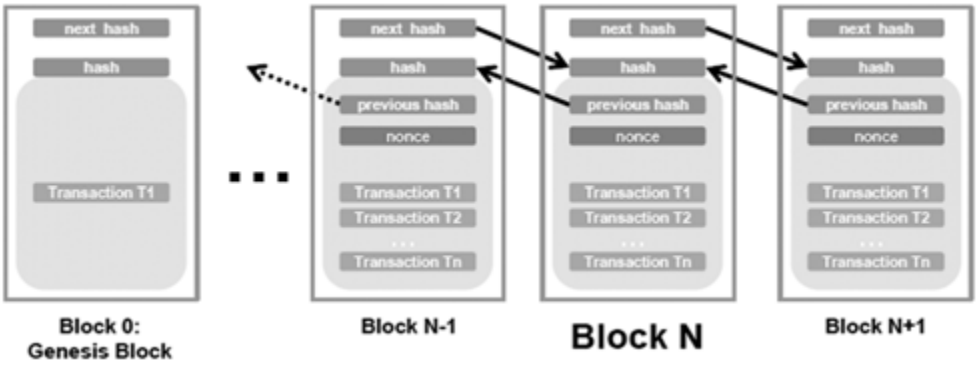
Слика бр. 22. Процес пребацивања порука у хеш вредност

Уколико се нека од вредности у оригиналној садржини документа који представља документ заштићен овим путем (оригинални садржај података у трансакцијама у блокчејну нпр.) одговарајућа хеш вредност се онда такође мења. Хеш вредност се користи за упоређивање и утврђивање чињенице да ли је дошло до измена у садржини заштићеног документа.

Требало би напоменути да криптографске хеш функције пружају могућност да се теоретски не могу пронаћи две исте поруке са истим хеш

Хеш функција треба да буде детерминистички одређена, тј. када се два пута позове над идентичним подацима (нпр. две ниске које садрже потпуно исте карактере), функција треба да произведе исту вредност. То је од кључног значаја за исправност готово свих алгоритама на основу хеширања. Хеш функције обично нису инвертибилне, што значи да није могуће реконструисати улазну вредност x само из њене хеш вредности x(x). У многим апликацијама уобичајено је да се неколико различитих вредности слика у исту хеш вредност и то стање зовемо хеш колизијама. Ови судари могу изазвати забуну међу објектима, што може допринети да алгоритми раде спорије и да буду мање прецизни. Хеш функције су дизајниране тако да се што више смањи вероватноћа судара. За криптографске намене, хеш функције су пројектоване на такав начин да је немогуће реконструисати било какав улаз само из хеш функције, без трошења великог рачунарског времена.

вредностима. Међутим ово ипак зависи од многих околности. Актуелни стандарди обухватају стандарде хеш алгоритама који носе ознаку СХА 2. Сви претходни стандарди не могу постићи ниво овог садашњег стандарда у могућности шифровања и опасности од дешифровања, као овај[123].



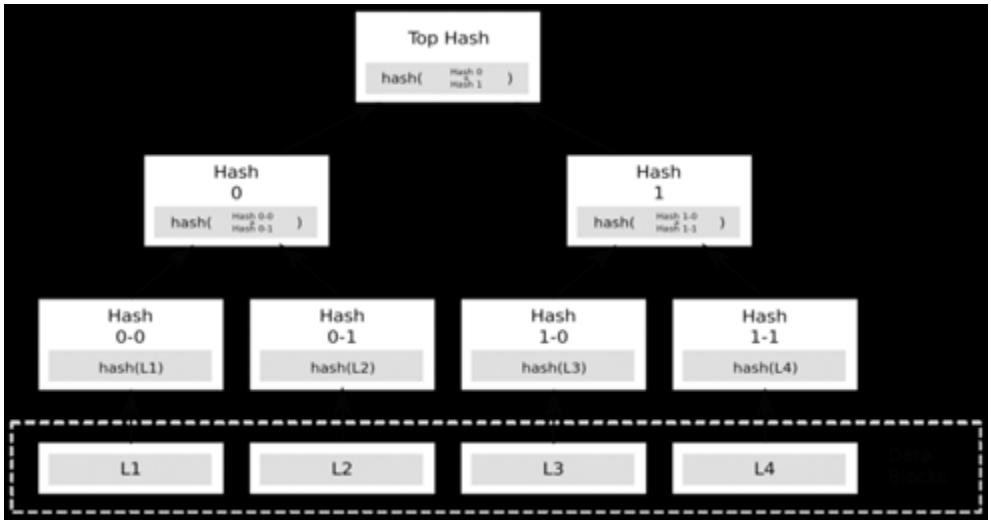
Слика бр. 23. Приказ изгледа блока са трансакцијама, насловима и хеш вредностима

У блокчејн технологијама подаци о трансакцијама претварају се у хеш вредност (просто им се додељује путем математичких функција адекватан облик хеш вредности која је непроменљива док се са оригиналним подацима ништа не ради) и похрањују се заједно са њима у блок. Нови подаци ће у суштини бити у форми блока са хеш вредности, узимајући у обзир и хеш вредности података из претходних блокова (који већ чине део ланца) Уколико хеш вредност није у складу са претходно описаним подацима из низа претходних блокова не може се верификовати, последично исто не може бити део блокчејна у питању. Блок се састоји од наслова и података о трансакцијама.

- Указује на претходни блок у ланцу (нпр. кратку комбинацију слова везану за одређени сет података - хеш)
- Временску одредницу која индикује време уношења блока у ланац блокова и
- Хеш дрво или „меркл дрво“ (погледати илустрацију бр. 3.) које излаже све трансакције укључене у блок[124].

[123] Више о томе на https://base.garant.ru/70414158/ или на https://en.wikipedia.org/wiki/Hash_function последњи пут приступљено 21.09.2022.год.

[124] Концепт хеш дрвета назван по Ралфу Мерклу (Ralph Merkle) који га је патентирао 1979. Ово дрво приказује структуру мреже у којој сваки екстерни корисник (назван нодом - чвором) бива одређен хешом; сваки други чвор који се грана даље садржи специфичну хеш вредност свих подчворова испод тог специфичног. Хеш гране омогућавају ефикасну и безбедну верификацију садржаја бројних датотека.



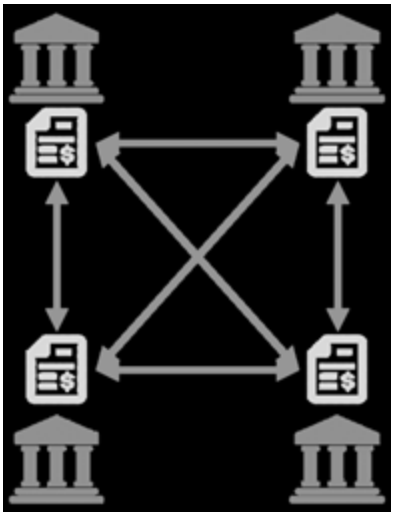
Слика бр. 24. Меркл дрво (Извор: Hash Tree, illustrated by David Göthberg, English Wikipedia, 20 August 2005)

Уношење хешева у наслов блока омогућава претраживања трансакција преко хешева као њихових препознатљивих знакова; према томе није неопходно да се читају сви подаци у блоковном ланцу (погледати и слику бр. 23.). У претрази наслов и гране Меркл дрвета су аутоматски читљиви. Разлика са претрагама у традиционалним хард копи књиговодственим евиденцијама јесте да ДЛТ функционишу као децентрализован систем; сваки учесник има своју сопствену копију или део регистра, идентичну са другим копијама осталих учесника (чворова) и сви виде исто. То такође подразумева да сви имају приступ свим подацима укљученим у дигиталну књиговодствену евиденцију[125].

Процес верификације података и обезбеђивање пристанка осталих учесника у блокчејну у вези уношења нових блокова информација врши се аутоматски. Након прибављања пристанка (одобрења) нови блокови се

[125] Верификовање дигиталних трагова кроз праћење у блоковима је идентично физичком књиговодственом праћењу, блокови функционишу аналогно као књиговодствени уноси дигиталног књиговође. Блокови су функционално исти као и папири, које користе svi učesnici како би унели трансакције и потписали их. Чинећи то, на тај начин, они пружају ауторизацију свих претходних папирних трансакција. Овај се поступак наставља онолико дуго колико има трансакција и простора на папиру. Оног тренутка када се папир поопуни верификује се печатом, нове трансакције се бележе на новом папиру, оног тренутка када је попуњен папир и верификован на описан начин везује се са претходним папиром (обезбеђен потписом и печатом на ивицама претходног и наредног папира). Функционално говорећи идентична активност се остварује у оквирима блокчејн технологије.

региструј у ланцу и криптографски обезбеђују од стране оних корисника који су предузели претходне трансакције кроз повезивање актуелних блокова са ранијим блоковима. Ланац сачињен на овај начин је веома тешко изменити. Практично је немогуће уништити га због постојања веома великог броја копија истих скупова података (доступним у различитим блоковима). Описана технологија просто омогућава да се међу особама, лицима која се не познају оствари размена података, без страха да ће доћи до њене измене. Као основни постулат у вези са финансијским трансакцијама јавља се постојање потребе да одређено тело врши надзор над трансакцијама и учествује у верификацијама трансакција. Ово то чини излишним, јер према приказаном не постоји потреба за тим телом када то ради целокупна мрежа (или један њен значајан део) и таква евиденција има способност репродуковања без обзира на жеље било ког учесника у поступку.



Слика бр. 25. Шематски приказ начина одржавања аутентичности књиговодственог стања

Чињеница је да овако приказане карактеристике блокчејн технологије омогућавају неколико значајних елемената у безбедносном смислу у погледу финансијских трансакција. Оне просто:

- Обезбеђују праћење порекла
- Повећавају транспарентност активности
- Појачавају поверење

Криптографске хеш функције: јединствено идентификују трансакције, а уједно их и и штите – онемогућавајући измене у садржини података о таквим трансакцијама. Асиметричне енкрипције (асиметрично

шифровање) појачавају и имплементирају тајност и онемогућавају довођење у питање сигурности и тачности.

ciphertext = F(private_key, plaintext)
plaintext = F(public_key, ciphertext)

Док је симетрична енкрипција – шифровање – класичан и много мање поуздан модел овакав:

ciphertext = F(key, plaintext)
plaintext = F(key, ciphertext)

Слање поруке у оквиру асиметричне енкрипције у циљу прикривања такве поруке за доступност другим лицима подразумева постојање два сета кључева за дешифровање порука – јавних и приватних кључева, за свако лице. Па тако, на пример, особа А која хоће да пошаље поруку особи Б, мора своју поруку шифрирати јавним кључем примаоца поруке. Овако шифрирана порука може бити откључана само од стране корисника – особе Б, са њеним приватним кључем. Особа А може доказати да је управо и само она саставила дату поруку, потписујући је сопственим приватним кључем. А особа Б може верификовати тај потпис коришћењем јавног кључа особе А. Једино тако функционише овај систем асиметричне енкрипције.

П2П мреже обезбеђују у оваквим случајевима децентрализацију и толеранцију могућих грешака. У оваквом систему консенсуални протокол производи дистрибуирану валидацију блокова.

Могуће је и поред овако описаних карактеристика блокчејна усмерити активности недобронамерних активиста (хакера, хактивиста, пентестера и сл.) у правцу напада на описане структуре. Овакви напади су могући, али тешко изводљиви и мало вероватни. Такође могуће су и тзв. виљушке[126] али се у решавању проблема који креира овакав феномен пришло са практичног аспекта – дужи ланац се рачуна, да не би било даљих и већих проблема.

[126] Биткоин рачва, виљушка (bitcoin fork). Ланац трансакција је сталан и јасан. То значи да се обично не одваја. Реч виљушка или чак можда бољи термин рачва доста добро описује феномен. Ово је назив феномена у систему у коме се један велики ланац дели на два дела, а након раздвајања они настављају да раде и постоје независно један од другог. Након што је дошло до развоја рачве или виљушке, добијамо две из једне криптовалуте, јер сада постоје два ланца трансакција. То се десило 2017. године са највећом крипто валутом на свету - Биткоин. Ланац је био неподељен, али је почетком године добио грану, израчвао се. То није значило да сам Биткоин од тада не постоји. Он наставља да ради независно од било кога, према истим правилима као и раније. Међутим, тада се појавила још једна независна крипто валута која је добила име Биткоин Кеш. Дакле, за реч форк, превод веома добро карактерише суштину овог феномена.

У сумирању – блокчејн технологије подразумевају специфичан тип дистрибуираног облика књиговодствене евиденције (ДЛТ). Изграђени су на одавно установљеним технологијама: хеш вредностима, асиметричној енкрипцији, П2П мрежама и консензуалним протоколима. Блокчејнови се примарно састоје од листа трансакција, блокова који су повезани хеш вредностима. Консензус протокол типа – PoW користи се најчешће код актуелних криптовалута.

5.2. Историјски део

Током октобра месеца 2008. године чувени алијас Сатоши Накамото објавио је „вајтпејпр" (eng. *whitepaper*) о биткоину, са свим објашњењима блокчејн технологије, улогом у овој криптовалути и фактички целом свету обзнанио намеру иза биткоина и реално приказао увезивање неколико технолошких момената са другим реалним моментима финансијског тржишта правећи од тога револуционарно искоришћавање постојећих технолошких предности, са недостацима валутног тржишта и финасијских деривата кроз нуђење алтернативе реалним „фијат" валутама. Након овога и полаког развоја разумевања капацитета и домашаја, као и могућности овако креираног простора за примену финансијских и економских деривата у дигиталним областима и окружењу, сазрева схватање циљева и сврхе истих, па се већ у децембру 2009.год. „ископава или рудари (мајнује)" први блок „постајања" (*genesis block*)[127] а што представља реално први моменат реалне имплементације блокчејн технологија у сфери криптовалута у свету. Након овога, већ у мају 2010.год. остварена је прва светска јавна трансакција и купопродаја преко примене криптовалута када је купљена пица (две велике пице)[128] за износ од 10000 биткоина (у овом тренутку – 07.10.2022. у вредности од 23838786400.00 динара – да, 23 милијарде динара) који је тада вредео око 40 америчких долара (USD). Ласло Хајнец (Laszlo Hanyecz) је тада својих 10000 Биткоина (БТЦ) разменио на следећи начин, обзиром да биткоин није био признат као средство плаћања, понудио је локалним блогерима да му неко прими његових 10000 БТЦ а за узврат у размену тај неко купи две пице, што се и десило[129]. Већ девет месеци касније у фебруару 2011.год. биткоин стиче

[127] https://www.investopedia.com/terms/g/genesis-block.asp последњи пут приступљено 07.10.2022.год.

[128] https://www.ndtv.com/business/the-first-bitcoin-transaction-was-for-buying-pizzas-more-interesting-tidbits-inside-2512643 последњи пут приступљено 07.10.2022.год.

[129] https://www.ndtv.com/business/the-first-bitcoin-transaction-was-for-buying-pizzas-more-interesting-tidbits-inside-2512643 последњи пут приступљено 07.10.2022.год.

паритет са валутом америчким доларом – USD, што на тржиштима валута и нема неки одјек у том тренутку, али касније ће добити значајан ехо. Већ у новембру 2013.год. биткоин прелази вредност од 1000 USD, а 2015 у августу постаје апсолутни хит након помињања од стране Блумберга. Но, ово не утиче на неко потпуније и шире прихватање криптовалута као средства плаћања, првенствено од стране држава у свету и њихових банака постоји отпор који одражава неизвесност и неспремност за шире укључивање у такве финансијске токове са таквим дериватима. Већ 2017. године ово почиње да се мења, када нагло почиње раст фирми и економских и трговинских субјеката који почињу да прихватају криптовалуте као средство плаћања, првенствено биткоин. Те године у децембру биткоин достиже вредност од 19783,06 USD. Највећу вредност ова валута достигла је 12.11.2021.год. у висини од 64400,00 USD, да би у овом тренутку била на вредности коју смо поменули у динарима (19900 USD).

5.3. Типови блокчејна

Најважнија је разлика између јавних и приватних блокчејнова. Опструктивни утицај блокчејн концепта је везан за јавне блокчејнове. Јавни блокчејнови су потпуно доступни свима, базирани су на тзв. извору отвореног кода (*open source code*)[130] и софтверска решења су потпуно доступна и свима приступачна. Свако без ограничења личне или географске природе може инсталирати адекватан софтвер за рад са јавним блокчејном на сопственом уређају, запамтити у целости или фрагментима датотека, као и учинити њихове копије доступне осталим корисницима. У сваком случају трансакција ће бити прихваћена тек уколико се остали чворови или корисници сагласе за то. За приступ блокчејну нису неопходна права приступа, нити се она захтевају у било ком облику, и ни једно тело не управља блокчејном, он је у потпуности децентрализован. Јавни блокчејнови су по правилу децентрализовани. Нови блокови се верификују од стране целе мреже, и није неопходно да се оформи посебно тело за надзор операција. Према томе јавни блокчејнови су сигурни. Свако ко жели да измени податке у бллокчејну мора да добије дозволу од осталих корисника. Као резултат овога манипулација података у јавним блокчејновима је скоро немогућа[131].

[130] Извор отвореног кода је слободно доступан било коме, свако га може даунлоадовати мењати и дистрибуирати своју верзију у неограниченом броју копија. Не постоје накнаде за лиценце или било које друге рестрикције у коришћењу. Потпунију дефиницију наћи на: Open Source Initiative website: https://opensource.org/osd

[131] Пример за јавне блокчејнове најчешће представљају Биткоин и Етереум, али се овај последњи у последње време мења у систему (15.09.2022.).

Са техничког аспекта приватни блокчејнови су засновани на истој технологији повезивања блокова у ланце као и јавни, али постоје суштинске разлике. Приватни блокчејнови у власништву су централног тела (једне или више јединица). Власник може одлучити ко може приступити мрежи а ко не, његова функција је аналогна са функцијом централног мрежног администратора. Приватни блокчејнови се користе када мрежа садржи поверљиве податке, последично активности на књиговодственом делу захтевају ауторизацију администратора. Могућност да одређена особа користи приватни блокчејн уобичајено произилази из споразума закљученог између самих корисника. Приватни блокчејн се користе често, али не и увек у пословима са лукративним карактером. Ови облици блокчејна нису по правилу децентрализовани, суштински у питању је криптографски обезбеђен дистрибуирани облик књиговодствене евиденције (ДЛТ). За сврху остваривања трансакција за учеснике у мрежи ипак је неопходна трећа страна – мрежни администратор.

5.4. Блокчејн као концепт без потребе за поверењем

Као што је већ објашњено овај концепт нема потребе за питањем поверења, као што је то случај у банкарским трансакцијама – поверење је препуштено аутоматизму и сигурности система блокчејн концепта. Стране ступају у правне односе без оптерећења и ослањају се на принцип *bona fides* према којем се очекује да стране морају у доброј вери поступати у складу са правилима правног посла и принципа који он са собом носи. Овакви услови везују се и произилазе из пословног угледа доброг привредника, али података из јавног регистра или личног убеђења. Вера у солвентност и сигурност у остваривању противуслуге или узвратне облигације представља централну тезу традиционалног облигационог права. У овом случају није неопходно да постоји оваква вера у сигурност узајамне облигаторне активности, техничке могућности похрањивања описаних неизмењених података на централизован и свима доступан начин ово чине ирелевантним. Просто, технологија представља сигурносни аспект у оваквим односима а сам систем блокчејна није зависан од било ког чвора посебно. Као резултат описаног код јавних блокчејна искључивање посредника (који врло често у реалном животу значајно наплаћују овакве услуге превалујући цене коштања сопствених активности на кориснике, чиме остварују значајно већи профит) може у финансијским трансакцијама учинити банке небитним, и потпуно их искључити из једначине, али не и у случајевима приватних блокчејнова. Код приватних блокчејнова концепт без потребе за поверењем нема адекватну имплементацију

– обзиром да се учешће у њима условљава дозволом или испуњавањем одређених услова. Њима се оперише од стране ограниченог броја учесника мреже, према заједнички дефинисаним правилима, где је у том случају концепт поверења заснован на затвореној заједници учесника који су иницирали приватни блокчејн. У овом случаје се не говори о концепту без потребе за поверењем већ се појединачним лицима поверава ова улога гаранта и поверење се везује за то лице.

5.5. Питање паметних уговора код блокчејн технологија

Паметни уговори представљају другачији појам од блокчејнова али су ова два термина веома повезана. Паметни уговор представља блокчејн базирани рачунарски програм (низ алгоритама и пратећих елемената на неком програмском језику - софтвер) који спроводи аутентификацију, омогућава и имплементира уговорне норме садржане у програмском коду – софтверу. Заснован је на криптографском процесу који омогућава примену правних послова – уговора, у случајевима када су испуњени услови предвиђени програмским кодом. У складу са споразумом (сагласношћу воља) који су усвојиле стране у уговору паметни уговор аутоматски испуњава обавезе (облигације) предвиђене њиме. Оног тренутка када се паметни уговор унесе у блокчејн (у облику програмског кода - софтвера) уговор може бити испуњен и активиран у складу са учитаним програмским кодом. Основна сврха примене паметних уговора јесте да се уговорни однос учини ефикаснијим и економски одрживијим, али и олакшају активности странака у уговору, са мање могућности прављења грешака, одлагања или спорних елемената. Тежи се томе да се уговорне стране не баве тривијалним елементима правног посла, а да *essentiallia negotii* буде што је могуће потпуније и правилније остварен. Кључна карактеристика паметних уговора јесте то да се они могу приказати у форми софтвера – рачунарског, програмског, кода и да се могу извршити аутоматски – рачунарским системом, зато се они разликују од традиционалних уговора, који се уобичајено склапају путем преговора, писаних аката (када је то обавезни елемент уговора) и конклудентних радњи. Паметни уговори су само-примењујући и само-активирајући рачунарски програми засновани на програмским алгоритмима[132].

[132] Predrag Cvetković, Liability in the context of blockchain-smart contract nexus: introductory considerations, UDK: 347.4:[004.7:336.74 004.7 336.74, International Scientific Conference „Responsibility in the Legal and Social Context", held at the Faculty of Law, University of Nis, on 18 September 2020, pp.82-100. p.90.

Основне карактеристике паметних уговора су:

1. Паметни уговори креирају се путем програмирања уз коришћење отвореног извора кодирања, њихова стандардизација и извршење је скоро потпуно без трошкова чиме се смањују уговорни трансакциони трошкови
2. Они умањују маневарски простор за двосмислено или апстрактно тумачење чиме се увећава ефикасност реализације уговорних обавеза; оног тренутка када су се стране усагласиле око садржине одредаба уговора програмски код извршава те одредбе без могућности да дође до доцње или неадекватног и непотпуног извршења уговорних обавеза.
3. Они су дизајнирани да функционишу без посредника (у децентрализованом формату)
4. Они су само-извршавајући програми, нарочито у блокчејн технологија која за циљ има да обезбеди странкама да остварују аутоматске трансакције; извршење може бити засновано на подацима из програма или подацима прикупљеним из окружења у којем се трансакција одиграва; паметни уговори свој безбедносни аспект црпе из блокчејн инфраструктуре (велики број чворова): на пример, није могуће реализацију трансакције зауставити од стране индивидуа или група корисника, осим уколико то није посебно унето у програмски код.

Паметни уговори, као и у случају учесника у блокчејну носе са собом обавезу, на коју корисници пристају, плаћања одређене накнаде за прерачунавање и рачунарске – електронске операције извршене од стране децентрализоване виртуелне машине (рачунарског система) блокчејна за паметни уговор[133].

Паметни уговори се могу комбиновати како би омогућили креирање инвестиционих средстава која аутоматски извршавају инвестиционе одлуке налогодавца, како у виду слања исплата инвестиционом адресату тако и за дистрибуцију зараде. Ово и јесте циљ најпознатијег од свих паметних уговора који је смисао имао у иницијалној понуду валута – новчића криптовалуте (ИЦО) – " ДАО" паметног уговора. Апстрактније објашњено власништво над одређеним облицима својине, овлашћење на примену својинских права може се повезати са токенима дистрибуираним путем блокчејна. Овако је могуће различитим облицима робе – аутомобили, некретнине, акције, гаранције банака и сл. управљати и

[133] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder: Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction (Princeton University Press, 2016) ch 10.7.

преносити их путем паметних уговора[134]. Могуће је разликовати три типа (архетипа) токена.

ДАО тип је још 2016.године настао у Берлину смишљен да служи као дистрибуирано инвестиционо средство. Инвеститори су били у могућности да шаљу етереуме и добију заузврат токене ДАО – а, који су има давали права предлагања путева инвестиција тако прикупљених средстава у дугим блокчејн базираним инвестиционим пројектима, пружајући тако право гласа у вези са таквим предлозима, али и могућностима учешћа у подели профита који се таквим инвестицијама остваре. Тада је непознати хакер успео да сифонира угрубо 1/3 фонда (који је достигао износ од 150 милиона Етера) који је том приликом остварен. Путем веома темељне и комплексне ванредне процедуре (тешка или тврда виљушка) девелопери језгра етереума успели су да поврате историју свог блокчејна и поврате средства инвеститора. Сама процедура указује на решења митигације ризика несигурних програмирања и њиховог убацивања у блокчејн. Овај напад је довео до шизме у Етереуму на мејнстрим Етереум и Етереум класик, чији следбеници сматрају да је хакер искористио правно перфектно недостатак (бубу) у паметном уговору и да се тако усмерена средства нису требала вратити инвеститорима[135]. У овом случају постоји, дефинитивно, приказ конфликтних подручја између закона и програмирања, која морају бити решавана на највишем нивоу – уз учешће интервенције државе. То се у случају САД дешава на начин тумачења ДАО токена као облика деоница, односно банкарских гаранција, те се на њих примењују правила која важе за гаранције и деонице, односно хартије од вредности.

Како је већ речено три су архетипа токена – валутни, средствени и инвестициони. Неки ИЦО се издају у циљу креирања нове криптовалуте, на пример код Етереум ИЦО корисници су могли за биткоине у ИЦО заузврат да добију етереуме[136]. Ови токени су издати у циљу функционисања као средство плаћања добара и услуга изван платформе. Другим ИЦО понудама токена се намеравало обезбедити функционално средство инвеститорима различито од платежносг средства за друге облике роба и услуга у сврху приступа продукту

[134] Hacker, Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Monetary Systems', Working Paper (7 July, 2017), in Regulating Blockchain. Techno-Social and Legal Challenges, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich, Oxford University Press, 2019, pp. 140-166 https://ssrn.com/abstract=2998830 (accessed on 25 October, 2022, at 13 et seq.; SEC Report, at 2 et seqq.

[135] Arvicco, 'A Crypto-Decentralist Manifesto' (Ethereum Classic Blog, 11 July, 2016), https://ethereumclassic.github.io/blog/2016-07-11-manifesto/ (accessed on 25 October, 2017).

[136] Narayanan et al. (n. 20) ch 10.7.

који су девелопери развили или развијају[137]. Кључна разлика са валутном је да се компонента средства нуди само као облик приступа са функцијом обезбеђеном и пруженом од стране издаваоца токена. Као илустрацију можемо навести ситуацију у којој валутна компонента токена омогућава држаоцу плаћање роба и услуга изван платформе, нпр. плаћање одеће на OpenBazaar – у. Токени се креирају на Етеруму на пример уз коришћење ЕРЦ20 стандарда, и у оквиру таквог система уносе се паметни уговори и стандардизују токенизацију таквих паметних уговора, типично садржавајући такав облик компоненте средства. Пример је фајлкоин (filecoin) који је најуспешнији ИЦО до сада издат 2017.год. прикупљајући 250 милиона[138]. Овај фајлкоин установио је децентрализовану мрежу простора за похрањивање података преко заузимања простора на рачунарима широм света. Држаоци токена троше токене за похрањивање и приступ (уз могућност повраћаја) подацима а рудари (мајнери) зарађују токене похрањивајући и сервисирајући податке. Многи други овакви коини су: Статус (Status), Банкор (Bancor), Парагон (Paragon) Етереум и сл. Трећи архетип је ситуација у којој издати токени у ИЦО – у имају инвестициону компоненту која подразумева имовинска својства која обећавају инвеститорима позитивне будуће приливе (крипто) валута.

5.6. Функционисање блокчејна у криптовалутама

Пластично објашњење функционисања блокчејн технологије у оквиру криптовалута је следеће: адресе треба разумети као нпр. провидне ормариће у које свако може пласирати криптовалуте – на пример биткоине кроз отворе за унос валута, међутим нико други, осим оних лица која поседују приватне кључеве, те уметнуте валуте не може подићи нити њима располагати. Ово подразумева да се велики број оваквих ормарића јавно налази доступно и видљиво свима, сви могу записивати и видети трансакције, чак и снимати исте а блок представља скуп више оваквих ормарића у низу и везују се „ланцем“ објашњеним хешом и информацијама о претходним и следећим блоковима. Књиговодствена евиденција која је овде присутна није ништа друго до регистровање стања, биланса и трансакција које су свима транспарентне и представљају заједничку и прихваћену евиденцију истог.

[137] Овакви токени се називају апликациони токени. Видети Rohr/Wright (n. 13) 8-24; on tokenization in general, see Van Valkenburgh et al., 'Distributed Collaborative Organisations: Distributed Networks and Regulatory Frameworks', Working Paper (2015), http://bollier.org/sites/default/files/misc-fileupload/ files/DistributedNetworksandtheLaw%20report,%20Swarm-Coin%20Center-Berkman.pdf, at 11 et seq.

[138] CoinSchedule, 'Cryptocurrency ICO Stats 2017', https://www.coinschedule.com/stats.php (последњи пут приступљено 28.09.2022.

Треба навести да је по правилу у евиденцији негде око 3500 трансакција по блоку. Величина једног блока у блокчејну је 4 бајта (*bytes*), хедер блока има 80 бајтова, број трансакција величине је око 1-9 бајтова док се листа или списак трансакција могу спаковати на величину до 2 мега бајта (MB). Трансакција представља трансфер вредности криптовалута која се објављује мрежи и сакупља у блокове – блокчејн технологије. Она представља:

1. Иницијалну намеру – интенцију која се објављује мрежи
2. Након тога трансакција мора бити валидирана:

a. Да ли постоје неопходна средства на располагању одређене индивидуе
b. Да нису ова средства већ пренета некоме другом

3. Рачунари у мрежи обрачунавају и валидирају (верификују, потврђују) ове рачунице (есенцијално у питању је низ различитих погађања од стране самог рачунара, док се не потврди тачан број)
4. Трансакција је прихваћена или одбијена од стране мреже

Како се креира биткоин адреса – просто – бира се насумични 256 – тобитни број и похрањује се на сигурном и безбедном месту. Ово може бити било који број и нема опсаности да га још неко поседује (има их више него атома у целом универзуму). Са овим 256 – тобитним приватним кључем креира се број уз помоћ елиптичне криве коју користи биткоин – ЕЦДСА (ECDSA) криве. Ту вредност онда провлачимо кроз СХА 256 хеш, а потом кроз РИПЕМД (RIPEMD) 160, још један алгоритам хеширања. Након тога конвертујемо резултат у Бази58 (Base58)[139]. Овоме се дода чексум[140] и након тога префикс и добијамо адресу[141].

[139] У нормалном свакодневном комуницирању користимо базу од 10 бројева а прикази различитих база дати су уз базу 58:

База	Карактери
2 (binary)	1
10 (decimal)	123456789
16 (hexadecimal)	0123456789abcdef
58	123456789ABCDEFGH JKLMN PQRSTUVWXYZabcdefghijk mnopqrstuvwxyz

[140] Чексум представља малу количину података који омогућава проверавање да ли је други део низа података онакав какав би требао бити (омогућава успостављање односа међу подацима које даље омогућава проверавање тачности таквог односа и након одређеног протека времена или додавања података на претходни низ).

[141] Одличан приказ дат је на адреси Graphical Address Generator (royalforkblog.github.io) последњи пут приступљено 11.10.2022.год.

Три су примарна типа биткоин адреса:

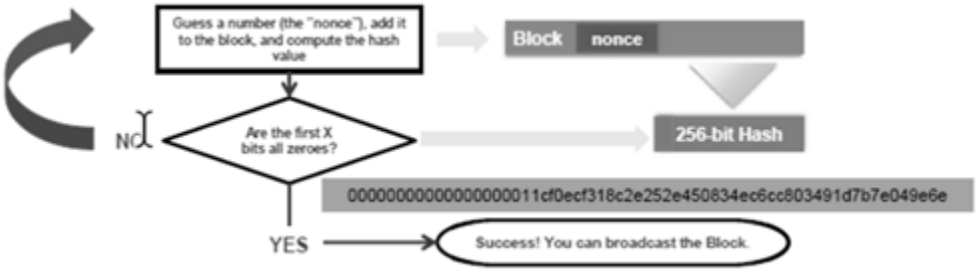
- P2PKH (Pay-to-Public-Key-Hash)
  - Стандардне трансакције
  - Један јавни кључ у трансакцији другом јавном кључу
- P2SH (Pay-to-Script-Hash)
  - имају захтеве који морају бити испуњени пре одвијаања трансакције
  - P2SH адреса почиње бројем 3
- Випеструки потписи (Multisignature)
  - Најчешће коришћени примери P2SH адреса
  - више од једног приватног кључа се захтева за одвијање трансакције
  - и адресе вишеструких потписа почињу бројем 3

У смислу разумевања животног циклуса трансакције неопходно је објаснити следеће (у случају биткоина): први корак подразумева отварање биткоин новчаника; други корак је проналазак адресе која је пријемна адреса валуте (адреса, на пример, продавца) на коју се уплаћају средства – износ криптовалуте; трећи корак је давање налога електорнском новчанику исплате одређеног износа биткоина на описану адресу, следећи корак подразумева потписивање трансакције уз коришћење приватног кључа у асиметричној криптографској енкрипцији; након тога се предузима мајновање (рударење) односно велики број компутација (обрачуна, рачунарских операција погађања) а затим се трансакција придодаје меморијском пулу новог блока; транаскција се тада пропагира – јавно пријављује мрежи на којој се мора валидирати мрежним чворовима; потом успешни рудар (мајнер) пропагира нови блок у мрежи; у следећем кораку чворови верификују резултат, а потом ве потврда трансакције видљива на мрежи, да би после све више конфирмација било учињено са сваким новим блоком.

Веома интересантно код трансакција јесте да се у њих могу у структурама описаним претходно уносити мале хекса-децималне поруке од којих је чувена она из 2009.године „"*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*"" међутим, иако су оне веома корисне у циљу идентификације држаоца или власника адресе, на велику несрећу свих заинтересованих превише је скуп као облик комуникационог средства, али ипак се тим путем може креирати изјава која ће бити свима доступна и представљати, на пример, легат лица које је желело да се његова изјава памти. Пример трансакције са идентитетом је: 6c53cd987119ef797d5adccd76241247988a0a5ef783572a9972e7371c5fb0cc. Ово представља серију микро-порука које креирају оруђе којим је могуће „свући" (даунлоадовати) датотеке Wikileaks-a.

5.7. Појмови од значаја код криптовалута а у вези са фунционисањем

Консензуални протокол доказа о раду (PoW) подразумева да је велики број чланова мреже вољан да валидира (проналази и верификује) трансакције. Мотивација која стоји иза овога је, по правилу, лукративна, први верификатор бива награђен за верификацију у одређеном номиналном износу криптовалуте. Бира се један по принципу случајног узорка да одлучује о следећем блоку. На овај начин ни један злонамерни учесник не може контаминирати блокчејн – зато што просто не може знати да ће бити изабран да пропагира сопствени блок. Ово је могуће, само уколико злонамерни учесници не преузму већину учесника мреже, а тада постоји вероватноћа која је значајна, да ће један од њих пропагирати следећи блок. Ово представља тзв. Сибил (Sybil) напад, којем је подложан PoW. Како иначе реално функционише PoW? Како је већ речено, не постоји начин да се реверзибилно инвертује хеш функција, а једини метод проналаска вредности уноса која одговара одређеном хеш критеријуму јесте применом метода претраге сирове силе (brute-force). Овај метод подразумева вишеструке покушаје погађања те вредности засноване на великом броју прорачуна – компјутација. Врло често овакав систем користи се у примени код PoW. Актуелни мајнери управо ово раде, поседујући велике количине рачунара са значајним, јаким конфигурацијама умрежених – увезаних у ригове са великим бројем графичких картица веома великих брзина (које имају и бржу ДДР 6 меморију на вишим тактовима) омогућавајући значајно брже прерачунавање и обрачунавање и пружајући могућност да се повећа вероватноћа могућности „погађања" вредности која се тражи. (Илустрација бр. 26). Мотивација се овде везује за време и новац који они улажу у поступак рударења – где се очекује награда или блок награда и накнада за погодак – верификацију трансакција.



Слика бр. 26. Илустрација PoW консензус протокола

Поред приказаног овај концепт има још неколико интересантних карактеристика. Првенствено, он за чланове мреже представља веома тежак посао, мотивација је проблем сама по себи. У једној великој мрежи момент

среће и успеха само једног успешног „мајнера“ може мотивисати, али како мотивисати све оне остале који, у том смислу, без опипљивог резултата тако тешко и дуготрајно раде? Једина могућност је увођење лукративног концепта за чворове који валидирају трансакцију и пронађу блокове награђују се путем нових токена које генерише мрежа, они примају делове тзв. трансакционе провизије. Из овог разлога они се одређују као „мајнери“ правећи алузију на рударе – који копају руду, одређујући парадигму као лукративни посао. У вези са овим је од значаја да се објасни и ситуација у којој може да се деси да два или више мајнера верификују исту трансакцију. Уколико су овако креиране верификације у консензуалном систему, па се скоро истовремено уведу два различита блока на различитим чворовима онда постоји ризик да постоје два конфликтна под-ланца. У таквом случају ланац који расте брже привлачи више рачунарских капацитета за који се генерише више нових блокова, за њега се претпоставља да је аутентичан, док се други расформира[142] а што се дешава на основу консезусних правила блокчејна. Сваки ажурирани ланац пропагира се и објављује од чвора до чвора а тачност и исправност новог блока се математички верификује од стране сваког чвора. Уколико се утврди да је одређени блок некомпатибилан са претходним елементом аутоматски се одбацује. Додатни проблем овог концепта јесте да се у систем који је описан на овај начин улаже огромна количина новца која све више није трошковно оправдана. На страну цене коштања ригова са све више прескупим компонентама, у питању је и значајна количина електричне енергије која се тим путем троши (илустрација бр. 6.), а поред очувања окружења и природе о којем нико не говори више, у питању су веома високе цене узроковане околностима рата у Украјини.

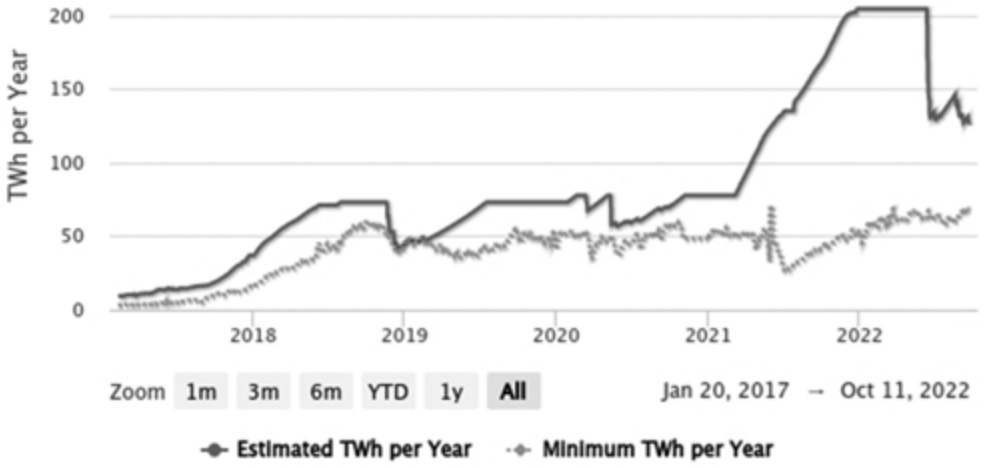
Тренутна процена је на 140 Терават часова што је целокупна потрошња нпр. Малезије или Шведске. Овај концепт више нема вредносну ефикасност, обзиром на скупоћу његовог експлоатисања. Ово јесте само један од разлога што неки облици криптовалута прелазе на друге концепте консензуалног протокола.

У вези са ризицима које криптовалуте носе интересантно размишљање уводе Дирксмајер и Сил[143] указујући на ризике на микро, мезо и макро нивоу. Први микро ниво постоји као ризик за најнижи ниво целог поступка, самог корисника имаоца криптовалуте и манифестује се у „ризику случајног

[142] Philipp Hacker, Chris Thomale: Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law, European Company and Financial Law, 2018, pp. 645-696, p. 654.

[143] Claus Dierksmeier и Peter Seele, Cryptocurrencies and Business Ethics, у Journal of Bussiness Ethics, Springer Science+Business Media Dordrecht 2016 и 2018 Vol. 152, No. 1 (September 2018), pp. 1-14 (14 pages).

брисања или губитка", нпр. код алткоина „губитак" је скоро ненадокнадив. Следећи ризик, који је значајно опаснији, микро левела јесу хакерски напади – у виду крађа нпр. алткоина, кроз неовлашћени приступ електронским новчаницима или дигиталним мењачким платформама. На мезо нивоу ризик долази од угрожавања највећих ланаца трансфера фиат валута (реалног новца) Western Union, MoneyGram и сличних. Њихов одговор још није потпуно видљив. Такође, због несталности криптовалута, у вредности и актуелности на таквом тржишту и других карактеристика овог облика валута оне не могу адекватно испунити неколико значајних функција стандардних валута укључујући нпр. гаранцију вредности у виду златних резерви или сл. На макро нивоу најпре су у питању ризици несталности мењачког курса, при чему исто подгрева шпекулације, а што води ка шпекулативним мехуровима на тржиштима нпр. Биткоина и даљим нестабилностима, са потенцијалом за нестабилан утицај на целокупни финансијски систем.



Слика бр. 27. Потрошња у Терават часовима (TWh) за продукцију Биткоина у последње четири године. (Извор: https://digiconomist.net/bitcoin-energy-consumption)

5.8. Криптоимовина

НБС дефинише у Србији, као референтна државна агенција – тело „Дигитална имовина, односно виртуелна имовина, означава дигитални запис вредности који се може дигитално куповати, продавати, размењивати или преносити и који се може користити као средство размене или у сврху улагања"[144]. Такође

[144] https://nbs.rs/sr_RS/ciljevi-i-funkcije/nadzor-nad-finansijskim-institucijama/digitalimo/ последњи пут приступљено 22.09.2022.год.

иста институција дефинише и виретуелну валуту као: „Виртуелна валута је врста дигиталне имовине коју није издала и за чију вредност не гарантује централна банка, нити други орган јавне власти, која није нужно везана за законско средство плаћања и нема правни статус новца или валуте".

Пружање услуга повезаних с дигиталном имовином уређено је Законом о дигиталној имовини (*Службени гласник РС*, бр. 153/2020) и подзаконским актима надзорних органа (Народне банке Србије и Комисије за хартије од вредности) донетим на основу тог закона. Народна банка Србије надлежна је за одлучивање у управним поступцима, доношење подзаконских аката, надзор над обављањем послова и остваривање других права и обавеза надзорног органа у делу који се односи на виртуелне валуте као врсту дигиталне имовине. Дозволу за пружање услуга повезаних с виртуелним валутама издаје Народна банка Србије.

Према дефиницији FATF препорука (*Recommendations*) ажурираних у октобру 2021[145] виртуелна имовина представља дигиталну референцу вредности којима се могу дигитално трговати, преносити и могу бити коришћене за плаћање у инвестиционе сврхе. Виртуелна имовина не укључује дигиталне облике фиат валута, хартија од вредности или других финансијских облика имовине.

Према једној дефиницији крипто имовине у појам улази размењива виртуелна имовина која применом криптографије бива и додатно обезбеђена неким дистрибутивним књиговодственим стањем.

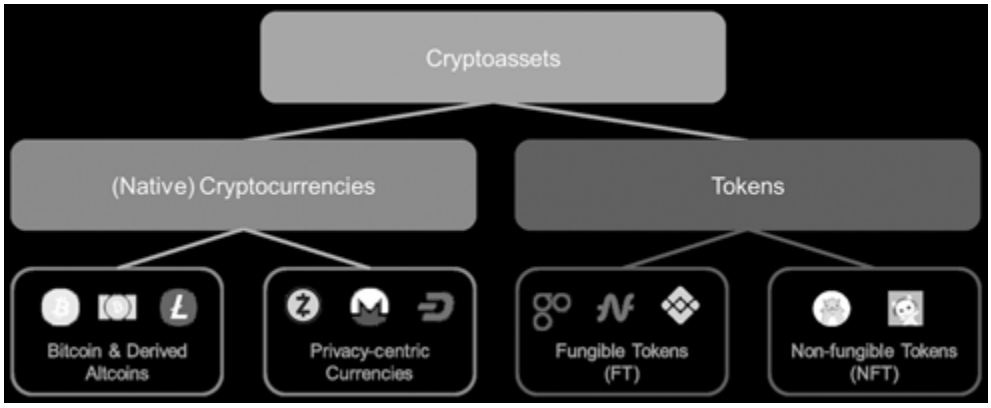
Као једна од подела чији је основ хијерархијско устројство одређена је ова (Слика бр. 28.) на криптоимовину, у које улазе примарне криптовалуте (а које се даље деле на биткоине и изведене алткоине, приватно – центричне валуте (монеро, зкеш, деш)) и токене (који се даље деле на нефунгибилне – неразменљиве (НФТ) и фунгибилне – размењиве (ФТ) токене). Поред описаних неопходно је поменути и нпр. лајткоин, верџ и ауроракоин, од којих први, на пример, бива скоро идентичан са биткоином али процесира трансакције четири пута брже од биткоин мреже, други рекламира себе као сервис који нуди анонимне трансакције кроз прикривање транаскција кроз TOR[146] мрежу и трећи ауроракоин који је креиран као вид алтернативне валуте у циљу замене Исландске круне као званичног средства плаћања.

НФТ и ФТ у ери блокчејна додатни капацитети се искоришћавају увођењем размењивих и неразмењивих токена. Просто, када је једном вредност приказана у дистрибуираном финансијском књиговодственом

[145] https://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf последњи пут приступљено 22.09.2022.год.

[146] Видети Ивановић, З. Opus citatus.

стању блокчејна она се може пренети у било који облик токенизације било чега. Два су основна аспекта о којима се размишља код токена – размењиви и неразмењиви, дакле код размењивих – исти се могу мењати за било који други токен, док су неразмењиви јединствени. Фунгибилност се може превести угрубо као могућност да се дата замењива (генеричка) ствар замени неком идентичном – као код генеричких ствари. Нефунгибилни (неразмењиви) токени су уникатни – не може постојати ни један сличан њему. На пример то могу бити и дигиталне и физичке ствари као нпр. патике, авионска карта, диплома на одређено лице или имовина лика у дигиталној игрици. Ови НФТ омогућавају власницима да докажу своју својину над њима и сопствену аутентичност. Они директно омогућавају трговину на маркету и обезбеђују слободу да се верује (или не размишља о пореклу и могућностима злоупотребе у вези са пореклом продате ствари и стварног идентитета учеснику у поступку) јер се јединствен идентитет НФТ-а упоређује и потврђује од стране оригиналног издавача или услуге која проверава аутентичности.



Слика бр. 28. Хијерархијска структура криптоимовине

Јединствене или уникатне карактеристике НФТ-а су:

1. Недељивост – НФТ – и се историјски јављају као недељиви што им даје употребљивост и корисност.
2. Дефицитарност је једна значајна карактеристика НФТ – а која представља основ из којег црпе сопствену вредност. Иако софтвераши могу креирати колико год хоће облика имовине тако је у оквирима њихових моћи и овлашћења да ограниче број НФТ – а услед потребе за дефицитарношћу.
3. Јединственост – непоновљивост, НФТ-и морају према дефиницији бити неразмењиви и уникатни, уколико то не би били спадали би у другу

категорију токена. Метаподаци сваког НФТ – а представљају неизмењиви облик евиденције која пружа аутентичност овим облицима вредности.
4. Имовински атрибути – Власништво – они постоје на ДЛТ – у везујући се за одређени рачун – Оригинални креатори НФТ – а контролишу приватне кључеве тих рачуна на којима постоје НФТ – и и могу их пренети на било који рачун.
5. Транспарентност – из разлога што су ДЛТ децентрализоване и неизмењиве и где се издавања, трансфери и активности токена могу бити јавно верификовани – купци могу веровати и потврдити аутентичност специфичног токена.
6. Интероперабилност – НФТ – и се могу размењивати, продавати или куповати преко различитих ДЛТ – а уз коришћење децентрализованог моста или централизоване службе за размену.

5.9. Стандарди за НФТ – е

Постоје различити облици платформи на многим мрежама који се користе за израду и издавање НФТ – а. Они су по правилу интероперабилни, а што значи да се могу размењивати или се њима може, са релативном лакоћом, трговати на различитим ДЛТ – овима НФТ – ови се могу похранити у „новчаницима" (*wallet*) (које специјализовани трејдери (трговци) нуде као услугу у најближем смислу „портфолија" за хартије од вредности али се исти популарно називају новчаницима) и на тај начин користити за трговину на другим отвореним маркетима. НФТ маркети повезују њихове издаваоце са купцима. Постоје различити усвојени НФТ стандарди који егзистирају на многобројним блокчејн мрежама.

ЕРЦ-721

Представља токенизовани стандард првобитно предложен још 2017. год. и уписан на Солидитију (*Solidity*) на Етереум (*Ethereum*) блокчејну. Уз коришћење овог стандарда омогућава се кодирање са мање муке, предвидљивије и оно које се може вишесруко користити. Овај стандард је онај који најпре омогућава свакоме креирање јединствених неизмењивих токена за дигиталне колекције. ЕРЦ – 721 омогућава мапирање јединствених идентификатора адреса, које верификује поседник оваквих идентификатора.

ЕРЦ - 1155

Побољшани стандард верзије ЕРЦ – 721 који је добио верзију 1155, омогућава паметним уговорима операционализацију ФТ – а и НФТ – а. Са

овим токенским стандардом идентификатори представљају вишеструке имовинске класе. ЕРЦ – 1155 обезбеђује девелоперима (програмерима) да изврше значајно велике количине трансфера токена преко паметних уговора чиме се умањује притисак на мрежу и омогућава уштеда на трансакционим накнадама. Платформа ОтвореноМоре (OpenSea) недавно је развила репозиторијум за ЕРЦ – 1155 стандард.

Не – етереумски стандарди

Етереум мрежа сматрана је веома широко прихватајућим ДЛТ – ом за креирање и издавање НФТ-а. Али ипак, растуће накнаде и леклустер (*lackluster*) проблеми отерали су програмере према другим јавним ДЛТ – овима. Ове алтернативе нуде боље перформансе, ниже накнаде а чак и могућности токенизације НФТ – а без потребе да се користе спори или потенцијално лоши паметни уговори. На пример, Hedera омогућава корисницима – програмерима обогаћавање (*mint*) неизмењивих токена уз примену Хедера токен сервиса по попусту од 99% са карактеристикама које одликују могућност брзог преноса (мање од 3 секунде) са коначношћу (без чекања информације о блоку) и са мање трошкова (мање од $0.001 USD у hbar-има). Прави реални пример је Хедера корисник ИНФИНИТЕ бај СУКУ који је мигрирао са Етереума у циљу креирања НФТ – а ембедованих у физичке тагове (реалне ознаке) у циљу верификације аутентичности ретких патика и друге луксузне робе.

5.10. Долазећи НФТ стандарди

Фракциони НФТ – и, према данашњем увреженом схватању НФТ – и се схватају као ексклузивни, власнички атрибути, што подразумева да је купац НФТ – а уједно и једини власник. Овакво стање и статус НФТ – а представља потпуно супротно стање идеји предложене децентрализације ДЛТ – а. Обзиром на овако схваћене недостатке нове класе НФТ – а које се јављају на тржишту називају се фракциони неизмењиви токени – ФНФТ. Идеја која стоји иза пласмана ових токена јесте да се омогући свима да поседују фракцију НФТ – а. ФНФТ су практичнији и лакши за примену код виртуелне робе, али би им најадекватнија права употреба била у физичкој роби као нпр, уметнинама, традиционалним инвестицијама, сакупљачким узорцима. На пример, Хедера токен сервис омогућава издавање таквих токена који се даље могу поделити (фракционализовати) са деловима које поседују друга лица.

У последњих неколико месеци у 2022. години НФТ – и су постали значајно популарни. За примену и коришћење НФТ – а неопходно је поседовати децентрализовани софтвер који може издавати јединствене и дефицитарне

дигиталне објекте. Први пројекат који је иницирао неке активности на НФТ маркету био је CryptoKitties који је репрезентовао диготалне мачиће путем НФТ – а. Увођење НФТ – а може се кокристити за токенизовање имовинских вредности, дигиталних идентитета и много тога још. Најпопуларнији су:

Физички и дигитални облици сакупљачких колекционарских физичких и дигиталних ствари Могуће је токенизвати буквално све, омиљеног спортисту или јавну личност, такође се могу токенизовати класичне колекционарске ствари, као на пример -код филателије – поштанске марке, новчићи, значке и сл. Посебно је значајно у последње време токенизовање сакупљених елемената и игрицама – посебних оружја, оклопа, додатака на прикупљене ствари и материјале, на пример у игрици Fortnite, иако сама игрица не користи ДЛТ ни НФТ – е, а поједине игрице су чак промениле сопствену инфраструктуру како би омогућиле примену НФТ – а и размену елемената у оквиру игара. За све су заслужни стандарди ЕРЦ – 1155 па на даље. *TopShot* игрица омогужава размену преко ДЛТ и НФТ – а, такве платформе омогућавају корисницима куповину, продају и другу врсту размене преко других виртуелних машина уз коришћење НФТ – а или правог новца у дигиталном облику, или криптовалута. Посебно је интересантно укључивање комерцијализације виртуелних некретнина, нпр. *Decentraland*, *The Sandbox*. Дигитална или физичка уметност може бити интересантна за токенизацију – обзиром да НФТ омогућава фракционализацију права својине, односно својинских права. Могућност да се одређена физичка ствар претвори у облик крипто имовине са тренутном ликвидношћу, пружа невероватне нове хоризонте за коришћење. Више различитих платформи ово већ лини сурово реално могућим. *TOKO by DLA Piper,* пружа могућност власницима уметнина да своје радове продају преко НФТ – а, иза свега стоји Хедера токен сервис, који омогућава њихову трговину а токени репрезентују само дело.

5.11. Идентификација и сертификација

НФТ могу садржати јединствене информације програмиране унутар њих самих о роби или имовини, а што их чини идеалним за издавање идентификационих прерогатива, сертификата, чак и лиценци и квалификација. Јединствен документ или сертификација издата на блокчејну као један НФТ може се користити за израду медицинске документације, лични профил, едукативну историју, као и друге најразличитије атрибуте у виду дигиталних карактеристика а која се може даље предати појединцу чиме им се пружа потпуна контрола над њиховим подацима.

6. Шта је OSINT? – Појмовно одређење

Open source intelligence (OSINT) техника подразумева прикупљање података из тзв. отворених, односно јавно доступних извора, у циљу њиховог коришћења у обавештајне сврхе. Не постоји прецизан датум када се термин OSINT први пут појавио, међутим, као релативни појам вероватно се користи стотинама година за описивање чина прикупљања обавештајних података коришћењем јавно доступних ресурса. У новијој историји, OSINT је током Другог светског рата уведен као обавештајни алат од стране многих безбедносних служби, али са експлозивним растом Интернет комуникација и огромном количином дигиталних података које производи јавност широм света, OSINT постаје потреба за различите организације, на пример владине службе, невладине организације (НВО) и пословне корпорације, које почињу у већој мери да се ослањају на OSINT, а не на приватне и класификоване податке.[147] OSINT извори се разликују од осталих облика обавештајних података јер јавности морају бити легално доступни без кршења уставних норми које се односе на гарантована права и слободе, првенствено права на приватност, али и ауторских и сродних права. Ова разлика чини могућност прикупљања OSINT извора примењивим у различитим сферама, а не само безбедносним. На пример, предузећа могу имати користи од коришћења ових ресурса да би стекли сазнања о својим конкурентима, а да притом таквим активностима не крше правила која се односе на нелојалну конкуренцију и економску шпијунажу.

Министарство одбране Сједињених Америчких Држава, OSINT дефинише као *„обавештајне информације које се производе од јавно доступних информација и прикупљају се, користе и благовремено дистрибуирају одговарајућој публици у сврху испуњавања специфичних обавештајних захтева.“*[148]

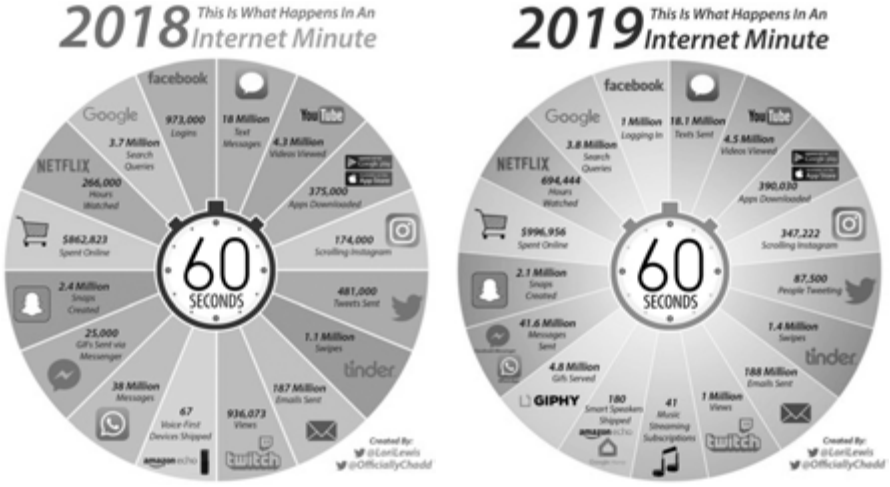
Многе процене најразличитијих обавештајних актера показују да велика већина корисних информација које поседују обавештајне службе потичу из јавних извора (OSINT). Друштвене мреже отварају бројне могућности за истрагу било које врсте због огромне количине корисних информација које се могу наћи на једном месту. На пример, може се добити велики број личних података о било којој особи широм

[147] N. A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools,* 2018., стр. 1.

[148] National defense authorization Act for fiscal year 2006, Public Law 109-163, доступно на https://www.govinfo.gov/content/pkg/PLAW-109publ163/html/PLAW-109publ163.htm, приступљено 18.04.2020. године.

света тако што ће бити пронађен само Фејсбук налог те особе, под условом да исти није лажан или намерно преправљен, како би се пласирале погрешно усмеравајуће информације. Поред великог значаја за обавештајну заједницу, OSINT прикупљање је јефтиније и мање ризично од традиционалних метода за прикупљање података, јер све што је потребно за прикупљање података из OSINT ресурса су рачунар, Интернет веза и адекватно знање.[149]

Као што је наведено, количина података, и интензитет комуникације која се остварује преко Интернета расте великом брзином, па је самим тим и њихова претрага отежана. Примера ради, статистика платформе Јутјуб говори да се сваког минута објави око 300 сати видео материјала, док друштвена мрежа Фејсбук у моменту писања овог рада има око 2,5 милијарде активних корисника и 83 милиона лажних налога.[150]



Слика бр. 29: Приказ интеракције корисника на тренутно водећим дигиталним платформама у временском интервалу од једног минута у 2018. и 2019. години.[151]

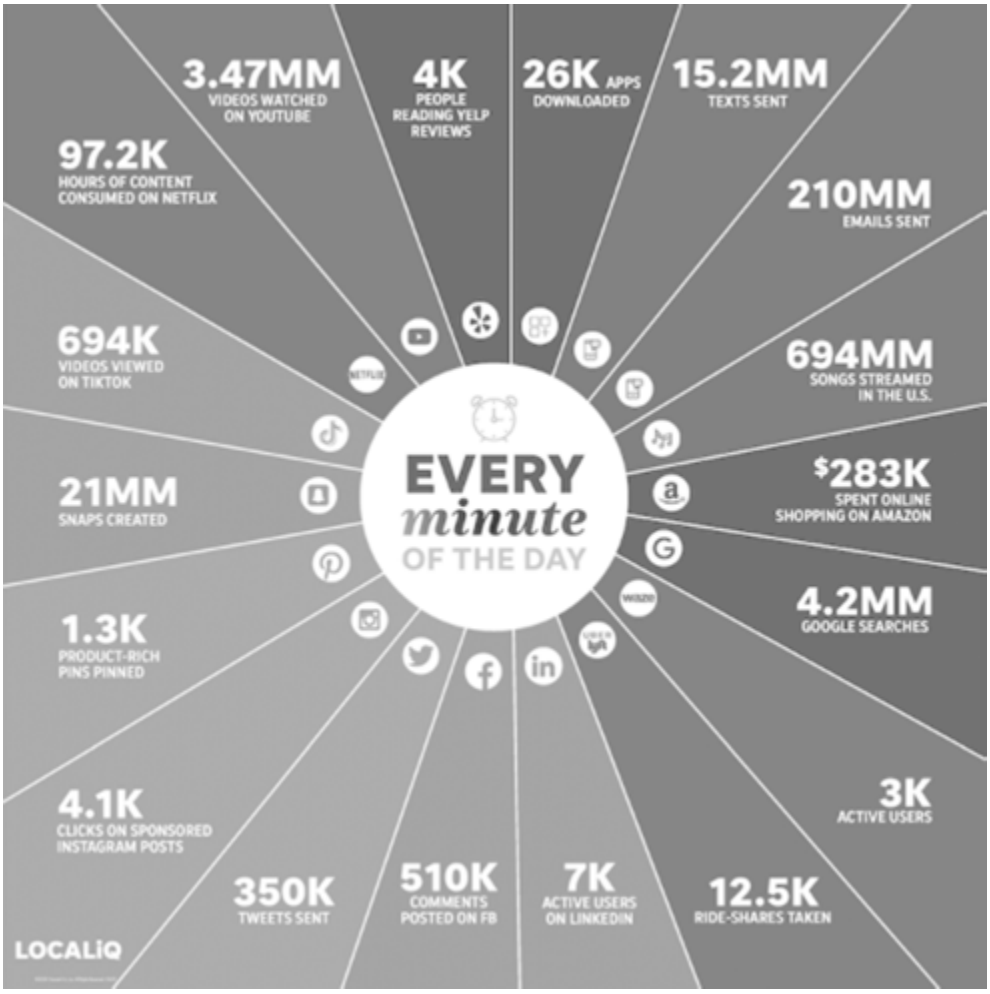
На слици бр. 29. се могу уочити промене у трендовима коришћења појединих Интернет платформи и сервиса у временском периоду од једне

[149] N. A. Hassan, R. Hijazi, Op.cit., стр. 3.

[150] Global social media stats counter, доступно на https://gs.statcounter.com/social-media-stats и Facebook Investor relations, доступно на https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx приступљено 18.04.2020. године.

[151] Visual Capitalist, „What Happens in an Internet Minute in 2019?“, доступно на https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/, приступљено 18.04.2020. године.

године. Са једне стране драстичан пораст коришћења појединих, као нпр. „Netflix“ или „Instagram“, а са друге пад као код „Twitter“-а, говори о динамичности промена и миграцијама корисника међу друштвеним мрежама, које су условљене различитим факторима као нпр. политика коришћења.[152]



Слика бр. 30. 2021.год.

Дешава се, да се приликом претраге јавних извора дође и до поверљивих података који нису на адекватан начин заштићене. Такви „процурели“ подаци се могу нпр. пронаћи на веб страницама као што је

[152] Jacob K., The Verge: „Twitter keeps loosing monthly users, so it's going to stop sharing how many“, 2019., доступно на https://www.theverge.com/2019/2/7/18213567/twitter-to-stop-sharing-mau-as-users-decline-q4-2018-earnings, приступљено 16.06.2020. године.

„Викиликс“[153]. Парадоксално, иако поверљиви и прикупљени бесправно, такви подаци су чињеницом да су постали јавно доступни постали погодни за OSINT методу прикупљања података.

Према НАТО приручнику о прикупљању података из јавних извора[154] из 2001. године, постоје четири категорије података који се могу добити из јавних извора:

- Генерички подаци из примарних извора, као нпр. фотографије, аудио и видео материјал, сателитске фотографије, базе података, метаподаци итд;
- Генерички подаци који су прошли кроз одређени одређени процес обраде и филтрације како би задовољили одређене критеријуме или потребе, као нпр. књиге које обрађују одређене теме, чланци, дисертације, журнали, технички извештаји, интерна документа комерцијалних предузећа, као и други садржаји који су обрађени од стране њихових твораца. Називају се још и „сивом литературом“ (grey literature), јер се објављују ван традиционалних и академских дистрибутивних канала;
- Подаци из јавних извора који су претворени у информације које су откривене, обрађене и намењене да задовоље одређене критеријуме и потребе у најширем смислу;
- Потврђени подаци из јавних извора, који поседују висок степен тачности и који су потврђени другим изворима који нису јавни, или подаци из поузданих и респектабилних јавних извора. Имају нарочит значај, јер се може десити да дође до намерне јавне објаве нетачних података у циљу ометања OSINT анализе.[155]

Како OSINT подразумева све јавно доступне изворе, укључујући оне на Интернету и ван њега, такве изворе можемо поделити у четири групе:

- Интернет (форуми, блогови, друштвене мреже, видео платформе, платформе за претрагу физичких и правних лица, регистрованих домена и ИП адреса, геолокацијске податке, као и све друго што се може пронаћи он-лајн што ће бити предмет основне обраде овог рада);

[153] Викиликс је међународна непрофитна медијска организација коју је 2006. године основао Џулијан Асанж и која објављује анонимне дојаве и „процурале“ поверљиве државне информације. Од свог оснивања, објавила је преко 10 милиона поверљивих докумената и и другог материјала који су изазвали велико интересовање и контроверзе у светској јавности. Доступно на https://wikileaks.org/, приступљено 18.04.2020. године.

[154] NATO Open source Intelligence handbook, доступно на http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf, приступљено 18.04.2020. године.

[155] Пример поуздане информације би био нпр. у случају када национални ТВ сервис уживо преноси дочек страног председника на аеродрому.

- Традиционални масовни медији (радио, телевизија, новине, књиге магазини);
- Специјализовани журнали, академске публикације, дисертације, годишњи извештаји предузећа и компанија;
- Фотографије и видео снимци укључујући и метаподатке[156]
- Геопросторне информације (нпр.комерцијалне мапе и картографије)

Како данас живимо у информатичкој ери, издавачи, корпорације, универзитети и други актери пребацују своје пословне процесе у дигитални облик. Такође, број корисника друштвених мрежа ће наставити да се увећава, као и број „Интернет ствари"[157], што ће довести до огромног повећања количине дигиталних података који долазе из великог броја сензора и машина, чинећи примарним он-лајн изворе података за OSINT анализе у будућности.[158] Процене су да ће до 2025. године укупан број дигиталних података произведених од стране „Интернет ствари" достићи 180 зетабајта[159], као и да ће 2021. године, 20% човекових активности укључивати услуге барем једне од великих ИТ компанија (Гугл, Епл, Фејсбук, Амазон).

6.1. Ко је заинтересован за OSINT податке?

Подаци прикупљени из јавних извора могу допринети различитим организацијама, које ће бити наведене у даљем тексту[160].

Државни органи, посебно безбедносне службе, сматрају се највећим корисником OSINT извора. Огромни технолошки развој и широка употреба Интернета широм света учинили су владе значајним корисницима OSINT обавештајних података. Владама су потребни OSINT извори за различите сврхе као што су национална безбедност, борба против тероризма,

[156] Метаподаци дају ближе информације за разумевање података који се објављују. Они у великој мери олакшавају поновну употребу објављених података. Најчешћа дефиниција метаподатака јесте да су то подаци о подацима. Сврха постојања метаподатака јесте лакше проналажење неког документа (извора информација). Постоје три врсте метаподатака: описни, административни и структурни. Више о метаподацима на порталу отворених података Р. Србије, доступно на https://data.gov.rs/sr/posts/metapodatsi/, приступљено 18.04.2020. године.

[157] Internet of Things (IoT) односи се на паметне уређаје са уграђеном електроником, софтвером, сензорима и могућношћу повезивања са произвођачем, оператером или другим уређајима, омогућавајући тако напредне услуге и директнију интеграцију физичког света и рачунарских система, као нпр. паметни сатови, телевизори, аутомобили и др.

[158] N. A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools,* Op.cit., стр. 6.

[159] Internet of things, Technology Blog, доступно на https://techblog.comsoc.org/2016/03/09/idc-directions-2016-iot-internet-of-things-outlook-vs-current-market-assessment/, приступљено 18.04.2020. године.

[160] N. A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools,* Op.cit., стр. 12.

он-лајн праћење активности терористa, разумевање домаћих и страних јавних ставова о различитим темама, снабдевање креатора политике потребним информацијама за утицај на њихову унутрашњу и спољну политику и коришћење страних медија попут телевизије у циљу добија тренутних информација о различитим догађајима који се дешавају у иностранству. Службе безбедности комбинују јавно доступне информације са подацима стеченим применом других мера и радњи из својих надлежности (нпр. сателитских слика, материјала прибављених путем уређаја за тајни надзор комуникација) како би одговориле на одређено питање или предвиђале будуће догађаје. Такве службе имају потребне ресурсе за прикупљање и анализу огромних количина података на Интернету. Очекује се да ће се процес прикупљања OSINT података од стране државних органа појачати док се даље будемо кретали кроз информатичку еру.

Међународне организације попут Уједињених Нација користе OSINT изворе за подршку мировним операцијама широм света. При креирању своје политике, УН балансира забринутости суперсила и националних држава, и она мора бити што транспарентнија. Да би то постигли, УН су установиле да је погоднije користити OSINT изворе (укључујући нпр. комерцијалне сателитске снимке) за своје обавештајне потребе уместо зависити од извештаја својих држава чланица, који могу имати сукобљене политике. Хуманитарне организације попут Црвеног крста, користе OSINT изворе како би им помогли у напорима за пружање помоћи у временима кризе или катастрофе. Они користе OSINT податке како би заштитили своје ланце снабдевања од терористичких група анализом друштвених мрежа и апликација за комуникацију како би предвидели будуће терористичке акције. НАТО у великој мери зависи од OSINT извора у сврхе прикупљања обавештајних података, као и за прављење планова за мировне операције. Такође, користи комерцијалне сателитске снимке за планирање операција, јер немају све земље чланице НАТО-а такве могућности. НАТО је објавио три упутства о томе како се користе јавни извори и то: „НАТО приручник за прикупљање података из јавних извора“[161], „НАТО књига за прикупљање података из јавних извора“[162] и „НАТО експлоатација интернета за прикупљање обавештајних података“[163].

[161] NATO OSINT Handbook V 1.2, доступно на https://archive.org/details/NATOOSINTHandbookV1.2/mode/2up, приступљено 18.04.2020. године.

[162] NATO OSINT Intelligence reader, доступно на http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf, приступљено 18.04.2020. године.

[163] Intelligence Exploitation of the Internet, доступно на https://nsarchive2.gwu.edu//NSAEBB/NSAEBB436/docs/EBB-005.pdf, приступљено 18.04.2020. године.

Полиција користи OSINT изворе за заштиту грађана од злостављања, сексуалног насиља, крађе идентитета и других кривичних дела. То се може постићи праћењем канала друштвених мрежа за интересантне кључне речи и слике како би се спречило кривично дело пре његовог извршења. Службе за спровођење закона користе OSINT за надгледање и праћење мрежа криминалаца у различитим земљама. На пример, користе OSINT тактику за прикупљање информација о безбедносно интересантним лицима и извршиоцима кривичних дела да би направили комплетан профил за сваког од њих. Такође користе OSINT изворе за сузбијање кривичних дела фалсификовања и кршења ауторских права на мрежи.

Пословне корпорације. Информације су моћ, а корпорације користе OSINT изворе за истраживање нових тржишта, праћење активности конкурената, планирање маркетиншких активности и предвиђање свега што може утицати на њихово тренутно пословање и будући раст. У прошлости је коришћење OSINT извора било ограничено на велика предузећа са добрим обавештајним буџетима. Данас, уз широку употребу Интернета, мале компаније са ограниченим буџетима могу ефикасно да користе OSINT изворе и уврсте стечене информације у своје пословне планове. Предузећа такође користе OSINT обавештајне податке у друге непрофитне сврхе, као што су борба против цурења података, знајући да је пословно излагање поверљивих информација и безбедносна угроженост њихових мрежа разлог будућих сајбер напада; креирање своје обавештајне стратегије о спољним и унутрашњим претњама кроз анализу OSINT извора и комбинујући ове информације са другим информацијама да би се постигла ефикасна политика управљања сајбер ризиком која им помаже да заштите своје финансијске интересе, репутацију и базу корисника. OSINT метода је посебно корисна за компаније које раде у одбрамбеној индустрији, из разлога што такве компаније морају бити у потпуности свесне околности са којима се њихови купци суочавају, како би на одговарајући начин развиле своје производе и будуће купце циљале одговарајућом опремом.

Људи свесни питања приватности. Обични људи који би желели да провере како потенцијални нападачи могу „провалити" у њихове рачунаре и шта њихов пружалац услуга Интернета (Internet Service Provider) зна о њима. Такође, они желе знати ниво изложености на Интернету како би затворили било који безбедносни јаз и избрисали све приватне податке које су можда ненамерно објавили. OSINT је одличан алат за проверу како нечији дигитални идентитет изгледа спољном свету, и на тај начин омогућава да појединци сачувају своју приватност. Они такође могу да користе OSINT за борбу против крађе идентитета, нпр. у случају лажног

представљања. Заправо, сви корисници Интернета користе OSINT технике на један или други начин, као нпр. када траже нешто на Интернету. Било да се ради о компанији, школи, универзитету или особи, то заправо представља прикупљање неког облика OSINT података.

Терористичке и криминалне организације. Терористи користе OSINT изворе за планирање напада, прикупљање информација о циљевима пре него што их нападну (нпр. помоћу сателитских слика као што су Google Maps и Earth за истраживање циљане локације), за придобијање више истомишљеника анализом друштвених мрежа, прибављање информација које су случајно открили поједине организације (како направити импровизовану експлозивну направу итд.), као и ширење своје пропаганде широм света користећи различите медијске канале. Такође, извршиоци кривичних дела могу користити ове методе како би се припремили за извршење нрп. провалних крађа, и уверили да је власник стана отпутовао на одмор и сл.

6.2. Начини прикупљања података

Подаци из јавних извора се могу прикупљати помоћу три методе: пасивне, полу-пасивне и активне[164]. Која ће се метода употребити зависи од ситуације у којем поступак прикупљања делује наспрам врсте интересантних података. Ове методе прикупљања се обично користе за описивање начина на који онај који прикупља податке оставља своје дигиталне трагове.

Пасивно прикупљање. Ово је најчешће коришћена метода при прикупљању OSINT података. Заправо, све OSINT активности би требале представљати пасивно прикупљање, јер је главни циљ прикупљање информација само путем јавно доступних извора. Коришћењем ове методе, власник информација нема сазнања о активностима прикупљања обавештајних података. Ова врста претраге је врло анонимна, и из техничке перспективе открива ограничене информације, јер се не шаљу никакави пакети података на циљани сервер - било директно или индиректно - а главни ресурси који се могу прикупити су ограничени на архивске податке (углавном застареле информације), незаштићене датотеке остављене на циљаним серверима и садржај присутан на циљаним веб локацијама. Пример за пасивно прикупљање података би подразумевао класично претраживање интересантних веб локација, база података, кешираних података који су јавно доступни, у циљу прикупљања нпр.

[164] N. A. Hassan, R. Hijazi, *Op. cit.,* стр. 14.

ИП адреса, бројева телефона, физичких адреса итд. Такав процес може бити и аутоматизован употребом специјалних алата, тзв. веб кролера (web crawler).

Полу-пасивно. Са техничког становишта, ова врста прикупљања подразумева слање ограничених пакета података циљаним серверима, како би се стекле опште информације о њима. Ова врста преноса података настоји да личи на типични Интернет саобраћај да не би скренула пажњу на „извиђачке" активности. На тај начин се не спроводи детаљна истрага мрежних ресурса циља, већ се само лагано истражује без покретања било каквог аларма на страни циља. Иако се ова врста прикупљања сматра анонимном, власник може знати да се дешава прикупљање података ако истраже проблем (проверавањем логова сервера или мрежних уређаја). Међутим, иако би дошло до откривања, власници сервера такву врсту активности не би могли да га припишу рачунару онога ко претражује. Пример за овакав метод прикупљања података би подразумевао да се нпр. прегледају метаподаци јавно доступних докумената.

Активно. Ова метода подразумева директну комуникацију са системом у циљу прикупљања обавештајних података о њему. Циљ може постати свестан процеса прикупљања, јер ће особа/ентитет који прикупља информације користити напредне технике за прикупљање техничких података о циљаној ИТ инфраструктури као што су приступ отвореним портовима, скенирање рањивости, скенирање апликација на веб серверу и још много тога. Овај саобраћај ће изгледати као сумњиво или злонамерно понашање и оставиће трагове на циљаном систему детекције и спречавање провале. Извођење напада социјалног инжењеринга на мету такође се сматра врстом активног прикупљања информација, и подразумева одређену врсту деловања према мети, како би се она навела да предузме жељену акцију која је штетна по њу. Примери за такав начин прикупљања података зависе од маштовитости нападача: од наизглед легитимних имејлова колега или шефова који траже креденцијале ради логовања на систем због наводног хитног посла, до слања имејлова или СМС порука са обавештењима о великим попустима у радњама које жртва често посећује који садрже линкове који ће инсталирати малициозни софтвер на рачунару или мобилном телефону. Тактика се углавном заснива на фингирању таквих околности где се од жртве очекује брза и непромишљена реакција. Након крађе креденцијала за логовање односно инсталације малвера, може доћи и до злоупотребе истих на различите начине који могу укључивати крађу новца, идентитета и др.

6.3. Предности и изазови

Главне предности ове методе прикупљања података су следеће:

- **Мање ризично**: Коришћење јавно доступних информација за прикупљање обавештајних података нема ризика у поређењу с другим облицима прикупљања обавештајних података, као што су коришћење људских извора на терену за прикупљање информација, посебно у непријатељским земљама.
- **Исплативо**: Прикупљање података из јавних извора је углавном јефтиније у поређењу с другим обавештајним изворима. На пример, коришћење људских извора или шпијунских сателита за прикупљање података је скупо. Мала предузећа са ограниченим буџетом за прикупљање обавештајних података могу искористити OSINT изворе уз минималне трошкове.
- **Једноставност приступа**: OSINT извори су увек доступни, без обзира где се налазите, и углавном су ажурирани. OSINT изворе могу користити различити актери у било ком обавештајном контексту. Све што је потребно су адекватне вештине и алати за правилно прикупљање и анализирање. На пример, безбедносне службе могу предвидети будуће нападе анализирајући активности на друштвеним мрежама, док корпорације могу да их користе за израду нових стратегија ширења тржишта.
- **Правна питања:** OSINT ресурси могу се делити међу различитим страна без бриге о кршењу било које лиценце за ауторска права, јер су ти ресурси већ јавно објављени. Нека ограничења важе за дељење сиве литературе, под којом се подразумевају домаћи и страни материјали и публикације које су доступне путем специјализованих канала и нису комерцијалне, те је њихово прибављање знатно отежано. Ради се нпр. о разним годишњим извештајима, техничким документацијама, пројектима, необјављеним рукописима, евалуацијама и извештајима владиних служби, пословних и индустријских корпорација, које не потпадају под библиографску контролу и уобичајене системе публикације и дистрибуције. Дељење таквих материјала у одређеним случајевима може представљати кршење Закона о ауторским и сродним правима и Закона о тајности података.
- **Помоћ финансијским истражитељима**: OSINT омогућава нпр. специјализованим државним агенцијама да открију утају пореза, и друге малверзације у области финансијског пословања. Многе познате личности и неке компаније могу бити укључене у утају пореза, а праћење њихових налога на друштвеним мрежама и објава начина живота може имати велики значај за надлежне органе који их могу процесуирати због непријављеног прихода. Такав пример се десио у држави Њујорк, САД,

када је против више лица, физиотерапеута покренут кривични поступак због издавања лажних рачуна у износу од 41 хиљаде долара за своје наводне услуге према деци ометеној у развоју, док је истрага утврдила да се једна од оптужених у моменту издавања лажног рачуна налазила на плажи у Доминиканској Републици, а као доказ на суду је прихваћена фотографија објављена на личном Фејсбук налогу.[165]

- **Борба против фалсификовања путем интернета**: OSINT технике могу се користити за проналажење лажних производа и услуга, као и усмеравање надлежних органа за затварање таквих веб локација, или слање упозорења корисницима да се престану са куповином таквих производа. Ово је велика предност OSINT-а, посебно када се бори против фалсификованих фармацеутских и природних здравствених производа.
- **Одржавање националне безбедности и политичке стабилности**: Ово би могла бити и најважнија улога OSINT –а, јер може помоћи владама да разумеју ставове својих људи и одмах делују како би избегли будуће сукобе. Одговорне владе користе OSINT технике у својим будућим стратегијама, посебно за своју унутрашњу политику, док у супротном случају постоји опасност у смислу усмеравања јавног мњења и креирања лажних вести, те на исти начин циљане и координиране злоупотребе алата о којима је реч.

Са друге стране, све методе прикупљања обавештајних података имају одређена ограничења, па тако ни OSINT није изузет од овог правила. У даљем тексту ће бити објашњени неки од изазова са којима се суочава OSINT прикупљање података.

- **Огромна количина података**: Прикупљање података из јавних извора може произвести огромну количину података који се морају анализирати да би имали неку вредност. Наравно, постоје многи аутоматизовани алати за ову сврху, а многе владе и велике корпорације развиле су сопствени скуп алата и техника вештачке интелигенције за филтрирање прибављених података. Међутим, огромна количина података остаће изазов за оне који се баве овом методом прикупљања података.
- **Поузданост извора**: Треба имати на уму да се OSINT извори, посебно када се користе у обавештајном контексту, морају темељно проверити од стране класификованих извора[166] да би им се могло веровати. Многи

[165] Jared G., Miami Herald: „Photo proves therapist lied about helping disabled kids and stole $41,000, prosecutors say“, доступно на https://www.miamiherald.com/news/nation-world/national/article219529365.html, приступљено 21.06.2020. године.

[166] Под класификованим изворима се подразумевају службене евиденције и базе података којима располажу органи за спровођење закона. Почетна информација се може уочити на Интернету, али се она мора проверити и упоредити са расположивим

субјекти објављују нетачне информације како би довеле у заблуду поступак прикупљања OSINT -а. Мотиви за то могу бити различити: од праћења реакција заинтересованих субјеката (Ко реагује? На који начин? Да ли приликом реакције долази до објављивања неких података који до тада нису били познати?), дискредитације (нарочито ако се ради о особама из јавног живота), до избегавања кривичног гоњења (нпр. објављивање садржаја који указује на то да се неко лице налази у иностранству итд.).

- **Људски напори**: Огромна количина података сматра се највећим изазовом за прикупљање OSINT -а. Људи морају да виде резултат аутоматизованих алата да би знали да ли су прикупљени подаци поуздани; такође их морају упоредити са неким класификованим подацима (ако се говори о безбедносним сужбама) да би се обезбедила њихова поузданост и релевантност, што подразумева трошење времена и људских ресурса.

6.4. Да ли Србија прати светске трендове?

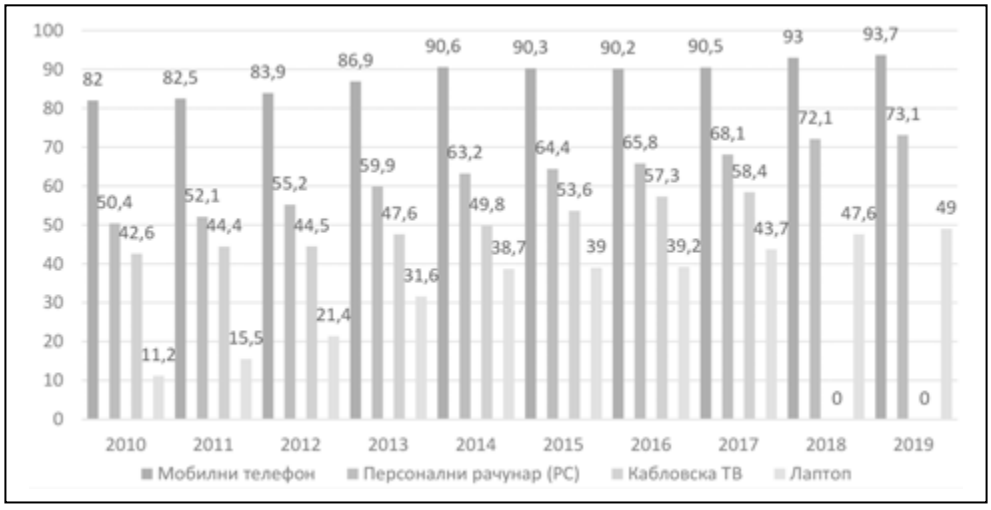
Већ је наведено да је револуција Интернета претворила свет у мало село, што значи да тај процес није заобишао ни Р. Србију. Учешће дигиталних технологија у свакодневном животу човека у Србији није на истом нивоу као у развијеним западним државама, делом и због тога што поједине компаније које управљају одређеним дигиталним сервисима не виде Србију као профитабилно подручје. Међутим, тај јаз постаје све мањи, јер слобода тржишта дозвољава домаћим ИТ компанијама да створе алтернативу сервисима великих ИТ корпорација и тако одређене услуге приближе просечном кориснику. У даљем тексту ће као резултат рада на обради ове теме графички бити приказани трендови раста коришћења рачунара и Интернета у Р. Србији за период од 2010. до 2019. године[167], на основу преузетих података Републичког завода за статистику, који указују на охрабрујућу чињеницу да се број домаћинстава која поседују широкопојасну Интернет конекцију повећава из године у годину. С обзиром да живимо у информатичкој ери, сасвим је очекивано постојање растућег тренда коришћења Интернета и рачунара, али је исто тако охрабрујућ податак постојања растућег тренда поседовања широкопојасне интернет конекције и рачунара у домаћинствима у Србији, што нас доводи до закључка да је у данашње време много лакше, јефитније и брже приступити Интернету него у 2010. години када је за неки такав подухват било потребно више опреме, времена и процедуре за приступ Интернету, поготову у мањим местима. С озбиром

класификованим подацима, јер се на тај начин смањује шанса да нетачна информација буде узета у разматрање као тачна.

[167] Републички завод за статистику, доступно на https://www.stat.gov.rs/sr-cyrl/, приступљено 18.04.2020. године.

на територијалну заступљеност Интернет прикључака, можемо закључити да су готово сва места, како мања, тако и она већа, у Србији покривена добром Интернет конекцијом и брзим протоком података.

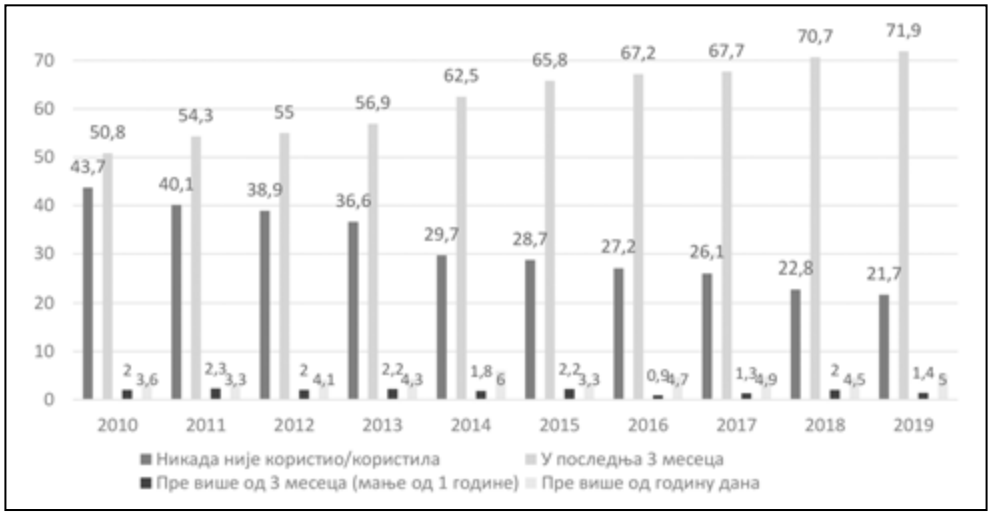
Поседовање адекватних уређаја је предуслов приступа Интернету. На графикону бр. 3 могу се видети статистички подаци поседовања одређених уређаја у домаћинствима. Као што се могло очекивати, мобилни телефон се ближи бројци од готово 100% поседовања. Може се приметити да поседовање персоналних рачунара и мобилних телефона имају готово исти тренд раста, док поседовање лап – топ рачунара не прелази 50% домаћинстава.



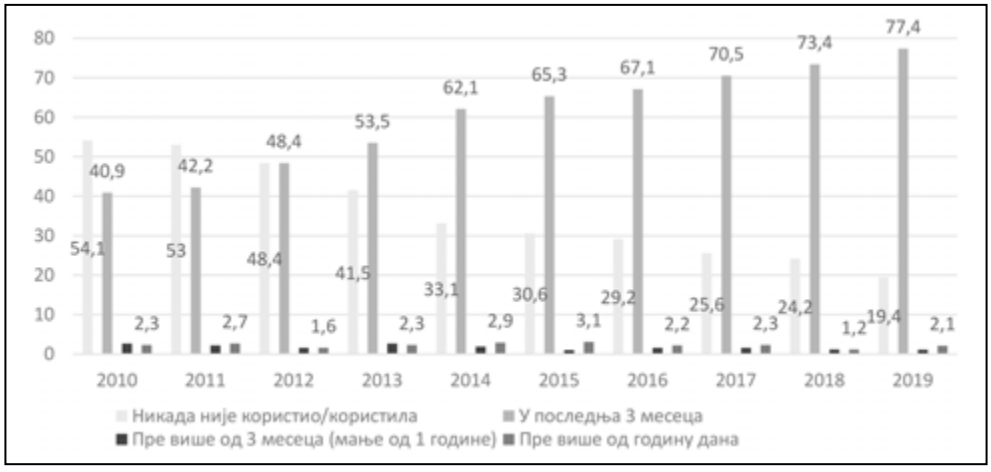
Графикон бр. 3. Врста уређаја која домаћинства поседују

Графикон бр. 4. Укупан приказ домаћинстава која поседују рачунар, Интернет прикључак и широкопојасну Интернет конекцију

Када помислимо на приступ Интернету, први уређај који нам пада на памет јесте рачунар. На графикону бр. 4 може се уочити да је 2014. године дошло до изједначавање броја поседовања рачунара и поседовања Интернет прикључка што указује да је готово свако домаћинство које поседује рачунар, поседовало и Интернет прикључак. Што се тиче широкопојасне Интернет конекције, она се изједначава у 2018. години. Међутим, у 2019. години јасно се види да постоје домаћинства која поседују Интернет прикључак и широкопојасну Интернет конекцију, а не поседују рачунаре. Ово се може приписати другим уређајима који се користе за приступ интернету (мобилни телефон, таблет рачунари итд.).



Графикон бр. 5. Учесталост употребе рачунара - појединац

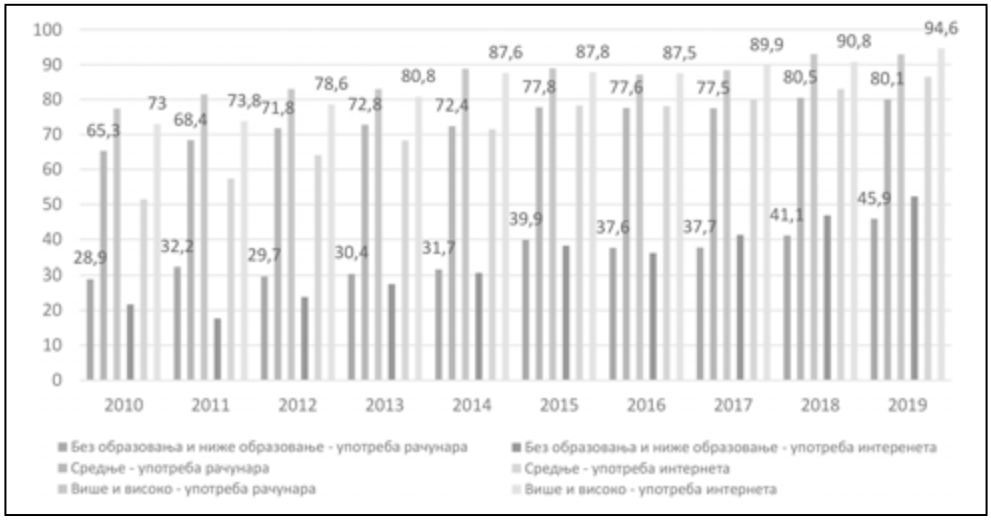


Графикон бр. 6. Учесталост употребе Интернета - појединац

На графикону бр. 5 може се уочити како број људи који никада нису користили рачунар, а који се у 2010. години кретао око 40%, има тренд линеарног пада да би у 2019. години тај број опао за половину, тј. приближио се бројци од 20%. Логично је за очекивати да ће ова бројка наставити са линеарним падом и да ће се у будућности врло вероватно приближити нули. Са друге стране, употреба рачунара од стране појединца у претходна три месца линеарно расте, такође се може уочити да је већ 2010. године, готово више од 50% испитаника користило рачунар и било оспособљено за његову примену.

На графикону бр. 6 може се јасно уочити како се употреба Интернета у Србији линеарно повећава током година, док број оних који никада нису користили Интернет убрзано опада.

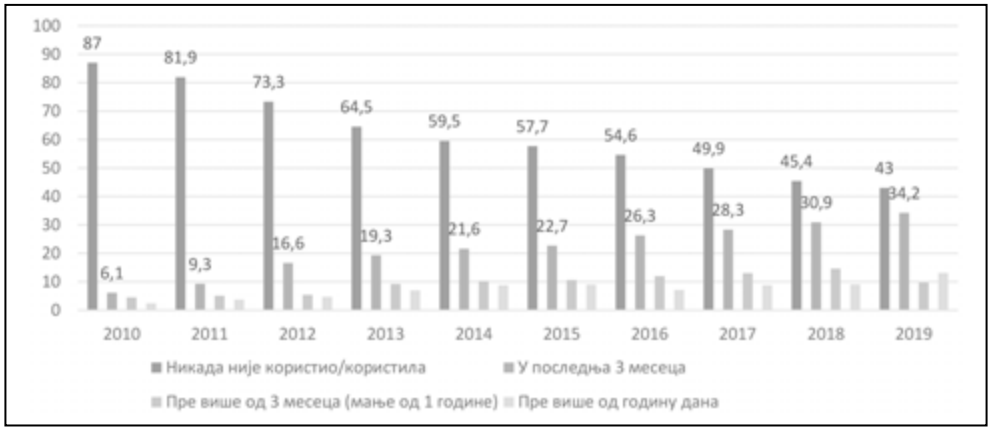
Графикон бр. 7 приказује увећану учесталост коришћења Интернета и рачунара код популације са вишим степеном образовања. Очекивано је да људи са вишим и високим степеном образовања највише користе рачунар и Интернет, што показује бројка од преко 90%. Такође, примећује се и тренд раста коришћења рачунара и Интернета код популације са средњом стручном спремом који се приближава деведесетом проценту.



Графикон бр. 7. Упоредни приказ степена образовања са употребом рачунара и Интернета

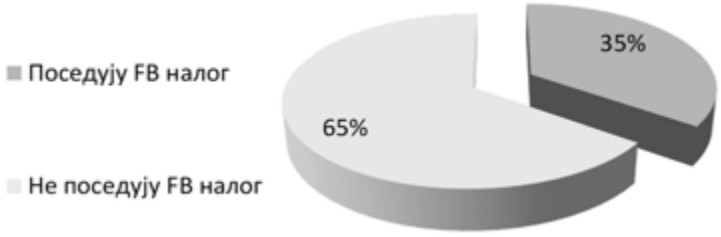
С обзиром на пораст броја коришћења рачунара и Интерента у Р. Србији, интересантно је да тренд куповине преко Интернета не прати тренд коришћења Интернета. Уочава се један, готово правилан линеарни раст тренда куповине преко интернета у односу на 2010. годину, али исто тако се може приметити да је број људи који никада нису куповали преко Интернета и даље велики у 2019. години, узимајући у обзир број корисника

Интернета и рачунара. Овакви резултати могу се приписати чињеници да су људи неповерљиви када се ради о куповини преко Интернета и упознати су са различитим видовима преваре приликом он-лајн куповине.



Графикон бр. 8. Куповина путем Интернета у Републици Србији

Графикон бр. 9 приказује проценат коришћења друштвене мреже Фејсбук у односу на укупан број Интернет корисника у Р. Србији, према истраживању Internetworldstats[168] из децембра 2018. године, које наводи да је у том моменту у Р. Србији Интернет користило око 6,326,000 људи. Ако се ове бројке упореде са регионом, може се уочити да становници других држава више користе Фејсбук, и то Црна Гора (50,9%), БиХ (42,8%), Албанија (47,7%).



Графикон бр. 9. Коришћење Фејбука у Републици Србији

6.4.1. Јавно доступне информације

Организације и појединци често објављују велику количину информација на Интернету. У случају организација, то може бити резултат жеље за промовисањем њихових активности и усмеравањем њихове интеракције

[168] Internet World Stats, доступно на https://www.internetworldstats.com/europa2.htm#links, ажурирано у децембру 2018. године, приступљено 20.04.2020. године.

са јавношћу. Неке осетљиве информације које терористи могу користити у незаконите сврхе доступне су и путем он-лајн претраживача који могу захватити и складиштити неадекватно заштићене информације са милиона веб локација. Надаље, приступ интернету детаљним логистичким информацијама, као што су видео краудсорсинг софтвери и апликацијама попут „Google Earth", које су намењене и углавном коришћене од стране појединаца за легитимне циљеве, може бити злоупотребљен ради извиђања потенцијалних циљева прегледом сателитских снимака високе резолуције, мапа и информација о терену и зградама.

На друштвеним мрежама попут Фејсбука, Твитера, Јутјуба и блог платформи, појединци добровољно или ненамерно објављују велику количину осетљивих информација на Интернету. Иако је намера оних који дистрибуирају информације можда обавештавање својих пратилаца у информативне или друштвене сврхе, неке од тих информација могу се злоупотребити у криминалне сврхе.

6.4.2. Сајбер напади

Један од пионира изучавања феномена сајбер тероризма, професорка Дороти Е. Денинг је описала сајбер тероризам као конвергенцију тероризма и сајбер простора. Сајбер тероризам представља нелегални акт и претњу по компјутерске системе, мреже и информације. Као и сваки облик тероризма, има политичку, идеолошку, верску, социјалну димензију. Циљ је изазавати панику и страх, како би се остварили одређени политички и друштвени интереси, а сам напад би требало да доведе до насиља над лицима или имовином, или да бар проузрокује довољно штете за генерисање страха. С обзиром да се одвија у сајбер простору, подразумева се да је сам терористички акт планиран, извршен или координиран помоћу рачунара и рачунарских мрежа.[169] Један од потенцијално најопаснијих облика напада терориста у сајбер простору је угрожавање критичне националне инфраструктуре држава. Непријатељске групе широм света потенцијално могу да хакују, односно да на нелегалан начин приступе компјутерским системима на које се ослања функционисање националне инфраструктуре, да угрозе рад тог система, искључе га или измене. Пример сајбер терористичког напада је виђен у Израелу 2012. године, када је „срушено"[170] неколико битних веб сајтова као што су берза Тел Авива и национална авио компанија. Поред наведеног, објављени су

[169] К. Јонев: „Сајбер тероризам и употреба сајбер простора у терористичке сврхе", Безбедност 2/2016, стр. 209.

[170] DDOS (distributed denial-of-service, напад ускраћивањем ресурса).

подаци више од 20 хиљада израелских кредитних картица.[171] За разлику од активности терористе на мрежи које су до сада описане, као нпр. ширење пропаганде или регрутовање у циљу извршења класичних терористичких напада употребом традиционалног оружја или других предмета, у случају сајбер тероризма примарна мета би био напад на виталну националну инфраструктуру употребом рачунара и рачунарских мрежа, са фокусом на системе који ће нашкодити нормалном функционисању државе и становништва, а то су пре свих енергетски и финансијски сектор. Иако се рачунари и рачунарске мреже експлицитно не наводе као средство извршења кривичног дела Тероризам из чл. 391 КЗРС, у ставу 3 овог члана су као заштитни објекти наведени државни и јавни објекти, саобраћајни и информациони системи и инфраструктура.

[171] The New York Times, Isabel Kershner: „2 Israeli Web Sites Crippled as Cyberwar Escalates“, доступно на https://www.nytimes.com/2012/01/17/world/middleeast/cyber-attacks-temporarily-cripple-2-israeli-web-sites.html, приступљено 29.04.2020. године.

7. „Dark Net" као сегмент интернета од значаја за терористичке организације

Терористи и организоване криминалне групе су такође открили предности Даркнет-а и почели да користе тајне платформе. Иако се дуго претпостављало да су терористички напади координирани посредством Даркнет-а, чврсти докази о терористичкој употреби те платформе стигли су тек у августу 2013. године када је америчка Агенција за националну безбедност (НСА) пресрела шифроване комуникације између вође Ал-Каиде Ајмана Ал-Завахирија и Насера Ал-Вухајсија, вође јеменске Ал-Каиде са Арапског полуострва. Институт за студије националне безбедности открио је да се близу дест година комуникација између челника светске мреже Ал-Каиде била барем делимично одвијала на Даркнет-у.[172]

Терористичке организације и организоване криминалне групе злоупотребљавају Интернет дужи временски период. Међутим, показало се да је тзв. „површински" односно видљиви део Интернета превише ризичан за оне који траже анонимност, јер је постојала могућност њиховог праћења и проналаска. Већина веб локација и профила на друштвеним мрежама на „површинском" вебу који се повезују са тероризмом су надгледане од стране безбедносних служби, које их затварају. Са друге стране, на Даркнет-у, децентрализоване и анонимне мреже доприносе избегавању хапшења и затварању илегалних платформи. Како је у свом извештају навела Беатрис Бертон, „Активности Исламске државе на „површинској" мрежи су надгледане што је приморало џихадисте да траже нова сигурна уточишта на мрежи".[173] Са друге стране она је указала и на структуре које су креиране од стране организованих криминалних група, које представљају векторе омогућавања деловања у оваквим оквирима на начин који обезбеђује анонимност. Веома брзо су препознати ови кулоари од стране организованог криминала и организованих криминалних група.

Након терористичких напада у Паризу у новембру 2015. године[174], ИСИС се окренуо Даркнет-у како би ширио вести и пропаганду у покушају заштите идентитета присталица те организације и заштите њеног

[172] The Institute for National Security Studies (INSS), „Backdoor Plots: The Darknet as a Field for Terrorism", 2013., стр. 1, доступно на https://www.files.ethz.ch/isn/170411/INSSInsights464.pdf, приступљено 29.04.2020. године.

[173] Berton, Beatrice, „The dark side of the web: ISIL's one-stop shop?". Report of the European Union Institute for Security Studies, 2015., доступно на https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf, приступљено 29.04.2020. године.

[174] Серија терористичких напада извршена од стране терористичке организације Исламска држава, у којој је страдало око 150 људи, доступно на https://www.b92.net/

садржаја од „хактивиста“[175]. Тај потез долази након што су стотине веб локација повезаних са ИСИС-ом уклоњене у оквиру кампање „Операција Париз“ (OpParis) коју је покренуо хакерски колектив „Анонимус“. Медијско крило Исламске државе, „Ал-Хајат Медија Центар“, објавило је линк и објашњења о томе како доћи до њихове нове Даркнет странице.[176]

Извештај из априла 2018. године, под називом „Терор у мраку“, резимира налазе студије коју је спровело удружење „Хенри Џексон“[177], откривајући растућу употребу Даркнет-а од стране терористичких организација. Истраживање показује како терористи и екстремисти стварају све већи број сигурних уточишта на Даркнет-у како би се планирали будући напади, прикупљала средства и регрутовали нови следбеници. Овај извештај наглашава следеће намене Даркнет-а за терористичке сврхе:

- **Терористи користе енкрипцију како би се боље сакрили**: праћење „површинског“ Интернета од стране друштвених мрежа и безбедносних служби резултирало је бржим темпом уклањања екстремистичких садржаја са платформи друштвених мрежа. У вези са тим је и већа употреба екстремистичких платформи Дарк Нета-а као „џихадистичког сигурног уточишта“ за планирање напада. Докази указују да регрутери користе Даркнет за планирање и покретање терористичких напада, јер је откривање од стране безбедносних служби мање вероватно. Иако се почетни контакт може успоставити на површинским веб платформама, даље инструкције о приступу џихадистичким веб локацијама на Даркнету се најчешће дају путем апликација које користе end-to-end енкрпцију[178], попут „Telegram“-а.

info/vesti/index.php?yyyy=2015&mm=11&dd=14&nav_category=78&nav_id=1062857, приступљено 29.04.2020. године.

[175] Израз настао спајањем речи хакер и активиста, означава особу која злоупотребом информационих технологија напада одређени рачунар мотивисану одређеним политичким или друштвеним циљевима. Checkpoint, „What is Hacktivism“, доступно на https://www.checkpoint.com/definitions/what-is-hacktivism/#, приступљено 29.04.2020. године.

[176] Gabriel Weimann: „Going Darker? The challenge of dark net terrorism“, Woodrow Wilson Center, Washington, стр. 3, доступно на https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf, приступљено 01.05.2020. године.

[177] Malik, N. „Terror in the Dark“, a report by the the Henry Jackson Society, London, 2018., доступно на https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf, приступљено 01.05.2020. године.

[178] E2EE (end-to-end encryption), је систем комуникације у коме је садржај читљив само пошиљаоцу и примаоцу, користећи специјалне кључеве за енкрипцију. На тај начин преглед садржаја трећим странама као што су Интернет или сервис провајдери није омогућен. Више о овој теми: Takanori Isobe, Kazuhiko Minematsu, „Breaking Message

Дискусије о томе како правити бомбе, планирати терористичке нападе „усамљених вукова", како користити возила као оружје, где убадати људе за максималан ефекат и како направити лажни прслук за самоубиство или маскирати њихову активност, са циљем да се убеде потенцијални регрути предузимање њихових напада често су главне теме на овим форумима Даркнета. За многе терористичке организације, Даркнет елиминише потребу за физичким састанком за планирање напада и пружа виртуелно место састанака за терористичке операције, где комуникација може подстаћи регруте да самостално изврше нападе уз минималну обуку или искуство. То је сличан начин на који Даркнет користе они који купују дрогу, ватрено оружје или дечију порнографију, јер се смањује ризик од физичког хватања у вршењу кривичних дела.

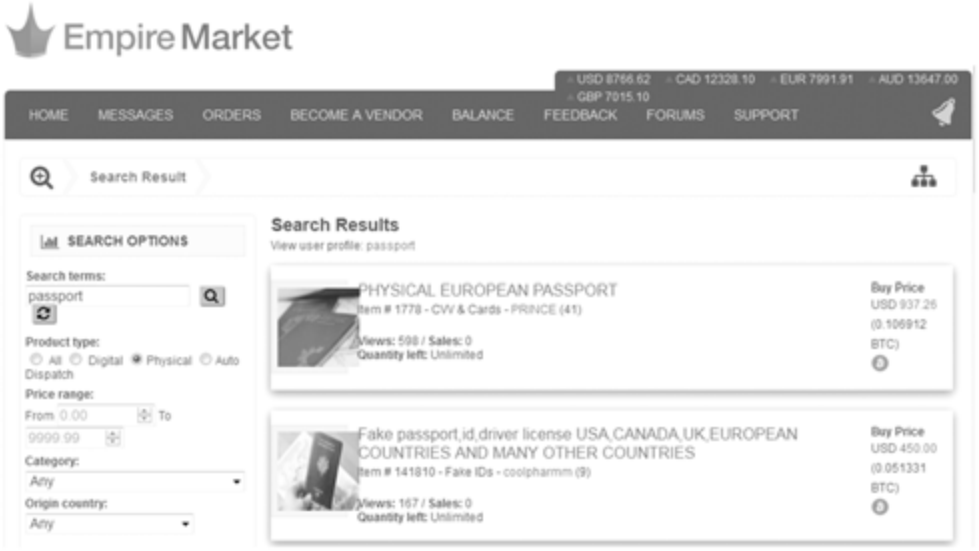
- **Терористи користе Даркнет за регрутовање**: Имајући у виду неприступачност шифрованих канала попут „Telegram"-а и Даркнета, није изненађујуће да се на тим каналима ретко врши масовно регрутовање. Уместо тога, терористичке организације имају за циљ да привуку заинтересоване симпатизере са површинског веба и друштвених мрежа у сигурније канале Даркнета за даљу интеракцију и индоктринацију.
- **Терористи користе Даркнет као резерву пропаганде**: Уклањање екстремистичких и терористичких садржаја са површинске и дубоке мреже - нарочито у случајевима када посебни алгоритми и софтвери вештачке интелигенције врше „масовно" уклањање - повећава ризик за губитак доказа у кривичном поступку против појединаца који деле такав садржај или пружају материјалну подршку. Већи део овог материјала касније се поново појављује на Даркнету.
- **Терористи користе криптовалуте у циљу финансирања и избегавања откривања токова новца**: Терористи, попут осталих криминалаца, користе криптовалуте зато што у финансијском окружењу пружа исти облик анонимности као шифровање за комуникацијске системе. Прикупљањем средстава и извршавањем финансијских трансакција на мрежи са Биткоином, терористи и други криминалци могу избећи уплитање финансијских регулатора или других лица која би могла предузети кораке да спрече њихово пословање. Према извештају Европола из 2015. године, Биткоин се налазио у истрагама високог профила који укључују размену између криминалаца и коришћен је у више од 40% таквих трансакција у Европској Унији.[179]

Integrity of an End-to-End Encryption Scheme of LINE", доступно на https://eprint.iacr.org/2018/668.pdf, приступљено 01.05.2020. године.

[179] EUROPOL 2015 Internet Organised Crime Threat Assessment (IOCTA), стр. 46, доступно на https://www.europol.europa.eu/activities-services/main-reports/

Мохамед Али, стар 31. годину, софтверски програмер из Ливерпула у Великој Британији, осуђен је на казну од осам година затвора, након што је 4. фебруара 2015. покушао да купи отров рицин преко Даркнет-а. Користећи надимак „Weirdos 0000", Али се обратио добављачу на Даркнет-у и разговарао о ценама смртоносне супстанце и могућим попустима за веће поруџбине и поновну сарадњу. Платио је добављачу са надимком „Psychochem" 2.1849 биткоина (око 225 америчких долара у то време за 500мг праха рицина - довољно да убије између 700 и 1.400 људи. Продавац је у ствари био тајни агент ФБИ, који је полицију у Енглеској обавестио пре него што је послао Алију безопасни пакет. Када је Али примио пакет, полиција га је брзо ухапсила. Нису пронађени никакви докази који би сугерисали да је Али планирао терористички напад или чак да је имао намеру да некога повреди. На суду, тврдио је да је био једноставно „радознао" о Даркнету.

Слика бр. 31: Студија случаја злоупотребе Даркнета у Великој Британији[180]



Слика бр. 32: Преглед понуде фалсификованих путних исправа на Даркнет сајту „Emprire Market"

internet-organised-crime-threat-assessment-iocta-2015, приступљено 01.05.2020. године.

[180] BBC News, „Breaking Bad fan jailed over Dark Web ricin plot", доступно на https://www.bbc.com/news/uk-england-34288380, приступљено 01.05.2020. године.

Поред наведених облика злоупотребе, Даркнет тржиште омогућава набавку фалсификованих докумената ради вршења илегалних активности, доприноси трговини људима и илегалној миграцији и ослабљује системе граничне контроле, што може може повећати ризик од терористичких активности на тај начин што омогућава терористима прибављање украдених и фалсификованих путних исправа. На пример, прелиминарна претрага на Даркнет сајту „Empire Market", је дана 02.05.2020. године дала 5 страница резултата за понуду лажних пасоша више држава, које укључују банковне изводе и возачке дозволе као доказ идентитета.[181] Наркотици (укључујући прекурсоре, нове психоактивне супстанце – НПС али и фалсификоване медикаменте) представљају убедљиво највећи облик незаконитих активности на даркнету. Само прелиминарни преглед неколико даркнет маркета у овом тренутку нуди преко 30000 понуда продаваца наркотика, уз велики дијапазон класификација истих, нпр. Монополи маркет (Benzos 79, Cannabis 671, Dissociatives 26, Ecstasy 28, Pharmaceuticals 99, Psychedelics 133, Steroids 136, Stimulants 71), затим АСАП маркет (Stimulants 2393, 2-FA 0, Adderal 51, Cocaine 786, Crack 73, Meth 399, Other 98, Pressed pills 42, Speed 358, RCs 25, Cannabis & hashish 3150, Buds & flowers 1592, Concentrates 404, Edibles 340, Hash 400, Other 42, Prerolls 22, Seeds 3, Shake 57, Synthetic 72, Topicals & others 2, Drug paraphernalia 8, Steroids 559, Barbiturates 10, овај маркет нуди као и већина других и остале облике робе и услуга надаркнету па међу њима и преваре - Fraud 3571, банковне рачуне – Bank accounts 157, кредитне и дебитне картице – Credit cards 441, остале активности у вези са преварама –Fraud related 814, Other 1327, као и физичку робу (крадене ствари, недозвољене и сл.) Physical goods 97, препарате за губитак тежине – Weight loss 26, синтетичке наркотике - Ecstasy 961, MDA 15, MDMA 503, Methylone & BK 0, Other 7, Pills 359, фалсификоване рецепте – Prescription 623, као и опиоиде – Opioids 813, Buprenorphine 28 Codeine 77 Dihydrocodeine 3, Heroin 360, Hydrocodone 18, Hydromorphone 11, Morphine 28, Opium 11, Other 22, Oxy 131, Pills 9, фалсификати - Counterfeits 113, валуте – Currency 69, злато и накит – Gold & Jewellery 36, дисоцијативи Dissociatives 642, GHB 48, Ketamine 580, MXE 0, Other 1, дигиталне робе - Digital goods 4844, податке – Data 683, хакерске услуге – Hacking 698, Information 492, Other 1574, Security 71, Software 181, Tutorials 650, Benzos 592, Other 6, Pills 181, Powder 6, RC 0, Xanax 223, Psychedelics 1203).

[181] „Emprire Market", доступно на http://gojqkfm3gidro6rguinyb4gg6col22d3zec6i633z-reyxvq35m5eghad.onion/home, приступљено 02.05.2020. године.

Осим лажних докумената, наркотика, финансијских инструмената – картица, налога за е плаћања и сл, куповина илегалног оружја је још једна могућност коју екстремисти могу злоупотребити. Недељу дана након терористичких напада у Паризу, новембра 2015. године, објављено је да су четири аутоматске пушке коришћене у нападу првобитно купљене на Даркнету од једног продавца из Немачке, који је касније ухапшен под сумњом за илегално поседовање и продају оружја на Интернету. Француске и немачке власти ову тврдњу тек треба да провере и она остаје непотврђена. Према званичним документима тужилаштва у Штутгарту у Немачкој, оружје коришћено у нападима у Паризу новембра 2015. године купљено је на Даркнет-у од немачког добављача под именом корисничко име „DW Guns".[182]

Терористичке организације користе Даркнет као што су користили површински Интернет неколико деценија, међутим овај прелазак је омогућио технолошки упућеним појединцима нове прилике. „Отворени" интернет је коришћен да би се пружиле информације другим терористима, ради регрутације и радикализације, ширења пропаганде, прикупљање средстава и координације акција и напада. Неке од ових активности, сада су прешле на дубље слојеве интернета. На пример, терористички пропагандни материјал сада је смештен на Даркнету.

Платформа за комуникацију „Telegram" је врло популарна за комуникацију међу члановима екстремистичких групација. Та платформа омогућава слање шифрованих текстуалних и мултимедијаних порука неодређеном броју чланова. Развијена је 2013. године од стране руског предузетника Павела Дурова, и функционише у оперативним системима Android, Windows и iOS. Једна од кључних карактеристика Телеграма је шифровање порука од почетка до краја (end-to-end encryption). То значи да чак ни творци апликације не знају идентитет корисника, што га чини веома привлачним криминалцима и терористима. Компанија која стоји иза Телеграма толико је сигурна у безбедност комуникација да је два пута понудила награду од 300 хиљада долара првој особи која би могла пробити њену енкрипцију. Такве карактеристике ову платформу повезују са корисницима и садржајем Даркнет-а, јер ће информације о новој Даркнет адреси бити дистрибуирана путем Телеграма. Ова платформа је доживела велики успех, како међу обичним корисницима, тако и међу терористима, међутим то се десило тек 2015. године, када је опција тзв. „Канала" била

[182] Forbes, Nikita Malik: „How The Darknet Can Be Used By Terrorists To Obtain Weapons", доступно на https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/#7c3a90be62cd, приступљено 02.05.2020. године.

понуђена. Тада је дошло до велике миграције са других друштвених мрежа, нарочито са Твитера[183]. Само четири дана након увођења опције „Канала", медијски оперативци ИСИС-а су на Твитеру започели оглашавање сопственог канала названог „Nashir", у преводу „Дистрибутер". У марту 2016. године, отворено је 700 нових канала који се повезују са Исламском државом.[184] Када је затражен коментар о овој појави, директор Телеграма Павел Дуров признао је да ИСИС заиста користи Телеграм да би осигурао сигурност својих комуникација, али је додао: „Мислим да је на крају крајева приватност и наше право на приватност важније од страха да ће се лоше ствари догодити, попут тероризма."[185] Са аспекта криминалистичког поступања, ова изјава је забрињавајућа, јер немогућност прибављања чак и основних корисничких информација на овој платформи за комуникацију која је достигла број од 400 милиона месечних корисника умногоме везује руке безбедносним службама у праћењу појава које се везују за тероризам. Алгоритми који препознају и уклањају терористички садржај на платформи не могу остварити исти резултат као људски и технички капацитети безбедносних служби, које би податке тражиле искључиво на основу законитог захтева правосудних органа.

Још једна безбедна апликација за комуникацију коју су терористи прилагодили је „TrueCrypt". Један од припадника ИСИС-а, кога је француска полиција ухапсила у августу 2015. године, открио је детаље о овом програму. Реда Хаме, ИТ стручњак из Париза, који је путовао у Сирију да се придружи и бори на страни ИСИС-а, уместо тога, прошао је брзи курс за обуку и послат је назад у Француску како би извршио напад. Хаме је изнео детаље своје обуке за коришћење „TrueCrypt"-а, апликације за шифровање, као и да му је пре повратка у Француску, дат УСБ уређај који садржи тај програм. „TrueCrypt" је 2004. године покренуо Паул Ле Роук, програмер и криминалац, који је управљао светским картелом за продају

[183] Gabriel Weimann, „Terrorist Migration to the Dark Web", Terrorism Research Initiative, 2016., стр. 42, доступно на https://www.jstor.org/stable/pdf/26297596.pdf?refreqid=excelsior%3A85c63cb404e3dede02d74b93b6e77f6e, приступљено 02.05.2020. године.

[184] International Center for Counter-Terrorism (ICT),"The Telegram Chat Software as an Arena of Activity to Encourage the 'Lone Wolf ' Phenomenon", 2016., доступно на https://www.ict.org.il/Article/1673/the-telegram-chat-software-as-an-arena-of-activity-to-encourage-the-lone-wolf-phenomenon#gsc.tab=0, приступљено 02.05.2020. године.

[185] The Washington post, Sarah Kaplan: „Founder of app used by ISIS once said „We shouldn't feel guilty." On Wednesday he banned their accounts.", доступно на https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/founder-of-app-used-by-isis-once-said-we-shouldnt-feel-guilty-on-wednesday-he-banned-their-accounts/, приступљено 02.05.2020. године.

дроге, оружја и прање новца из базе на Филипинима. Ле Роук је ухапшен у Либерији под оптужбом за кријумчарење дроге у септембру 2012. године. Али „TrueCrypt" је и даље активан, што објашњава зашто га терористи ИСИС и даље користе за шифровану комуникацију и размену података.[186]

7.1. Биткоин као валута терористичких организација

Направљен 2009. године, Биткоин је криптографска P2P верзија електронског новца која омогућава плаћање путем Интернета заобилазећи традиционалне финансијске институције[187]. Вођени растућом жељом за монетарним режимом независним од финансијских регулатора трећих страна, творци Биткоина су развили децентрализовани систем плаћања који финансијски посредник попут банке, не подржава. Технологија која подржава Биткоин заснива се на „блокчејн" систему који делује као виртуална јавна књига која обрађује и проверава сваку Биткоин трансакцију у мрежи. Систем „блокчејн"-а је дефинисан као „запис свих потврђених трансакција груписаних у блокове, од којих је свака криптографски повезана са претходним трансакцијама све до првобитног блока, стварајући тако „ланац блокова".[188]

Кључна карактеристика Биткоина је његова децентрализована мрежа која нема централни ауторитет који обрађује или проверава трансакције, већ је уместо тога повезана путем ланца мрежа на блокчејн-у који проверава и потврђује сваку трансакцију. То значи да свако може располагати Биткоином без одласка у банку или другу финансијску институцију, што би захтевало пружање проверљивих личних података. Биткоини се стварају кроз процес „рударења" како би се верификовала свака трансакција на блокчејн-у. Рудари су одговорни за груписање непотврђених трансакција у нове блокове и њихово додавање у глобалну књигу тзв. блокчејн. Сваки нови блок који рудари додају у ланац подразумева награду за њих. Додатни блокови отежавају потенцијалном нападачу да реорганизује блокчејн и два пута потроши исту валуту. Иако се информације које се односе на сваку трансакцију бележе на блокчејн-у, ове информације нису

[186] Gabriel Weimann, „Terrorist Migration to the Dark Web", Terrorism Research Initiative, 2016., стр. 42., доступно на https://www.jstor.org/stable/pdf/26297596.pdf?refreqid=excelsior%3A85c63cb404e3dede02d74b93b6e77f6e, приступљено 02.05.2020. године.

[187] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System", доступно на https://bitcoin.org/bitcoin.pdf, приступљено 02.05.2020. године.

[188] Garrick Hileman, Michel Rauchs, „Global Cryptocurrency Benchmarking Study", 2017., стр. 13, доступно на https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, приступљено 02.05.2020. године.

директно повезане са именима, физичким адресама или другим идентификационим информацијама, што их чини анонимним у одређеној мери, што усложњава напоре агенција за спровођење закона да идентификују појединачне трансакције и повежу их са корисницима[189].

Терористи и криминалци користе Биткоин за незаконите трансакције, јер он нуди сличне предности као и систем „hawala". Биткоин пружа финансијску сигурност јер блокчејн делује као непристрасни посредник, осигуравајући да једном потрошена валута у трансакцији буде неопозива. Мрежа спречава сваки покушај опозива верификоване Биткоин трансакције, осим ако прималац заиста не врати тзв. токене назад пошиљаоцу.[190]

У овом контексту, то осигурава да се новац не може дуплирати унутар мреже. Мрежа „рудара" осигурава да је свака Биткоин трансакција јединствена и легитимна. Ако настане покушај дуплирања, блокчејн одбацује трансакцију као фалсификовану и неисправну, што користи и криминалцима и терористима који купују робу и услуге на Даркнет-у, јер нема ризика од преваре ривалске криминалне организације са друге стране мреже.

У јануару 2015. године, компанија за сајбер-безбедност „S2T" са седиштем у Сингапуру открила је конкретне доказе да је терористичка ћелија, за коју се претпоставља да је повезана са Исламском државом и делује у Америци, почела да прикупља средства путем Биткоина. Прималац донација, идентификован као Абу-Мустафа тврдио је да масовне акције америчких агенција за спровођење закона на главним финансијским платформама, заједно са недостатком финансијских и других ресурса доступних присталицама Исламске државе у САД и Јужној Америци, значи да би Даркнет требало да се користи за прикупљање средстава у Биткоину.[191] Абу-Мустафа је прикупио око пет Биткоина, у вредности тадашњих око хиљаду америчких долара, пре него што је налог затворен.[192]

---

189 *Ibidem.*

190 Rotman, S., „Bitcoin versus electronic money", CGAP, Вашингтон, 2014., доступно на https://www.cgap.org/sites/default/files/Brief-Bitcoin-versus-Electronic-Money-Jan-2014.pdf, приступљено 02.05.2020. године.

191 Harman D., „U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests", доступно на https://www.haaretz.com/.premium-isis-uses-bitcoin-for-fundraising-1.5366305,приступљено 02.05.2020. године.

192 Forbes, Nikita Malik: „How Criminals And Terrorists Use Cryptocurrency: And How To Stop It", доступно на https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#26f895623990, приступљено 02.05.2020. године.

У новембру 2017. години, примећен је покушај кампање на друштвеним мрежама у циљу финансирања тероризма путем Биткоина од стране организације под називом „Al-Sadaqah" (добровољно давање). Иако су првобитни Фејсбук налози брзо угашени, ова група је наставила да води кампању преко отворених Телеграм канала и Твитера.

Слика бр. 33: Студија случаја злоупотребе друштвених мрежа и платформи за комуникацију у циљу финансирања тероризма путем Биткоина

Убрзо након почетка кампање средства су почела да пристижу. До тренутка када више нису откривени налози под овим именом, ова групација је прикупила око 800 америчких долара у Биткоину.

Слика бр. 34. Студија случаја злоупотребе друштвених мрежа и платформи за комуникацију у циљу финансирања тероризма путем Биткоина[193]

[193] Malik, N. „Terror in the Dark", op. cit., стр. 41.

Други пример финансирања тероризма злоупотребом Биткоина десио се у Индонезији, где је џихадистичка група прикупљала донације како од домаћих, тако и од међународних донатора на Дарквебу, прикупљајући на тај начин око 600 хиљада америчких долара.[194]

7.2. Колико анонимности пружа Биткоин?

Терористи и криминалци користе Биткоин због његове анонимности. Међутим, Биткоин није тако анониман као што се уобичајено сматра, јер користи блокчејн систем који служи као виртуелни запис свих трансакција на мрежи. Блокчејн је јавно доступан, што значи да неко са довољним нивоом рачунарске писмености може да следи дигиталне отиске анонимних трговаца.[195] Због тога се Биткоин често користи на Даркнету са претраживачем „Тор" за већу сигурност и анонимност. У том контексту, криминалци користе криптовалуте зато што у финансијском окружењу пружа исти облик анонимности као енкрипција на комуникацијским платформама.[196] Оба система отежавају напоре безбедносних служби за откривање компликованих шифрованих веб сервиса и блокчејн плаћања на Интернету. Опасност од криптовалута истакли су Европол, Интерпол и Базелски институт за управљање, који су утврдили да „постоји јасан консензус да дигиталне валуте представљају прање новца и претњу за финансирање тероризма[197]. Током 2017. године, америчка влада је предложила да Министарство за унутрашњу безбедност (Department of Homeland Security) проучи везу између Биткоина и тероризма због нивоа анонимности које нуде ове криптовалуте зато што терористима пружа „приватност" коју траже[198].

Од свог објављивања 2009. године, Биткоин је доживео значајну нестабилност тржишне вредности. Стални скокови вредности тржишне цене Биткоина у оквиру нерегулисаног финансијског система

[194] Wimmer, Andreas, Aulia Nastiti, „Darknet, Social Media, and Extremism: Addressing Indonesian Counterterrorism on the Internet." Deutsches Asienforschungszentrum Asian Series Commentaries, Vol. 30-2015., стр. 5, доступно на https://www.academia.edu/20813843/Dark_net_Social_Media_and_Extremism_Addressing_Indonesian_Counter_terrorism_on_the_Internet, приступљено 02.05.2020. године.

[195] Rotman, S., „Bitcoin versus electronic money", op.cit., стр. 1-2.

[196] EUROPOL 2017 Internet Organised Crime Threat Assessment (IOCTA), стр. 49, доступно на https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017, приступљено 03.05.2020. године.

[197] Malik, N. „Terror in the Dark", op. cit., стр. 41.

[198] Coindesk, „US Congress to Announce Study on Virtual Currency Link to Terrorism Today", доступно на https://www.coindesk.com/us-congress-announce-study-virtual-currency-link-terrorism-today,приступљено 03.05.2020. године.

криптовалута могу примамити више криминалаца, укључујући терористе, да користе Биткоин. У новембру 2017. тржишна цена Биткоина достигла је 8 хиљада америчких долара, а скочила је на нешто више од 11 хиљада америчких долара почетком децембра 2017. године[199]. Међутим, вредност је пала почетком 2018. године. Министарство финансија Велике Британије покренуло је покушаје повећања регулације и захтева од корисника криптовалута и виртуелне размене валуте да открију свој идентитет. Верује се да ће ова мера вероватно ограничити анонимност Биткоина и самим тим смањити његову привлачност криминалцима.

[199] The Telegraph, „Treasury crackdown on Bitcoin over concerns it is used to launder money and dodge tax", доступно на https://www.telegraph.co.uk/news/2017/12/03/bitcoin-crackdown-amid-fears-money-laundering-tax-dodging/, приступљено 03.05.2020. године.

8. Преглед појединих он-лајн OSINT платформи

Постоји велики број Интернет платформи које олакшавају претрагу јавно доступних информација. Такве платформе се обично групишу на основу области које интересују онога ко претражује. Поред бесплатних, постоје и комерцијалне платформе које наплаћују услуге и дају боље резултате. У даљем тексту ће бити представљене поједине бесплатне платформе које могу допринети у евентуалним он-лајн истрагама.

8.1. Global Incident Map

Платформа која географски приказује извршене терористичке нападе и друге насилне акте у реалном времену. Има широк спектар параметара за претрагу као нпр. по природи напада, држави, региону, времену, конкретној локацији, броју жртава. Селекција конкретног резултата ће показати кратак опис инцидента и спољну везу ка медијским порталима са више детаља.

Слика бр. 35: Платформа Global Incident Map[200]

8.2. Global Terrorism Database

Глобална база података о тероризму (GTD) је јавно доступна база података која укључује информације о домаћим и међународним терористичким нападима широм света у периоду од 1970. до 2018. године и укључује више од 190.000 случајева. За сваки догађај доступне су информације о датуму и месту инцидента, коришћеном оружју и природи циља, броју жртава и - када се препознају - одговорној групи

[200] Доступно на https://www.globalincidentmap.com/, приступљено 05.05.2020.

или појединцу. Национални конзорцијум САД за проучавање тероризма и реаговања на тероризам (START[201]) ставља GTD на располагање путем Интернета у настојању да повећа разумевање терористичког насиља како би се лакше могло проучити и поразити.

Слика бр. 36: Платформа Global Terrorism Database[202]

8.3. One Million Tweet Map

Платформа „Мапа милион твитова“ представља алат за претрагу и истраживање друштвених мрежа која врши визуелизацију објава на друштвеној мрежи Твитер на мапи света у реалном времену. Као и горе наведени Global Incident Map, постоји велики број филтера за категоризацију „Твитова“ и „Хаштагова“.

Слика бр. 37: Платформа One Million Tweet Map [203]

[201] Доступно на https://www.start.umd.edu/, приступљено 05.05.2020. године.

[202] Доступно на https://www.start.umd.edu/gtd/, приступљено 05.05.2020. године.

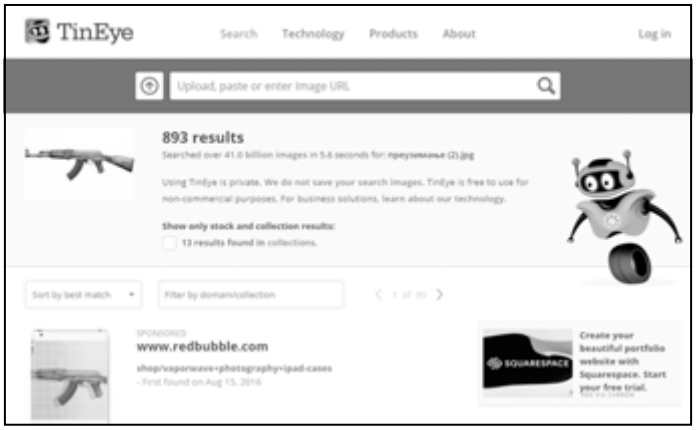
[203] Доступно на https://onemilliontweetmap.com/, приступљено 05.05.2020. године.

8.4. Wayback Machine

Wayback Machine је дигитална архива Интернета коју је креирала непрофитна организација са седиштем у Сан Франциску. Архива редовно посећује странице Интернета сваких неколико дана, недеља или месеци и архивира нове верзије уколико се садржај променио. Намера је да се садржај који би се иначе изгубио када год се страница битно измени или затвори, сачува и архивира, јер самим тим што је била објављена и што је неко могао видети као такву, постоји пуно право да се и сачува чак и ако је садржала неки спорни садржај.

Слика бр. 38: Платформа Wayback Machine [204]

8.5. Tineye



Слика бр. 39: Платформа Tineye [205]

[204] Доступно на https://archive.org/web/, приступљено 05.05.2020. године.

[205] Доступно на https://tineye.com/, приступљено 05.05.2020. године.

„Tineye“ (Тинај) је претраживач слика који је развијен од стране компаније са седиштем у Торонту у Канади. То је први претраживач слика на Интернету који користи технологију идентификације слика, а не кључних речи, метаподатака или водених жигова. Тинај омогућава корисницима да претражују Интернет користећи не кључне речи, већ слике. Након слања слике, Тинај ствара јединствени и компактни дигитални потпис слике и упоређује га са осталим индексираним сликама. Овај поступак може пронаћи погодак чак и са врло модификованим верзијама послате слике, али обично неће вратити сличне слике у резултатима.

8.6. Metapicz

Metapicz (Метапикс) је он-лајн платформа која омогућава читање EXIF метаподатака који се уписују у фотографију приликом њеног стварања. У зависности од фото-апарата, количина података који се уписују у фотографију могу варирати од основних као што су марка и модел апарата, па све до GPS координата, чак и позиције у којој се налазио апарат. Након учитавања фотографије, ова платформа ће прочитати и приказати расположиве EXIF метаподатке. Треба напоменути уколико се претражује фотографија која је претходно прошла кроз „филтере“ друштвених мрежа и апликација за комуникацију, ових података неће бити, из разлога што наведене платформе „пакују“ слике тако да заузимају што мање меморије на серверима, бришући на тај начин податке непотребне просечном кориснику, као и због најразличитијих примедби у погледу права, дужности и обавеза НВО и других актера.

Слика бр. 40: Платформа Metapicz [206]

[206] Доступно на http://metapicz.com/, приступљено 05.05.2020. године.

8.7. Start.me[207]

Платформа Start.me је користан менаџер пречица које олакшавају свакодневни рад на рачунару. Поред наведеног, она на једном месту сабира линкове ка великом броју корисних он-лајн ОСИНТ алата.

8.8. Други облици платформи

Неки од веома употребљивих платформи су:

- Social searcher https://www.social-searcher.com/
- Social Catfish https://socialcatfish.com/
- People looker https://www.peoplelooker.com/
- Truth Finder https://www.truthfinder.com/people-search/
- Brand 24 https://razorsocial.com/go/brand24aff/
- Tweet binder https://www.tweetbinder.com/

[207] Доступно на https://start.me/p/wMdQMQ/tools, приступљено 05.06.2024. године.

9. Високотехнолошки криминалитет, претње и безбедност у сајбер простору

Србија се последњих година суочава са алармантним порастом случајева високотехнолошког криминалитета (ВТК), што јасно показује званична статистика. Према Извештају Националног центра за превенцију безбедносних ризика у информационо-комуникационим (ИКТ) системима, током 2020. године забележено је око 26 милиона сајбер напада на ИКТ системе од посебног значаја. Најчешћи облици инцидената су покушаји неовлашћеног упада у ИКТ системе и прикупљање података без дозволе. Такође, од почетка 2022. године примећено је више случајева превара путем интернета, крађе идентитета и података корисника финансијских институција попут Рајфајзен банке и Поште Србије, као и учестале претње новинарима путем друштвених мрежа. У последње време масовно се и-мејл обавештавају о подметнутим бомбама у разним јавним и приватним институцијама као што су болнице, школе, аеродроми, железничке станице, тржни центри и зоолошки вртови. Иако се касније показало да су лажни, ови извештаји су изазвали забринутост у друштву и привремено пореметили нормално функционисање погођених институција.[208]

Високотехнолошки криминалитет и сајбер напади постали су неизбежни део савременог свакодневног живота, а очекује се да ће у будућности постати још сложенији и учесталији. Из тог разлога, кључно је да државни органи буду спремни да брзо и ефикасно одговоре на све изазове, ризике и претње, уз поштовање људских права и владавине права. Сарадња са другим државама и међународним организацијама, као што су ИНТЕРПОЛ и ЕУРОПОЛ, такође ће бити од суштинског значаја с обзиром на анонимност нападача и прекограничну природу ових облика криминала.

9.1. Појам и дефинисање високотехнолошког криминалитета

Развој савремених информационих технологија, рачунара, рачунарских мрежа и интернета значајно је утицао на све аспекте свакодневног живота људи, промењујући начине комуникације, пословања и доступности информација широм света. Овај напредак је такође довео до појаве нових видова криминалитета који се извршавају коришћењем рачунара и интернета, познатих као високотехнолошки криминалитет. Ова појава представља комплексан феномен који захтева детаљну анализу и разумевање.

[208] Павловић, М.: *Борба против високотехнолошког криминала у Србији, достигнућа и изазови*, Београдски центар за безбедносну политику, Београд, 2022, стр. 2.

У светлу ових догађаја, у научном и стручном кругу постојала је дилема о природи, карактеристикама, начинима извршења, жртвама и учиниоцима, као и процесима откривања и доказивања високотехнолошког криминалитета. Будући да се ради о релативно новом типу криминалитета који се наставља развијати, дебате о овој теми постају још интензивније и шире. Интересовање за различите облике криминалитета који користе рачунаре и интернет не опада.

Појава и развој високотехнолошког криминалитета (ВТК) прати се у контексту компјутерске ере, почевши од времена првих рачунара до преласка у деценију 1990-их година прошлог века, када је почела ера интернета. Ова еволуција се може поделити на два главна периода, прва фаза обухвата време од настанка првих рачунара до 1990. године, док је друга фаза доживела значајне промене и иновације обележене експанзијом Интернета.[209]

Током 60-их и 70-их година 20. века рачунари су почели да се интегришу у пословне и друге околности, што је довело до појаве високотехнолошког криминалитета, пре свега у финансијским сегментима, уз подршку искључиво интерних инсајдера. Ограничена дистрибуција рачунара и ограничена повезаност са другим системима ограничавали су могућности за вршење компјутерских злочина. У случају да су се десили, ова врста злочина се обично повезивала са мањим бројем (или чак једним) рачунаром и ужим кругом људи. Карактеристика кривичних дела у овом периоду била је њихова оријентација ка великим корпорацијама или државним органима, с обзиром да су они били главни корисници главних рачунарских система. Поред тога, примењене су и методе манипулације телефонским системима (*phone phreaking*) и социјални инжењеринг.[210]

У последњих неколико деценија, развој информационих технологија и њихова широка употреба у пословном и економском окружењу донела је нове изазове у борби против криминала. Феномен „белих оковратника", тј. криминалних дела која се извршавају у оквиру пословних и корпоративних окружења, претпостављао је промену у природи криминалних активности. У складу са развојем информатичких система и њиховом широком употребом, компјутерски програмери, оператери и инжењери електронике укључивали су се у извршење криминалних радњи. Феномен „компјутерског криминала" је постао суштински изразит у савременом друштву. Криминалне активности које се некада одвијале у стварном свету сада се пренеле у виртуелни простор. Методи, технике и облици

[209] Brenner, S. W.: *Cybercrime: criminal threats from cyberspace*, An Inprint ABC-CLIO, LLC, Santa Barbara, USA, 2010, стр. 9.

[210] *Ibid*, стр. 10-13.

извршења кривичних дела су се значајно променили, а време извршења се сада мери у терминима извршења компјутерских инструкција.[211]

Важно је напоменути да географска ограничења више нису пречка за извршење кривичних дела у свету компјутерских технологија. Оваква измена у динамици кривичних активности представља нове изазове за организације, владине агенције и институције у борби против криминала. У светлу ових измена, организације и владине агенције су суочене са потребом за адекватном припремом и мотивацијом за сузбијање компјутерског криминала. Неопходно је континуирано усавршавање и имплементирање стратегија и техника борбе против ове врсте криминала у оквиру савременог дигиталног друштва.

Почетком 21. века, сектор информационо-комуникационих технологија (ИКТ) еволуирао је у значајан бизнис на светском нивоу, који траје и данас. Са напретком у рачунарству и високим технологијама, употреба ових средстава више није ограничена на хаковање и малвер, већ се користи и за вршење традиционалних кривичних дела као што су превара, крађа, изнуда и крађа интелектуалне својине на нове начине. Ова тенденција носи мањи ризик за криминалце и потенцијално већи профит.[212]

Даљи напредак у ИКТ-у је резултирао повећањем броја рачунара, мобилних телефона и других преносивих уређаја, као и развојем Интернета ствари (ИоТ). Увођење бежичног интернета значајно је олакшало комуникацију.[213] Поред тога, развијено је рачунарство у облаку и протоколи за гласовну комуникацију преко Интернета, што је довело до нових могућности за криминалну употребу софтверских апликација, простора за складиштење података и информација. Рачунарство у облаку омогућава јефтино коришћење инфраструктуре провајдера, што смањује трошкове за криминалне елементе и олакшава извршење кривичних дела као што су напади преко ботнет мрежа и процеса који захтевају велику количину рачунарске снаге.[214]

У историји развоја информатичке технологије, дефинисање високотехнолошког криминалитета представљало је предмет константног промена и разматрања. Од свог почетка, овај појам је био суочен са проблемом

[211] Parker, D. B.: *Computer Crime: Criminal Justice Resource,* National Institute of Justice, Washington, 1989, стр. 21-22.

[212] Lagazio, M., Sherif, N., & Cushman, M.: A multi-level approach to understanding the impact of cyber crime on the financial sector, *Computers & Security*, 2014, 45, стр. 60.

[213] Grabosky, P.: The evolution of cybercrime, 2006-2016, In T. J. Holt (Ed.), *Cybercrime Through an Interdisciplinary Lens*. Routledge, NewYork, 2017, стр. 26.

[214] Wall, D. S.: *Cybercrime: The transformation of crime in the information age*, Polity Press, Cambridge, UK, 2007, стр- 538.

неуједначених термина који су се користили у различитим периодима развоја. Неусаглашеност у терминологији је довела до недостатка јасности и консензуса у дефинисању и објашњавању ВТК. У последњих неколико деценија, појава сајбер криминала и његов утицај на друштво и економију добија све већу пажњу. У складу са тим, израз који се користи да опише феномен ВТК је „сајбер криминал" или „компјутерски криминалитет". Ова промена у терминологији одражава његову еволуцију и контекстуализацију у савременом друштву.

Наука о компјутерском криминалитету, у једноставном смислу, представља област која се бави кривичним делима и преступима који укључују компјутере и информатичке технологије. Ова област истражује како злоупотреба компјутерских ресурса може угрозити приватност корисника, нарушити функционалност рачунарских мрежа и комуникационих система, и послужити као средство за извршење различитих криминалних активности. Постоји очигледна веза између степена друштвеног развоја и распрострањености различитих облика компјутерског криминала. У мери у којој друштво напредује и технологија се шири, тако се отвара и већи потенцијал за извршење криминалних дела. То може резултовати у порасту разноврсности и комплексности метода које се користе за извршење криминалних активности, као и у увећању броја и степена компетентности појединца који учествују у оваквим делатностима. Компјутерски криминалитет обухвата широк спектар активности, укључујући како активну тако и пасивну употребу рачунара. Осим тога, он такође укључује задржавање доказа који се односе на кривична дела, било да су извршена на компјутеру или у електронском формату. Лица која користе рачунар или се ослањају на његову функционалност могу бити класификована као потенцијалне жртве оваквих кривичних дела, што обухвата како физичка тако и правна лица.[215]

Дефинисање појма компјутерског криминалитета представља изазов због његове релативно нове природе, динамике и разноврсних облика извршења. Овај недостатак консензуса произилази из сложености овог феномена, који захтева стално ажурирање и прилагођавање законских и регулаторних оквира.[216] Компјутерски криминалитет се може дефинисати као облик криминалног понашања који користи рачунарску и информатичку технологију у извршењу кривичних дела или у коме се рачунар

[215] Вилић, В.: *Повреда права на приватност злоупотребе друштвених мрежа као облик компјутерског криминалитета - докторска дисертација*, Ниш, 2016, стр. 93.

[216] Бошковић, М.: *Криминологија*, Правни факултет за привреду и правосуђе, Нови Сад, 2020, стр. 361.

користи као средство за извршење кривичних дела. Овај феномен обухвата широк спектар активности које могу укључивати незаконит приступ рачунарским системима, крађу података, дистрибуцију злонамерног софтвера, интернет преваре и многе друге облике дигиталног криминала. Основна карактеристика компјутерског криминала је његова способност да користи технолошке алате и ресурсе за чињење кривичних дела на глобалном нивоу, често прекорачујући границе националних закона и ограничења надлежности.[217] Ово ствара додатне изазове у борби против овог облика криминала, који захтева међународну сарадњу и координацију између различитих агенција и организација. Узимајући у обзир наведене карактеристике, јасно је да дефинисање компјутерског криминала захтева пажљиво сагледавање контекста и последица које овај феномен може имати на друштво, привреду и појединце. Стога, напредак у разумевању и борби против компјутерског криминала захтева интердисциплинарни приступ који укључује правне, технолошке, социолошке и етичке перспективе.

Компјутерски криминалитет представља озбиљну претњу у савременом друштву, укључујући различите облике незаконитих радњи у вези са рачунарским системима. Ове радње могу имати за циљ уништавање, отуђење или оштећење рачунарских система или њихових делова. Такође, у категорију компјутерског криминала спадају радње као што су уништавање, оштећење, отуђење и неовлашћена модификација софтверских и програмских производа, као и података. Ове активности могу произвести широк спектар последица по појединце и организације, укључујући финансијске губитке, губитак података и безбедносне претње. Поред тога, компјутерски криминалитет обухвата и извршење кривичних дела коришћењем рачунарских система, као и неовлашћено коришћење рачунарских ресурса и нарушавање система безбедности.[218] Због тога је неопходно усмерити пажњу и ресурсе на борбу против оваквих активности, као и на унапређење система заштите и безбедности информационих технологија.

Током протеклих година, разумевање компјутерског криминала је претрпело значајне промене, одражавајући еволуцију употребе рачунара. Овај облик криминала укључује неправилну употребу рачунара и њихову све већу примену у различитим сферама. С обзиром да је компјутерски криминал релативно нова појава, која се развијала упоредо са брзим напретком технологије, недостатак адекватне законске регулативе додатно отежава дефинисање ове појаве, која представља изазов за правосудни систем.

---

[217] Алексић, Ж., Шкулић М.: *Криминалистика*, Службени гласник, Београд, 2007, стр. 385.

[218] Петровић, С.: *Компјутерски криминал*, Војно-издавачки завод, Београд, 2004, стр. 61-62.

9.2. Појавни облици високотехнолошког криминалитета

Анализирајући релевантне дефиниције у вези са високотехнолошким криминалом, уочавамо недостатак јединствене дефиниције и усклађености у погледу тога која дела и понашања треба третирати као део овог облика криминала. Слична је ситуација и са одређивањем манифестација. Наиме, многи аутори, приликом утврђивања појаве високотехнолошког криминала, користе два приступа: један полази од општег појма сајбер криминала и обухвата све радње које имају карактеристике специфичне за ову појаву или појам, док други примењују метод набрајања, где они наводе или групне радње које се подразумевају под сајбер криминалом.

У документу Уједињених нација под називом „*Злочин у вези са рачунарским мрежама*" (енгл. *Crimes related to computer networks*), усвојеном на Десетом конгресу 2000. године, поред дефиниције сајбер криминала, наведени су и специфични облици овог кривичног дела у складу са Препоруком Савета Европе и листа ОЕЦД-а из 1989. и 1985. године. У ужем смислу, то су: неовлашћени приступ рачунарском систему или мрежи, кршењем мера безбедности (хаковање); оштећење рачунарских података или програма; компјутерска саботажа; неовлашћено коришћење комуникација из и у рачунарским системима и мрежама; компјутерска шпијунажа.[219]

Законодавство Републике Србије у потпуности препознаје озбиљност ових дела, дефинишући их као кривично дело у складу са Кривичним закоником.

Кривично дело *оштећење рачунарског система или података* има за последицу угрожавање заштићеног добра, што може резултирати озбиљним последицама по појединца, предузеће или чак цело друштво. То може довести до губитка података, нарушавања приватности, финансијских губитака или поремећаја у функционисању јавних услуга.[220]

Компјутерска саботажа, позната и као рачунарска саботажа, представља серију акција које се односе на манипулацију, уништење или преусмеравање рачунарских података или програма са циљем ометања нормалног функционисања рачунара. Овај облик саботаже може обухватити различите активности, укључујући брисање важних информација,

[219] United Nations: Crimes related to computer networks: background paper for the Workshop on Crimes related to the Computer Network, 2000, доступно на: https://digitallibrary.un.org/record/432653?v=pdf [10.04.2024.]

[220] Кривични законик Републике Србије, *Службени гласник РС*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019, чл. 298.

мењање података или програма, као и упаде у рачунарски систем ради ометања нормалног рада. Саботаже могу причинити оштећења на самом рачунару или другим уређајима за обраду података у систему. Ове активности могу имати различите циљеве, укључујући уклањање или онемогућавање приступа важним информацијама, штете компанији или организацији која користи рачунарски систем, као и кражу података за личне или финансијске користи.[221]

Са повећаном употребом рачунарских система, такође се повећава и ризик од рачунарских злочина, укључујући и *прављење и уношење рачунарских вируса*. Прављење и уношење рачунарских вируса представља озбиљан криминални чин који може проузроковати озбиљне последице, како за појединце, тако и за организације. Овај облик криминала се кажњава законом, а постоје различити облици и тежине овог дела, зависно од намера и последица које произилазе из напада. Особа која ствара рачунарски вирус са намером да га унесе у туђи рачунар или рачунарску мрежу чини основни облик овог кривичног дела. Сам чин прављења вируса представља основну радњу извршења овог дела. Рачунарски вируси су софтверски програми који имају способност да се реплицирају и шире штетне ефекте по систем у који су унети. Њихове врсте и карактеристике могу бити различите, а њихова сврха може бити разнолика - од крађе података до онеспособљавања система.[222]

Рачунарска превара је озбиљан проблем савременог друштва. Ова врста компјутерског криминала обухвата различите методе и технике којима се остварује финансијска корист за учиниоца или за неког другог. Мотиви за извршење овог кривичног дела могу бити различити, укључујући финансијску корист, личну корист или штету другима. Овај чин се обично спроводи уношењем нетачних података у рачунарску мрежу или систем, или неуношењем тачних података. Понекад се сам компјутерски систем манипулише или злоупотребљава да би се постигао циљ преваре. На пример, електронски системи могу бити хаковани ради добијања приступа финансијским подацима, преваре електронских плаћања или фалсификовања информација да би се стекла незаслужена корист. Овакве активности наносе штету појединцима, компанијама и друштву у целини. Поред финансијских губитака, компјутерска превара може проузроковати и кршење приватности, претње безбедности података, губитак пословног и јавног поверења у интернет и електронске системе.[223]

[221] Бошковић, М.: нав. дело, 2020, стр. 368.

[222] Кривични законик, чл. 300.

[223] Бошковић, М.: нав. дело, 2020, стр. 368.

Хакинг криминалитет представља озбиљну претњу за целокупну безбедност у дигиталном окружењу. Кривична дела која су повезана са хакерским активностима обухватају неовлашћени приступ рачунарским системима и базама података. Особе које се баве оваквим радњама, познате као хакери, често имају различите мотиве као што су жеља за авантуром, потврђивање својих вештина или чак само за забаву. Међутим, и покушаји хаковања из незлонамерних мотива могу имати озбиљне последице. Неупотребљивање личних података, угрожавање приватности, као и штете пословним системима, су само неки од потенцијалних ризика. Често путем хаковања се угрожавају не само рачунарски системи већ и особе или компаније које користе те системе.[224]

Спречавање и ограничавање приступа јавној рачунарској мрежи представља сериозно кривично дело које има за циљ да заштити интегритет и безбедност информационих система који су кључни за функционисање различитих институција и организација. Овај вид кривичног дела може се појавити у различитим облицима, од једноставних акта неовлашћеног спречавања или ометања приступа јавној рачунарској мрежи, до озбиљнијих случајева када је у питању злоупотреба службеног положаја. У основном облику кривичног дела, лице које неовлашћено спречава или омета приступ јавној рачунарској мрежи може бити кажњено новчаном казном или затвором до једне године. Ово се односи на случајеве када неко намерно блокира или пречи у нормалном коришћењу рачунарске мреже која је од јавног значаја. У случају да је учинилац овог дела службено лице, а као такав користи свој положај да спречи или омете приступ јавној рачунарској мрежи, ради се о квалификованом делу. Таква злоупотреба службеног положаја може имати озбиљне последице по безбедност и функционисање рачунарских мрежа, због чега је предвиђена казна затвора до три године.[225]

Компјутерске злоупотребе, познате и као компјутерске крађе или неовлашћено коришћење рачунара и рачунарских мрежа према домаћем законодавству, представљају озбиљан проблем који често има озбиљне последице. Овај облик криминала је чест и носи са собом велике економске и имовинске губитке. Овај облик криминала укључује разне активности као што су уношење, мењање, брисање или ометање рачунарских података или програма, с намером да се оствари незаконита економска добит. Последице оваквих дела могу бити разнолике, од директних финансијских губитака до штете по репутацију појединаца

[224] *Ibid*, стр. 366.

[225] Кривични законик, чл. 303.

или компанија. Један од најчешћих облика компјутерских злоупотреба, који такође има озбиљне последице, јесте злоупотреба крађе идентитета. Ово представља ситуацију у којој се неовлашћено користи идентитет неке особе ради остваривања користи или извршавања разних криминалних активности. То може укључивати крађу личних података попут имена, адресе, бројева личних докумената или банковних информација, што може довести до великих проблема за жртву, укључујући финансијске губитке, кршење приватности, па чак и правне проблеме.[226]

Надаље, битно је напоменути и феномен компјутерског прислушкивања укључује скривене методе снимања визуелног садржаја приказаног на монитору рачунара појединца. Ово се може постићи коришћењем видео опреме или повезивањем на монитор за праћење приказаних информација. Важно је напоменути да се компјутерско прислушкивање разликује од неовлашћеног приступа, јер укључује праћење информација без могућности манипулисања или одабира материјала који се преноси. Неовлашћено коришћење рачунарских ресурса обухвата активности као што су личне и комерцијалне активности, коришћење рачунарског хардвера и софтвера у приватне сврхе, као и учешће у рекреативним активностима на рачунару током радног времена.[227] Људи одговорни за ове злоупотребе су често запослени у компјутерским одељењима, укључујући оператере и програмере, који имају овлашћени приступ. Такве активности могу укључивати модификацију или уништавање рачунарских информација, ометање или ограничавање приступа овлашћеним корисницима. Мотивације за ове акције могу бити различите, укључујући личне освете, политичке факторе или незадовољство фирмом или колегама.

9.3. Криминалитет у виртуелном простору - претње и безбедност

Дефинисање сајбер простора

Да би се могао разумети сам појам компјутерског криминалитета, потребно је, пре свега, појаснити и дефинисати појам сајбер (онлајн) простора, у коме ове претње и облици овог криминалитета настају. У савременом друштву, са напретком технологије и информационих система, долази до веће глобалне повезаности, услед чега је употреба информационих технологија постала свакодневница, па настају многобројне и велике

[226] Бошковић, М.: нав. дело, 2020, стр. 367.

[227] Николић-Ристановић, В., Константиновић Вилић, С.: *Криминологија*, Прометеј, 2018, стр. 175.

промене у животу и раду људи. У једном таквом окружењу, долази до стварања тзв. сајбер простора, који се може објаснити појашњењем речи „сајбер" и „простор". Под термином сајбер, Гибсон (1984) подразумева оно што је виртуелно, невидљиво, неограничено, базирано на технологији.[228] Реч простор се може различито дефинисати, с обзиром на то да не постоји његова јединствена и општеприхваћена дефиниција.

Ипак, појам сајбер простора, како наводи Гибсон (1984), може се представити као свет рачунарских мрежа, у коме компаније, друштва и други субјекти теже да прикупе што више информација и података. Стога, сам сајбер простор, може се разумети као врста заједнице, у оквиру које су елементи реалног друштва приказани у виду битова и бајтова, путем рачунарских мрежа.[229]

Тасић и Бауер (2003) у оквиру „Речника компјутерских термина", објашњавају сајбер простор као окружење виртуелне реалности, у оквиру кога су особе повезане путем рачунарских мрежа и на тај начин обављају међусобну комуникацију.[230]

Америчко министарство одбране (*Department of Defence – DoD*) предлаже дефиницију сајбер простора као подручје у оквиру информационог окружења, које је састављено из информационе и мрежне инфраструктуре, која подразумева Интернет, телекомуникационе мреже, рачунарске системе, њихове процесоре и контролере. Ово се може разумети и као виртуелно окружење, у коме се путем рачунарских мрежа дигитални подаци преносе.[231]

На основу свега наведеног, може се извести општи закључак о појму сајбер простора, који подразумева да је то нематеријални, неограничен и виртуелни простор који је креиран од стране рачунарских мрежа. Дакле, овај појам настаје вештачким путем, односно, као последица развоја људског друштва, те све веће потребе за унапређењем комуникације, повезивање људи, као и деловањем технолошких иновација. Сајбер простор доводи до повећања могућности за размену информација и података, ефикасно и лако, па представља примаран комуникациони медиј у савременом глобалном друштву.[232]

[228] Вулетић, Д.: *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 9.

[229] Према: Parsons, T.: *Društva*, August Cesarec, Zagreb, 1998.

[230] Тасић, В., Бауер, И.: *Речник комјутерских термина*, Микро књига, Београд, 2003, стр. 373.

[231] Joint Publication 1-02: *DoD Dictionary of Military Terms*, DC: Joint Staff, Joint Doctrine Division, Washington, J-7, USA, 2008.

[232] Вулетић, Д.: нав. дело, 2010, стр. 10.

Рачунарске мреже доводе до великог напретка људске заједнице, те омогућавају ефикасну комуникацију, размену информација и обављање пословања, али исто тако садржи и своје негативне тенденције. Сајбер простор, колико год позитивно деловао на друштвену заједницу, не представља реалну заједницу, већ склоп виртуелног и вештачки створеног места.[233] Стога, бројни су аутори који наводе недостатке овог концепта, као и страх да ће се људи учешћем у виртуелним заједницима удаљити од реалног живота.[234] Са друге стране, постоје и они који сматрају да је улога сајбер простора позитивна, те да исти представља склоп новог и квалитетног. Са једне стране преставља својеврсну бибилотеку, неисцрпан извор информација и размене података, али са друге, тамне стране, истовремено је и извор негативних деловања, услед представљања порнографије на мрежи, политичког злостављања или иницирања пропаганди било које врсте.[235]

Према наведеном, може се закључити да је сајбер простор доступан свима, па као виртуелна заједница захтева поседовање рачунарских система и употребу информационих технологија. Без обзира на његове бројне користи по људско друштво, не могу се оспорити ни негативне последице које деловање у оквиру овог простора, носи са собом.

9.3.1. Појам и карактеристике сајбер претњи

Сајбер претње представљају један од највећих изазова за корпорације и државне владе данас. Оне не само да угрожавају безбедност информационих система, већ и наносе оштећења која могу имати далекосежне последице по бизнисе и друштво у целини. Политичари с правом упоређују сајбер нападе с терористичким актима, јер оба типа претњи захтевају брзу и ефикасну реакцију.[236]За разлику од традиционалних физичких напада, сајбер напади могу бити изведени из било ког дела света и прикривени тако да је тешко утврдити идентитет нападача. Ови напади могу обухватити широк спектар акција. Њихов обим и савремени методи за избегавање откривања чине их особито опасним за циљеве.

---

[233] Kollock, P., Smith, M.: *Communities in cyberspace*, Routledge, New York, 2001, стр. 32.

[234] Wellman, B., Gulia, M.: Virtual communities as communities – Net surfers don't ride alone, In Kollock P., Smith M., (ed) *Communities in cyberspace*, Routledge, New York, 2001, стр. 35.

[235] Ериксен, Т.: *Тиранија тренутка: брзо и споро време у информационом друштву*, Библиотека XX века, Београд, 2003, стр. 45.

[236] Walker, J., Williams, B., Skelton, G.: Cyber security for emergency management, Proceedings of the *IEEE International Conference on Technologies for Homeland Security*, 2010, стр. 477.

Један од највећих изазова у борби против сајбер претњи јесте идентификација и филтрирање злонамерних е-порука и порука које изгледају као оригиналне, али у себи носе штетне везе или прилоге. Такве поруке могу изазвати велике проблеме у системима безбедности, јер се често примаоци налазе у немогућности да их довољно брзо идентификују и блокирају.[237]

Најновији облик ових напада је превара путем е-поште, где се поруке маскирају тако да изгледају као да долазе од поузданих извора или познатих особа. Овај облик напада има за циљ да привуче кориснике и наведе их да отворе лажне веб странице које изгледају као оригиналне, али су наравно направљене са циљем да се украду корисничка идентификација, лозинке или финансијске информације. Ови напади могу имати различите облике, али један од најчешћих је усмеравање корисника на лажну веб локацију која веома личи на легитимну веб локацију.[238]

Уобичајен, али сложенији напад укључује дистрибуирано ускраћивање услуге, у којем се рачунарским системима шаљу велике количине саобраћаја који троше њихове ресурсе и узрокују њихов крах. Ови напади су ефикасни јер се легитимни захтеви за ресурсима и лоши захтеви, често не разликују, што отежава блокирање напада.[239] Друга техника је напад који подразумева мешање злонамерног кода између компоненти система како би се убациле измишљене команде или одговори. Овакав напад може имати различите ефекте, од крађе информација до прекида система, а исти се може ублажити коришћењем протокола за аутентификацију како би се осигурало да комуникација стигне до намењеног примаоца.[240]

Пракса показује да напади на рачунарске системе углавном представљају комбинацију неколико врста напада. У студији коју је спровео Вулетић (2017) разматране су различите врсте напада којима су рачунарски системи изложени. Ови напади представљају озбиљну претњу

[237] Kartaltepe, E., Xi, S.: Towards blocking outgoing malicious impostor emails, Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006, стр. 659.

[238] Yu, W., Nargundkar, S., Tiruthani, N.: A phishing vulnerability analysis of web-based systems, *Proceedings of the IEEE Symposium on Computers and Communications*, 2008, 326–331.

[239] Al Islam, A., Sabrina, T.: Detection of various denial-of-service and distributed denial-of-service attacks using RNN ensemble, *Proceedings of the Twelfth International Conference on Computers and Information Technology*, 2009, стр. 604.

[240] Guha, R., Furqan, Z., Muhammad, S: Discovering man-in-the-middle attacks on authentication protocols, *Proceedings of the IEEE Military Communications Conference*, 2007, 1-7.

безбедности мреже и података, а њихови утицаји могу бити широки и штетни. Прва врста напада, напад ускраћивањем услуга (енгл. *Denial-of-Service* - DoS), има за циљ да прекооптерети мрежни систем, што резултује падом конекције и спречава легалне кориснике да приступе мрежи. Најчешћи начин извршења овог напада је шаљење великог броја захтева серверу, што омета његово нормално функционисање. Други напад је преко *ботнета* (енгл. *bots*, скраћено од *robots*), где су компјутерски системи инфицирани програмима који омогућавају неовлашћеним лицима да преузму контролу над њима. Ови ботови се користе за нападе на безбедност земаља и њихове критичне инфраструктуре. Фишинг (енгл. *phishing*) представља напад на Интернету који се изводи путем лажних порука електронске поште или других Интернет сервиса, са циљем да се добију поверљиве информације од корисника. Спем (енгл. *spam*) је непожељна електронска пошта која се шаље без сагласности корисника, а често може садржати малициозне софтвере који могу угрозити систем. Социјални инжењеринг (енгл. *social engineering*) представља технику манипулације људима да би се добиле информације које би омогућиле приступ системима. Снифинг (енгл. *sniffing*) и спуфинг (енгл. *spoofing*) су напади којима се прикупљају информације или се креира утисак да је пренос извршен од стране овлашћеног корисника. Коначно, злоћудни програми представљају софтвере који наносе штету рачунарским системима, укључујући вирусе, црве, тројанце, шпијунске програме и друге.[241] Ови напади захтевају посебну пажњу и мере заштите како би се смањили њихови потенцијални утицаји на безбедност и функционалност рачунарских система.

9.3.2. Безбедност и заштита у сајбер простору

У сфери информационе безбедности, важно је разумети значај и примену дубинске одбране. Та стратегија обухвата три нивоа безбедности - низак, средњи и висок - сваки од којих је нацртан са одређеним корисничким профилима на уму. Низак ниво је предвиђен за особе које имају основне приступне праве и обављају рутинске пословне задатке. Средњи и висок ниво обезбеђују додатни слој сигурности, што је од кључног значаја за посебне корисничке категорије, као што су администратори и менаџери, чији приступ инфраструктурним ресурсима је значајно више. Управо због ове повећане осетљивости система, дубинска одбрана се описује као

[241] Вулетић, Д.: *Сајбер безбедност. Интегрална безбедност Републике Србије*, Факултет за пословне студије и право, Факултет за стратешки и оперативни менаџмент, Универзитет „Унион-Никола Тесла“, Београд, 2017, стр. 176-181.

стратегија која подразумева непрекидно праћење и идентификацију потенцијалних упада на различитим нивоима инфраструктуре. Ово обезбеђује рани детектовање неовлашћених активности и ефикасно издаје упозорења, што значајно повећава отпорност система на потенцијалне претње.[242]

Системи који се користе за детекцију упада у рачунарске системе обично функционишу на два основна начина: детекцијом аномалија и детекцијом заснованом на потписима. Детекција аномалија се односи на праћење и откривање необичног или абнормалног понашања у мрежи или систему. С друге стране, детекција заснована на потписима користи познате потписе напада како би идентификовала присуство познатих угрожавајућих активности. Међутим, један од изазова оваквих система је што они могу бити неефикасни у откривању нових, раније непознатих напада који не одговарају уобичајеним потписима. Због тога, за ефикасну заштиту, неопходно је имплементирати различите системе заштите који користе комбинацију ових метода и других напредних техника.[243]

У оквиру безбедности рачунарских мрежа, истраживачи и стручњаци се суочавају са изазовима у решавању безбедносних проблема који угрожавају критичне инфраструктуре. Класични приступи предлажу различите методе за одређивање и решавање ових проблема. На пример, један од таквих приступа укључује употребу вишеструких (паралелних) система за детекцију упада. Ови системи имају дизајн који омогућава паралелни рад и на тај начин повећава ефикасност детекције трпећи оптерећење. Међутим, овакав приступ не увек доводи до значајних побољшања у перформансама безбедности у односу на различите типове напада који се могу појавити.[244] Други приступ укључује употребу система за откривање упада који интегришу различите технологије за откривање упада из унутрашњих и екстерних извора. Овакви системи играју значајну улогу у борби против различитих претњи, укључујући и претње које су мотивисане инсајдерима и оне које долазе из спољашњег окружења.[245]

---

[242] Zhang, Y., Deng, F.,. Chen, Z., Xue, Y., Lin, C.: UTM-CM: A practical control mechanism solution for UTM systems, *Proceedings of the IEEE International Conference on Communications and Mobile Computing*, 2010, стр. 88.

[243] Li, P., Wang, Z., Tan, X.: Characteristic analysis of virus spreading in ad hoc networks, *Proceedings of the International Conference on Computational Intelligence and Security Workshops*, 2007, стр. 539.

[244] Shiri, F. I., Bharanidharan S., Norbik B. I.: A parallel technique for improving the performance of signature-based network intrusion detection system, *IEEE 3rd International Conference on Communication Software and Networks*, 2011, стр. 694.

[245] Wen, W.: An improved intrusion detection system, *Proceedings of the International Conference on Computer Applications and System Modeling*, 2010, 5, стр. 213.

Интеграција различитих технологија за откривање упада помаже у стварању сложених и ефикасних безбедносних система, што је од кључног значаја за заштиту критичне инфраструктуре од потенцијалних напада и претњи.

Поједини аутори представљају и иновативан приступ у откривању сложених напада на критичне рачунарске системе. Овај приступ карактерише комбинација метода заснованих на потпису и детекције упада са анализом стања. Поред фокусирања на откривање упада у мрежу, истраживачи су такође посветили пажњу праћењу и документовању напада који су успели да пробију безбедност мреже. Ово се постиже посебном анализом и откривањем аномалија у систему.[246] За успешну примену овог приступа неопходна је детаљна анализа нормалних услова рада, што омогућава успостављање основних стандарда и ограничења за идентификацију неуобичајених активности.

9.3.3. Правна регулатива за борбу против сајбер криминалитета

Међународни правни оквир

Компјутерски (сајбер) криминал је све више заступљен у савременим условима напретка људског друштва, те узрокује настанак бројних кривичних дела из ове области. У ту сврху, потреба за његовим правним дефинисањем и законском регулацијом, све више добија на значају.

Најзначајнији правни документи који се односе на сузбијање и спречавање настанка компјутерског криминалитета настали су под окриљем ОУН, Савета Европе и Европске Уније. Осим тога, постоји још низ других организација и иницијатива које се залажу за борбу против сајбер криминала, као што су: Интерпол, Канцеларија Уједињених нација за борбу против дроге и криминала (UNODC - *United Nations Office on Drugs and Crime*), група држава званих Г-8: Организација америчких држава (OAS - *Organization of American States*); Организација за економску сарадњу Азије и Пацифика (APEC - *Asia Pacific Economic Cooperation*), Организација за економску сарадњу и развој (OECD - *The Organization for Economic Cooperation and Development*), Организација за европску безбедност и сарадњу (OEBS – *Organizacion for Security and Co-operation in Europe*) и др.

У борби против компјутерског криминала, Уједињене нације су предузеле важне кораке у усвајању резолуција и принципа који се баве овим

[246] Nai Fovino, I., Masera, M., Guidi, L., Carpi, G.: An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. *IEEE 3rd Conference on Human System Interactions (HSI)*, 2010, 679-686.

изазовом у савременом друштву. Почев од 1990. године, када је на VII Конгресу УН прихваћена Резолуција о законодавству у области компјутерског криминала[247], фокус је био на превенцији криминала и одговарајућим мерама против кривичних дела.

Након тога, 1994. године усвојен је Приручник ОУН о спречавању и контроли компјутерског криминала[248], што је допринело бољем разумевању и усмеравању решења за борбу против ове врсте криминала. Надаље, у мају 1998. године у Женеви је усвојена Женевска резолуција о злоупотреби интернета у сврху сексуалне експлоатације.[249] Ова резолуција има за циљ да регулише питање трговине људима, проституције и сексуалне експлоатације на интернету.

Од 2000. године, када су Уједињене нације први пут усвојиле Резолуцију о борби против злоупотребе информационих технологија[250], па се до данас наставило усвајање законских аката и мера које су се бавиле овим проблемом. Кроз Резолуцију 2007/20, Уједињене нације препоручиле свим државама да ојачају своје правне механизме и законске оквире у области безбедности рачунарских система, што је реакција на пораст криминалних дела која су се одигравала у виртуелном свету.[251] Затим, Резолуција 65/230 из 2010. године наставила је овај напор, фокусирајући се на неопходност анализе компјутерског криминала и сигурности рачунарских система.[252] Циљ ових акција био је да се препознају

[247] United Nations: UN resolution on computer crime legislation, (Резолуција Уједињених Нација о законодавству у области компјутерског криминалитета), доступно на: http://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.14 [05.04.2024.]

[248] United Nations: Manual on the Prevention and Control of Computer-related Crime, (Приручник УН о спречавању и контроли компјутерског криминала), 1994, доступно на: http://www.uncjin.org/Documents/EighthCongress.html [05.04.2024.]

[249] United Nations: Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation, (Резолуција Уједињених Нација (тзв. Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације), 1998, доступно на: http://www.uri.edu/artsci/wms/hughes/ppr.htm [05.04.2024.]

[250] United Nations: UN resolution A/res/55/63 on combating the criminal misuse of information technologies, (Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија), 2000, доступно на: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [05.04.2024.]

[251] United Nations: Resolution 2007/20 of July 26, 2007, (Резолуција 2007/20 од 26. 07. 2007. године), 2007, доступно на: http://www.un.org/.../ecosoc/.../2007 [05.04.2024.]

[252] United Nations: UN General Assembly resolution 65/230, (Резолуција Уједињених Нација 65/230), 2010, доступно на: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [05.04.2024.]

слабости у борби против кибер криминала и да се пронађу начини за њихово савладавање. Формирање групе експерата за анализу компјутерског криминала у различитим земљама имало је за циљ да укаже на могућности за унапређење безбедности рачунарских система на националном нивоу.

Европска унија је, такође, важан актер у борби против криминала на интернету и заштити информационих система. Европска унија је у сарадњи са својим чланицама увела различите мере које имају за циљ регулисање приступа информационим системима и обезбеђивање безбедности података. На пример, одлука о нападима на информационе системе, која је ступила на снагу 2005. године, представља значајан корак у том правцу.[253] Ова одлука има за циљ прописивање стандарда за безбедност информационих система, регулисање приступа овим системима, као и увођење санкција за лица која врше кривична дела у сајбер простору. Ове и сличне иницијативе представљају значајан допринос заштити интернет простора и безбедности података у Европи.

Од правних инструмената насталих у оквирима Европске уније треба поменути три директиве: Директива о правној заштити компјутерских програма, Директива о чувању података који су добијени или обрађени приликом пружања јавно доступних услуга електронске комуникације или јавних комуникационих мрежа и Директива 2013/40/EU.

Домаћа правна регулатива

Након што је извршила потписивање Конвенције о високотехнолошком криминалу, као и Додатни протокол 2005. године, а затим и ретификацијом исте у 2009. години, Република Србија на себе је преузела одговорност да ради на регулисању законских оквира и докумената који ће дефинисати област компјутерског криминалитета и последице за кривична дела. Међу најбитнија правна документа чије одредбе имају утицаја и на области сајбер криминала која су донета у Републици Србији, могу се издвојити следећа:

1) Кривични законик Републике Србије,
2) Законик о кривичном поступку Републике Србије[254],

[253] European Union: Framework Decision on attacks against information systems of the Commission of the European Communities, (Оквирна одлука о нападима на информационе системе Комисије европских заједница), 2005, доступно на: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN [05.04.2024.]

[254] Закон о кривичном поступку, *Службени гласник РС*, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – одлука УС и 62/2021 – одлука УС.

3) Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[255],
4) Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима[256],
5) Закон о ауторским и сродним правима[257],
6) Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине[258].

Осим поменутих закона који регулишу област компјутерског криминалитета, треба напоменути и законе донете у Републици Србији који се односе на регулацију електронског пословања, које постаје примаран начин пословања, како физичких, тако и правних лица. Овде спадају следећи законски акти:

1) Закон о електронском потпису[259],
2) Закон о електронској трговини[260],
3) Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању[261] и
4) Закон о оптичким дисковима[262].

У светлу потребе за ефикасним сузбијањем компјутерског криминала у Републици Србији, важно је истаћи значај институција које су одговорне за спровођење одговарајућих закона и мера заштите од овог облика криминала. Државни органи имају кључну улогу у овом процесу, са циљем да допринесу повећању безбедности и смањењу ризика и инцидената у вези са компјутерским криминалом у земљи. Успешно спровођење мера за сузбијање компјутерског криминала захтева не само постојање одговарајућих законских инструмената, већ и обуку и специјализацију државних и надлежних органа. Поред тога, значајан допринос у овој борби имају институције попут Министарства трговине, туризма и веза, Републичке

[255] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Службени гласник РС*, бр.61/2005 и 104/2009.

[256] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, *Службени гласник РС*, бр. 32/2013.

[257] Закон о ауторским и сродним правима, *Службени гласник РС* бр. 104/2009, 99/2011, 119/2012, 29/2016 – одлука УС и 66/2019.

[258] Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, *Службени гласник РС*, бр. 46/2006, 104/2009 – др. закони и 129/2021.

[259] Закон о електронском потпису, *Службени гласник РС*, бр.135/2004.

[260] Закон о електронској трговини, *Службени гласник РС*, бр. 41/2009, 95/2013 и 52/2019.

[261] Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, *Службени гласник РС*, бр. 94/2017 и 52/2021.

[262] Закон о оптичким дисковима, *Службени гласник РС*, 52/2011.

агенције за електронске комуникације (РАТЕЛ) и Републичке радиодифузне агенције (РРА). Њихова сарадња и координација су од суштинског значаја за ефикасно супротстављање сајбер криминалу.

Континуирано унапређење и изградња капацитета ових институција је императив у борби против компјутерског криминала. Само јединством напора и сарадњом свих надлежних органа може се обезбедити да безбедност од ових савремених претњи.

10. Малолетници и сајбер криминал

10.1. Појам малолетног лица

Када се разматра питање малолетника, важно је узети у обзир различите аспекте који утичу на њихово дефинисање у законодавству. Различите правне норме у различитим земљама имају своје критеријуме за одређивање малолетника, што открива разноликост приступа овом питању. Најчешће се као основа за дефинисање малолетника користи календарски узраст, тј. број достигнутих година, али се узима у обзир и биолошки развој, психолошки развој и друштвена зрелост.[263] У многим законима, малолетници су лица која су навршила 14 година у време извршења кривичног дела, али још нису навршила 18 година. Детаљније, особе млађе од 14 година сматрају се децом, док се особе које су навршиле 18 година тумаче као одрасле особе.[264]

Важно је напоменути да се концепт малолетника може разликовати од земље до земље. На пример, у неким земљама, попут Сједињених Држава, пунолетство се достиже са 21. годином, што илуструје различите културне и правне приступе овом питању. У складу са важећим законодавством у Србији, малолетним је лице које је навршило 14 година, а пунолетство са 18 година. Такве одредбе се налазе у разним законима, као што су Кривични законик Србије, Закон о малолетним преступницима и кривичноправној заштити малолетника, као и Породични закон.[265]

Утврђивање статуса малолетника је кључни корак у судском процесу, посебно када су или жртве или извршиоци кривичних дела. Разликујемо их у две главне категорије: млађе малолетнике, који имају између 14 и 16 година, и старије малолетнике, који имају између 16 и 18 година, посебно је интересантан третман лица која спадају у категорију млађих пунолетних лица (18-21 година) који се изједначују у статусу и кривично – правном третману, са малолетним лицима, најпре оним од 16 до 18 година.

Правна заштита малолетника регулисана је низом прописа, укључујући Законик о кривичном поступку, Закон о малолетним учиниоцима кривичних дела и кривичној заштити малолетника, као и Закон о извршењу кривичних санкција. Ови прописи предвиђају посебне поступке

[263] Константиновић Вилић, С., Николић Ристановић, В., Костић, М.: *Криминологија*, Ниш, 2012, стр. 221.

[264] Прља, Д., Кораћ, В: Малолетници и сајбер криминал, У: *Малолетници као учиниоци и жртве кривичних дела и прекршаја*, Институт за криминолошка и социолошка истраживања, 2015, стр. 352.

[265] *Ibid*.

и мере заштите како би се обезбедила доступност правде и прилагођавање узрасту и степену развоја малолетника. У овим процесима учествују посебни органи, као што су јавни тужилац за малолетнике, органи старатељства, Центар за социјални рад, судије за малолетнике и савети за малолетнике.[266] Њихова улога је да штите интересе малолетника и да обезбеде да се поштују њихове потребе и права.

Када су малолетници укључени у кривични поступак, важно је водити рачуна о њиховом узрасту и психичком развоју. Због тога се поступци често одвијају без присуства јавности, хитно и у интересу заштите малолетника.

10.2. Облици сајбер криминала у којима учествују малолетна лица

Малолетници, све више постају или починиоци или жртве разних облика сајбер криминала. Ови случајеви укључују нелегално преузимање софтвера, музике и других фајлова, дистрибуцију вируса, неовлашћен приступ рачунарима и мрежама, као и дигиталну злоупотребу других малолетника. Такође, деца су све више изложена сајбер превари, злостављању и манипулацији путем интернета, као и конвенционалном криминалу који користи технологију и онлајн простор за праћење и контактирање потенцијалних жртава, са циљем вршења кривичних дела као што су трговина људима или сексуално злостављање. Овај алармантни тренд захтева хитне превентивне мере како би се деца и млади заштитили од сајбер криминала и обезбедило њихово безбедно коришћење интернета.

Конвенционални криминал све више користи сајбер простор као средство за вршење различитих кривичних дела, што показује све већу повезаност традиционалних облика криминала и дигиталне сфере. Сајбер простор пружа криминалцима могућност да припремају и извршавају кривична дела путем различитих информационих технологија, укључујући друштвене мреже као што су Фејсбук и друге платформе. Готово да не постоји конвенционални злочин који се не може делимично или потпуно припремити коришћењем информационе технологије.

Праћење и прикупљање информација о навикама потенцијалних жртава, које се касније могу користити у различите сврхе као што су убиство, трговина људима или људским органима, често се спроводи у сајбер простору. Чак се и кривична дела попут трговине дрогом или оружјем у одређеним сегментима припремају или спроводе коришћењем дигиталних технологија.

---

[266] *Ibid.*

Дигитално форензичко истраживање открива нови тренд везан за незаконите радње, а то је прикупљање информација са друштвених мрежа у циљу припреме будућих кривичних дела, као што је сајбер надзор. Овај вид праћења, за разлику од традиционалног физичког праћења, подразумева прикупљање корисничких података са друштвених мрежа попут слика, коментара, навика, који омогућавају праћење кретања одређене особе. Увођење услуга препознавања лица додатно олакшава процес прикупљања информација. У пракси постоје примери да су отмице вршене на основу анализе друштвених мрежа у циљу идентификације потенцијалних жртава. Случај планирања отмице М.П. путем Фејсбука јасно показује како друштвене мреже доприносе циљаној селекцији жртава.[267]

У савременом друштву све већи акценат се ставља на утицај слободног времена на криминално понашање малолетника. Међутим, често се занемарује важност анализе како ово слободно време може утицати на стварање и повећање броја малолетних жртава. Опште је познато да млади значајан део свог слободног времена проводе пред екранима компјутера, што може довести до изражених облика зависности.[268] Класификација зависности од интернета, обухвата пет основних подтипова понашања који су карактеристични за зависност од интернета. То укључује опсесивно тражење виртуелних пријатељстава, компулзивно посећивање сајберсекса и порнографских веб локација за одрасле, као и компулзивно коцкање и куповину на мрежи. Поред тога, претраживање и сурфовање интернетом и компулзивно играње видео игрица такође спадају у ову категорију зависности.[269]

Важно је напоменути да одређени обрасци понашања карактеристични за зависност од интернета могу додатно ослабити отпор малолетника на различита кривична дела, укључујући и она која се односе на безбедност рачунарских података. Стога разумевање и правилно управљање слободним временом младих постаје кључно за превенцију различитих облика криминала и заштиту младих од потенцијалних ризика које представља дигитално окружење.

У данашњем дигиталном добу, упознавање на мрежи може бити замка за многе, и одрасле и малолетне. Ова врста тзв. виртуелних пријатељстава носи са собом ризик од сусрета са злонамерним особама, често представљајући озбиљну претњу, посебно за одрасле. Ситуација постаје још

[267] *Ibid*, стр. 354.

[268] Стевановић З.: Интернет зависност - од игре до патологије, *Ревија за криминологију и кривично право*, 1/2013, 66-67.

[269] *Ibid*.

сложенија када су у питању малолетници, који могу бити посебно рањиви због својих карактеристичних особина које их чине лакшом метом за потенцијално злостављање. Када говоримо о виктимогеним предиспозицијама, које су специфичне особине или околности које одређену особу чине рањивијом на одређене облике криминалног понашања, јасно је да се ризици додатно повећавају. Аутор Миленковић истиче да ове предиспозиције могу појединца изложити већем ризику да постане жртва различитих облика криминала.[270]

Када дечаци и девојчице пролазе кроз пубертет, често се суочавају са изазовима везаним за њихов сексуални идентитет. У том процесу често посежу за онлајн садржајем који може задовољити њихове интензивне сексуалне импулсе. Међутим, ово понашање носи са собом ризике, посебно када су у питању веб странице за одрасле. Ова потрага за задовољством често је у сукобу са друштвеним ограничењима и забранама, што може додатно да закомпликује њихово емоционално и ментално благостање. Такође, поред емотивних изазова, млади људи који посећују ове сајтове често се излажу ризику од компјутерских вируса. Истраживања показују да су хакери развили злонамерне рекламе које се аутоматски покрећу приликом посете одређеним порно сајтовима, које могу да заразе рачунаре вирусом без потребе да корисник кликне.[271]

Уопштено говорећи, важно је разумети основне разлоге због којих неко постаје жртва, а то се најлакше може постићи анализом његових карактеристика. Слабост и различитост могу се идентификовати као кључне карактеристике жртава вршњачког насиља, а често се ради о њиховој комбинацији. Иако ова подела може бити прихватљива, због своје ширине постоји потреба за прецизнијим разграничењем поткатегорија.

Слабост може имати више различитих значења, па је оправдано разликовати поткатегорије као што су: 1) слабост у објективном смислу и 2) слабост у субјективном смислу. Објективно слабије жртве су обично физички инериорна деца која су слабије развијена од својих злостављача. То могу бити деца која су физички слабија, мање изражајна или касније улазе у пубертет, те она са тешкоћама у развоју. Ова деца често нису у стању да се одупру или бране, посебно у стварном свету, али могу реаговати на мрежи ако осећају да имају минималне шансе за одмазду. Жртве које су слабије у

---

[270] Миленковић, Ј.: Криминална виктимизација деце, *Зборник радова студената докторских студија права* (ур. В. Ђурђић, М. Лазић), Ниш, 2014, стр. 43.

[271] Спасојевић, Ђ., Миладиновић Боговац, Ж.: Малолетници као жртве кривичних дела учињених злоупотребом рачунарске мреже, *Научно-стручни часопис – Трендови у пословању*, 2018, VI(12), стр. 62.

субјективном смислу нису нужно физички инфериорне, већ се доживљавају као слабе због друштвених околности. То могу бити деца која су одбачена или неприхваћена у друштву својих вршњака, често стидљива или повучена. Они који су недавно променили школу или средину такође могу бити у овој позицији. Ова деца можда немају много пријатеља на друштвеним мрежама и често постају мете злонамерних вршњака који те мреже користе за штетне активности. Иако нису објективно слабе, ове жртве се могу представити као осветољубиви сајбер уходе или осветољубиви анђели, посебно склони удруживању са другом слично маргинализованом омладином. Понекад се осећај моћи може јавити као реакција на даље претње.[272]

10.3. Манипулисање у сајбер простору и сексуално искоришћавање малолетника путем Интернета

Сајбер манипулација је суптилан, али опасан облик психолошке манипулације која се одвија на Интернету кроз различите комуникационе платформе. Ове манипулације се најчешће врше преко јавних причаоница, сајтова за упознавање, тренутних порука и VOIP сервиса као што су ICQ и Skype, а однедавно друштвене мреже као што су Facebook, Instagram, Pinterest, Tumblr, Twitter и LinkedIn постају све чешће платформе за такве активности. Жртве ових манипулација најчешће су деца и малолетници узраста од 11 до 17 година. Крајњи циљ ових манипулатора је обично да дођу до физичког сусрета са својим жртвама, што често резултира сексуалним злостављањем, насиљем, укључујући дечју проституцију и порнографију.[273] Едукација о томе како препознати и реаговати на сајбер манипулацију, као и промовисање безбедних интернет пракси, кључни су кораци у борби против ове озбиљне претње.

У дигиталном добу, отварање профила на друштвеним мрежама попут Facebook-а постала је прва активност многих малолетника након добијања приступа интернету. Ова интеракција им омогућава да се повежу са својим вршњацима, играју игрице, учествују у интересним групама и деле садржај. Међутим, са виртуелним пријатељствима долази и одређени ризик. Није увек лако разликовати праве пријатеље од оних који користе лажне идентитете. Лажно представљање на интернету може имати озбиљне последице, посебно када су у питању малолетници. Пуштањем туђих слика и лажних информација одрасли се могу претварати да су малолетници како

[272] *Ibid*, стр. 63.

[273] Kopecký, K: Cyber grooming danger of cyberspace (study), In: *Dangerous communication phenomena for teachers with a focus on cyberbullying, cyberstalking, cybergrooming and other socio-pathological phenomena,* 2010, 1-18.

би задобили поверење деце. То може довести до опасних ситуација, укључујући контакте са намером да се почине кривична дела.[274]

У Србији су већ забележени случајеви оваквих кривичних дела. Најчешће жртве лажног представљања на интернету су деца, а посебно је алармантно када је у питању педофилија. Педофили користе интернет као средство за контакт са децом, представљајући се као њихови вршњаци и манипулишући њиховим поверењем. Покушавају да добију личне податке о деци, нудећи новац или друге услуге као искушење. Такође, често шаљу порнографски материјал или траже од деце да им пошаљу такав садржај, што може довести до уцена и злостављања.[275]

У таквим околностима, кључно је едуковати децу о безбедности на Интернету и подићи свест родитеља о потенцијалним опасностима. Такође, спровођење строжих мера контроле и надзора на интернету, као и сарадња са надлежним органима, неопходни су кораци у борби против оваквих злоупотреба.

10.3.1. Порнографија, технологија и њихове жртве

10.3.1.1. Порнографија од настајања до данас

Сам термин, порнографија, потиче од грчкох речи πόρνη • (pórnē) f (genitive πόρνης); – блудница и γράφειν • (gráphein) f (genitive γρᾰφω) - писати. Милан Вујаклија у свом „Лексикону страних речи и израза" порнографију преводи као „бестидна књижевност у уметност, а порнографски предмет би био онај који је бестидно насликан или написан, скаредан."[276] Сличан превод налазимо и код Братољуба Клаића „бестидна, штетна, развратна литература, непристојни блудни цртеж, слика"[277]. Данас је порнографија скоро потпуно у свом изразу попримила и обавезност присутности интернета, с обзиром на то да без интернета она има неки потпуно другачији ток бивања у оптицају. У ери технологије, порнографија од настајања до криминалистичке истраге којом се склања са „тржишта" бива на интернету. Због тога ове дефиниције нису адекватан опис садашњег стања, већ је једна од главних асоцијација на порнографију и екран одређеног уређаја на којем се она приказује или сајт на интернету са којег се преузима.

Са развојем интернета повећава се количина и доступност информација, док анонимност мрежепружа корисницима слободу да без бојазни

[274] Прља, Д., Кораћ, В: нав. дело, 2015, стр. 356.

[275] *Ibid*.

[276] Вујаклија М., Лексикон страних речи и израза, Просвета-Београд, 1980, стр. 790.

[277] Клаић Б, Велики рјечник страних ријечи, Зора Загреб, 1974., стр. 1403.

приступају и садржајима који су друштвено табуисани. Према статистикама из 2009. године, 12%4 свих веб сајтова је порнографског садржаја. Претрага порнографије на дневном нивоу чини 25% свих претрага, што порнографске садржаје чини појединачно најбројнијим на интернету.[278]

Дубока мрежа, најновији термин који наводи на мистификацију, у ствари је део интернета, који из разлога што није индексиран, није претражив, па тај део мреже класични претраживачи интернет страница не виде. Интернет индексирање укључује креирање специфичног списка речи који је везан за одређену интернет страну и који му се придружује, као кратак садржај странице који корисници не виде. Могућност прављења страница без икакве контроле је довела до појаве великог броја неиндексираних страна, па је дубока мрежа неколико пута већа од претраживог дела интернета, губитак података је јако велики, а информативни пропуст непроцењив због чега научни тимови раде на проналажењу нове врсте претраживача који би укључио и неиндексиране странице. Са тачке гледишта порнографије је битно да напоменемо да се сматра да је већина садржаја попут педофилије и истинских „снаф" филмова заправо негде у дубокој мрежи.[279]

Понашање корисника интернета је другачије док су на интернету, него у реалним животним ситуацијама. Мање се придржавају друштвених норми, чак и када не користе неки псеудоним, већ свој идентитет именом и презименом. Такво понашање је најсличније ефекту масе, када ће људи узвикивати ствари које иначе не би изговарали, због чега се читањем коментара испод неке вести или појаве може стећи лажни утисак о јавном мњењу, по коме има много више људи који се противе нечему. Људи који немају негативан став, често неће ништа написати, за разлику од много гласнијих неистомишљеника, што ће се и одразити на гласања „за и против", као и на учесталост негативних коментара.[280] Исто је и са негативним друштвеним појавама које зачињу или се настављају са реалног света на виртуелни. У наизглед непостојећем окружењу, особа испред себе види само екран одређеног уређаја и нема развијену свест о томе да се и у овом виртуелном окружењу одвијају исти процеси као и у

[278] Статистички подаци су преузети са странице http://internetfilter- review.toptenreviews.com/internet-pornography-statistics. html из рецензије у којој су наведени резултати акредитованих агенција и медијских кућа: ABC, Associated Press, AsiaMedia, AVN, BBC, CATW, U.S. Census, Central Intelligence Agency, China Daily,итд. (приступљено 17.09.2019.)

[279] Вучуровић М., Порнографија- од пећине до сајбер простора, Либерто Београд 2014. стр. 112.

[280] *Ibid*, стр. 176.

реалном; да и ту постоје кривична дела, жртве и учиниоци. Последице настале због речи или дела путем интернета и технологије врло су реалне, видљиве и опипљиве, те управо због тога високотехнолошки криминал[281] као термин ступа на сцену и са собом носи низ законодавних, системских али и социолошких промена у животима људи. Оснивају се нове институије, проширују постојеће, стварају нови закони и потежу нове друштвене теме како би сви били безбедни како у реалном свету тако и на интернету. Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала уређује се образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела одређена овим законом.

Високотехнолошки криминал представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику. У складу са овом законском дефиницијом у област високотехнолошког криминала спадају и кривична дела где се рачунари и рачунарске мреже јављају као средство извршења кривичних дела преваре, код злоупотреба платних картица на интернету, злоупотреба у области електронске трговине и банкарства, злоупотребе деце у порнографске сврхе на интернету (тзв. дечија порнографија), говора мржње на интернету (ширење националне, расне, верске мржње и нетрпељивости и сл).

10.3.2. Сексуално злостављање деце и малолетника. Исправна терминологија

Пре него што почнемо са анализом ове теме, потребно је посветити пажњу терминологији која је од стране светских стручних организација препозната као штетна, али се у народу, а нажалаост и у законодавству, усадила као кованица. Стручњаци су препознали штетност терминологије, која сексуално злостављање деце изједначује са порнографијом, те су створили „Луксембуршке смернице" из 2016. године.[282] У њима налазимо објашњење да је порнографија термин који се користи за одрасле особе које се баве споразумним сексуалним радњама које су (углавном) легално

[281] Високотехнолошки криминал (сајбер криминал) је појам који је настао почетком 70-их година, у периоду када су се почеле користити рачунарске мреже и системи.

[282] Doek J., Greijer S., Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Luxembourg, 2016, доступно на https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology

дистрибуиране широј јавности ради њиховог сексуалног задовољства[283]. Критика овог термина у односу на децу потиче из чињенице да се „порнографија" све више нормализује и може (нехотице или не) допринети смањењу тежине, тривијализацији или чак легитимизацији онога што је заправо сексуално злостављање и / или сексуално искоришћавање деце. .Даље, као и у горе описаним терминима, „дечија проституција" и „дечија проститутка", термин „дечија порнографија" ризикује да инсинуира да су дела извршена уз сагласност детета и да представљају легитимни сексуални материјал.[284] Дакле, исправан термин би гласио „сексуално злостављање деце" и „предмети порнографске садржине настали искоришћавањем малолетног лица", а не „дечја порнографија".

Такозвана „дечја порнографија" укључује децу која не могу (законски) пристати на сексуалне радње којима су изложена, и која могу бити жртве кривичног дела. Ово је општи приступ сектора за спровођење закона последњих година, и то је водећи пут у окарактерисању „дечије порнографије" као форензичких доказа сексуалног злостављања или искоришћавања деце. Организације за спровођење закона у многим земљама, као и Европол и Интерпол на међународном нивоу, имају тенденцију да одбаце термин „дечја порнографија" и користе било „материјал за сексуално злостављање деце" или „материјал за сексуалну експлоатацију деце".[285]

„Луксембуршке смернице" упућују и на специфичне случајеве у којима се фотографије или видео садржај стварају путем рачунара, али на њима су приказана деца која су сексуално злостављана. Наиме, израз „компјутерски (или дигитално) генерисан материјал за сексуално злостављање деце" обухвата све облике материјала који приказују децу која су укључена у сексуалне активности и / или на сексуални начин. Оно што је специфично је да производња материјала не укључује стварну злоупотребу и стваран контакт са децом, али је вештачки створен тако да изгледа као да су приказана права деца. То укључује оно што се понекад назива „виртуалном дечијом порнографијом" као и „псеудо фотографије". Иако је већина вештачки створеног материјала за сексуално злостављање деце генерисана рачунаром, важно је не искључити могућност да такав материјал, на пример, може да се црта руком. Компјутерски произведен материјал за сексуално злостављање деце није свугде илегалан, мада може штетно утицати на децу. У судској пракси и случајевима из наше државе који су анализирани у овом раду, није било

[283] *Ibid*, стр. 38.

[284] Doek J., Greijer S., Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Luxembourg, 2016,стр. 39.

[285] *Ibid*, стр. 40.

оваквих примера, али с обзиром на развој технологије и све блаже границе између виртуалног и реалног света, требало би пратити овај „тренд" и, ако је потребно, сместити га у одређени законски оквир.

10.3.3. (Непримењена) терминологија у држави и свету

Конвенција Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања није применила препоруке о исправној терминологији у области сексуалног злостављања деце, што сматрамо крајње чудним, с обзиром на улогу и важност ове европске организације. Наведена конвенција и даље користи термин „дечја порнографија" и одређује је као: „сваки материјал који визуелно приказује дете које се стварно или симулирано експлицитно сексуално понаша или сваки приказ дететових полних органа за првенствено сексуалне сврхе" (члан 20. став 2.)[286]. Овом конвенцијом се за државе уговорнице предвиђа обавеза да санкционишу: производњу дечје порнографије; нуђење или стављање на располагање дечје порнографије; дистрибуцију или пренос дечје порнографије; набављање дечје порнографије за себе или другу особу; поседовање дечје порнографије; свесно прибављање и приступ преко информационо-комуникационих технологија дечјој порнографији. Такође, Конвенција о високотехнолошком криминалу користи термин „дечја порнографија, где се наводи да, између осталих критеријума, дечја порнографија укључује лице које изгледа као малолетник (члан 9. став 2. тачка б.), а које учествује у експлицитно сексуалној радњи.[287] Сходно датом члану, нужно се поставља питање на основу којих параметара се објективно може тумачити да нека особа „изгледа" као да је малолетна. Такође би било логично да у случају порнографске представе на којој је приказана особа која има 19 година, а која „личи" као да је малолетна, и поред њене добровољности, постоји довољан основ за кривично гоњење. Иако логично, било би пожељно оставити што мање простора који је подложан различитим тумачењима, због осетљивости теме и категорије која се овим дефиницијама штити.

Ни домаће законодавство није применило препоруке о промени терминологије у циљу заштите деце и малоелтника, те се под предметима порнографске садржине настале искоришћавањем малолетног лица (што

[286] Конвенција Савета Европе о заштити деце од сексуалног узнемиравања и сексуалног злостављања-незванични превод, (http://arhiva.mup.gov. rs/) приступљено 17.09.2019.године.,стр. 8.

[287] Закон о потврђивању конвенције о високотехнолошком криминалу, *Службени гласник РС,* бр. 19, 2009.

законодавац назива дечјом порнографијом) на основу изричите законске одредбе (члан 185. став 6. КЗ-а) сматра сваки материјал који визуелно приказује малолетно лице које се бави стварним или симулираним сексуално експлицитним понашањем, као и свако приказивање полних органа детета у сексуалне сврхе. [288] Анализирајући Кривични законик РС, посебно чл. 112, где је објашњено значење израза овог законика, може се видети да законодавац нигде изричито не наводи шта појам порнографије заправо подразумева. Овакав пропуст умањује јасноћу кривичноправних одредби које се доводе у везу са овим појмом, па је дефинисање појма порнографије са кривичноправног аспекта изузетно значајно. Кривичноправно одређење порнографије нужно се мора ослањати на друштвене изворе овог појма.[289]

10.3.4. Кривичноправни оквир у Србији за борбу против дечије порнографије

10.3.4.1. Кривични законик

Кривична дела која се тичу високотехнолошког криминалитета у Републици Србији, први пут су законским изменама и допунама инкриминисана у Кривични законик РС 2003. године. Ово је било очекивано и неопходно, с обзиром на то да технолошки напредак није заобишао Србију, те је морао да постоји одређени правни оквир који би уредио свако могуће незаконито понашање на интернету и путем технологије генерално. Уз мање измене, Кривични законик Србије из 2005. године је преузео постојећа кривична дела, чиме се Србија мало касније придружила оним земљама које су законским путем уредиле кажњавање различитих видова злоупотребе рачунара и рачунарске технике.

У оквиру дефинисаних појавних облика високотехнолошког криминала, кривична дела спадају у групу коју чине дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминалитета. Такође, усвајањем Закона о изменама и допунама Кривичног законика 2009. године, извршене су измене законског описа кривичног дела приказивање порнографског материјала и искоришћавање деце за порнографију (члан 185. КЗ), и уведена два нова кривична дела: навођење малолетног лица на присуствовање полним радњама (члан 185а КЗ) и искоришћавање рачунарске мреже или комуникације другим

[288] Кривични законик, *Службени гласник РС*, 2016.

[289] Милан Манчевић, Дечја порнографија као облик високотехнолошког криминала – мастер рад, Правни факултет Универзитета у Нишу, 2017., стр.12.

техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185б КЗ).

Коначно, у актуелном Кривичном законику то изгледа овако:

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

(Члан 185)

(1) Ко малолетнику прода, прикаже или јавним излагањем или на други начин учини доступним текстове, слике, аудио-визуелне или друге предмете порнографске садржине или му прикаже порнографску представу, казниће се новчаном казном или затвором до шест месеци.
(2) Ко искористи малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу, казниће се затвором од шест месеци до пет година.
(3) Ако је дело из ст. 1. и 2. овог члана извршено према детету, учинилац ће се казнити за дело из става 1. затвором од шест месеци до три године, а за дело из става 2. затвором од једне до осам година.
(4) Ко прибавља за себе или другог, поседује, продаје, приказује, јавно излаже или електронски или на други начин чини доступним слике, аудио-визуелне или друге предмете порнографске садржине настале искоришћавањем малолетног лица, казниће се затвором од три месеца до три године.
(5) Ко помоћу средстава информационих технологија свесно приступи сликама, аудио-визуелним или другим предметима порнографске садржине насталим искоришћавањем малолетног лица, казниће се новчаном казном или затвором до шест месеци.
(6) Предметима порнографске садржине насталим искоришћавањем малолетног лица (дечија порнографија) сматра се сваки материјал који визуелно приказује малолетно лице које се бави стварним или симулираним сексуално експлицитним понашањем, као и свако приказивање полних органа детета у сексуалне сврхе.
(7) Предмети из ст. 1. до 4. овог члана одузеће се.

У складу са наведеним, основни и тежи облик могу се извршити према малолетнику, а додат је и нови тежи облик, који постоји ако се неки од прва два облика изврши према детету. Кривично дело, према последњим изменама и допунама, у основи има четири облика. Први облик дела постоји у ситуацији када се малолетнику прода, прикаже или јавним излагањем, или на други

начин учине доступним текстови, слике, аудио-визуелни или други предмети порнографске садржине или му се прикаже порнографска представа. За наведени облик кривичног дела предвиђена је новчана казна или казна затвора до шест месеци (чл. 185. ст. 1 КЗ). Дакле, у првом случају малолетнику се чини доступним порнографија, док се други случај односи на искоришћавање малолетника за производњу предмета или представа порнографске садржине. Други облик дела постоји у ситуацији искоришћавања малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу. Лице које направи фотографски, филмски или други снимак малолетника ради израде порнографског садржаја или га наведе да учествује у порнографској представи учиниће кривично дело искоришћавање малолетника за порнографију. За други облик дела предвиђено је кажњавање од шест месеци до пет година затвора (чл. 185. ст. 2 КЗ).

Трећи облик, представља квалификовани облик првог и другог дела и постоји уколико је неко од тих дела извршено према детету. За дело из првог облика према детету предвиђена је казна затвора од 6 месеци до 3 године, док је за друго дело према детету, предвиђена казна затвора од 1 до 8 година (чл. 185. ст. 3 КЗ). Четврти облик, представља посебни облик дела који постоји када лице прибавља за себе или другог, поседује, прода, прикаже, јавно изложи или електронски и на други начин учини доступним слике, аудио-визуелне и друге предмете порнографске садржине настале искоришћавањем малолетног лица. Прописана казна за четврти облик кривичног дела је казна затвора од три месеца до три године (чл. 185. ст. 4 КЗ). Дакле реч је о ширењу и стављању у промет дечје порнографије. Пети став предвиђа да ће се одузети предмети који су настали извршењем наведена три облика дела (чл. 185. ст. 5 КЗ).[290]

10.3.4.2. Остали правни акти

Осим кривичног законика, постоје и други правни акти који чине правни оквир за борбу против искоришћавања деце и малолетних лица у порнографске сврхе. Неки од њих су: Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, Законик о кривичном поступку, Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Уредба о безбедности и заштити деце при коришћењу информационо –комуникационих технологија. Када говоримо о свим овим законима, битно је да пре свега нагласимо важност проширења појма „дечја“ и на „малолетници“

[290] Кривични законик, *Службени гласник РС*, бр. 85/2005, 88/2005 -испр., 107/ 2005 -испр., 72/ 2009, 111/ 2009, 121/2012, 104/2013 и 108/2014.

због тога што је нужно заштитити све жртве ових кривичних дела које су малолетне, а не само оне које по закону спадају у старосну групу деце. Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица у члану 3 наводи Узраст учиниоца као јасно дефинисану категорију, са поделом на млађе и старије малолетнике, млађа пунолетна лица, али и разграничење у односу на децу у члану 2.[291] Дакле, потребно је усагласити остале акте са постојећим правним одредницама како би се што јасније дефинисале ове осетљиве старосне групе и њихова заштита.

У Закону о посебним мерама за спречавање вршења кривичних дела против полне слободе малолетних лица, уводна одредба каже да се овим законом прописују посебне мере које се спроводе према учиниоцима кривичних дела против полне слободе извршених према малолетним лицима одређених овим законом и уређује вођење посебне евиденције лица осуђених за та кривична дела.[292]

Наведени закон се примењује на учиниоце који су извршили следећа кривична дела:

1) силовање (члан 178. ст. 3. и 4. Кривичног законика);
2) обљуба над немоћним лицем (члан 179. ст. 2. и 3. Кривичног законика);
3) обљуба са дететом (члан 180. Кривичног законика);
4) обљуба злоупотребом положаја (члан 181. Кривичног законика);
5) недозвољене полне радње (члан 182. Кривичног законика);
6) подвођење и омогућавање вршења полног односа (члан 183. Кривичног законика);
7) посредовање у вршењу проституције (члан 184. став 2. Кривичног законика);
8) приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185. Кривичног законика);
9) навођење малолетног лица на присуствовање полним радњама (члан 185а Кривичног законика);
10) искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185б Кривичног законика).[293]

[291] Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица, *Службени гласник РС*, бр. 85/2005.

[292] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе малолетних лица, *Службени гласник РС*, бр. 32/2013.

[293] Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе малолетних лица, *Службени гласник РС*, бр. 32/2013.

Оно што је посебно занимљиво у овом Закону, је што су њиме прописане посебне мере које се према учиниоцима примењују након издржане казне затвора, као и одређене правне последице осуде. Сматрамо ово одличним начином превенције и контроле учинилаца, с обзиром на висок степен рецидивизма код истих. Међутим остаје нејасно да ли се ове посебне мере примењују само ако је пресудом изречена санкција казне затвора како је наведено, што се заправо односи на мали број пресуда, узимајући у обзир то да већина пресуда овим учиниоцима буде условна осуда или новчана казна. Врста санкције и висина одређене казне је увек појам који се у друштву субјективно доживљава. Чињеница је да овде репресија има и једну врсту превентивне улоге и да би изрицање максималних прописаних казни створило одређену климу у друштву, у којој је свима јасно да држава има нулту толеранцију када су искоришћавање деце и малолетних лица у порнографске сврхе и други облици сексуалног злостављања деце и малолетника у питању.

Посебне мере и додатна решења која нуде други закони морају се максимално искористити, све гране друштва се морају адекватно укључити у циљу заштите деце и малолетника. Управо се у дискусијама на ове теме уочава огроман недостатак квалитетних база података и генерално истраживања подржаних од стране државе. Дела која су већ учињена морају послужити као извор информација, знања и алата за борбу против будућих, како би се законске норме прилагођавале и побољшавале, а рад полиције, тужилаштава и судова унапређивао и трансформисао у складу са актуелним технолошким трендовима.

10.3.5. Улоīа технолоīије у начину извршења кривичноī дела

Кривично дело Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију може се извршити на различите начине. Са постављањем фокуса на начине извршења коришћењем интернета и других технологија нисмо превише сузили тај опус. Извршиоци овог дела су пронашли начин да злоупотребе технологију у сврху прибављања недозвољеног порнографског материјала и сваки извршилац је створио свој лични модус операнди у зависности од нивоа познавања рада на рачунару или телефону, претходних туђих искустава и других околности које утичу на то за шта ће се од технологије и софтвера учинилац определити. Наравно, сви програми, апликације, као и сами уређаји који се користе нису створени са наменом да буду средство путем којег ће се обављати забрањена радња, али људи су пронашли начин

да их злоупотребе. У овом делу ћемо покушати да објаснимо начин на који технологија најчешће бива злоупотребљена у сврху извршења кривичног дела из чл.185 КЗ-а.

10.3.6. П2П модел комуникације

Када поменемо дистрибуцију података, ту се обично мисли на активно преношење дечије порнографије од особе до особе, „на руке". Међутим, када говоримо о П2П дистрибуцији, она јесте условно речено пасивнија, али је свакако начин, те се као такав све чешће појављује као предмет истрага Учиниоци се најчешће служе погодностима које пружа П2П односно пеер то пеер модел комуникације путем интернета, којим се врши размена података. П2П је скраћеница од енглеског термина „*peer to peer*", где би буквалан превод гласио „вршњак вршњаку" односно једнак једнаком. Суштина се крије управо у том преводу, где се путем П2П мреже размена података врши директно између корисника, на тај начин што особа која има одређене фајлове у рачунуару, може да употреби софтвере који користе ову технологију како би их поделио директно другој особи, без потребе да прво постави податке на одређену платформу да би их друга особа преузела.

П2П мрежа омогућава да се одређене датотеке деле на више рачунара. Ако се ове мреже оставе „отворене", појединцима је дозвољено да анонимно деле датотеке. Већина П2П мрежа долази са подразумеваним подешавањима која омогућавају дељење корисничких датотека. Неко ко је у поседу порнографског материјала у којем су злоупотребљена деца и малолетници и ко похрањује своје податке на П2П мрежи потенцијално је одобрио приступ осталим рачунарима на мрежи. Ово представља дистрибуцију и доставу датотека.

Када је пре 12 година изашао први извештај Компаније за интернет широкопојасну мрежу „Сандвине" о глобалним Интернет феноменима, речено је да П2П мреже представљају готово 60% целокупног интернет промета. У то време П2П мреже нису се првенствено користиле за дељење „дечје порнографије" (или одрасле порнографије), већ се највећи део П2П саобраћаја састојао од музике, филмова, ТВ емисија и другог не-порнографског садржаја. Данас „Сандвине" извештава да П2П мреже и даље заузимају 10% целокупног интернет промета. Док су се људи окренули Нетфликсу, Јутјубу и сл. (који заједно чине отприлике 50% целокупног интернет промета) за гледање ТВ емисија и филмова, П2П мреже остају примарни канал за појединце који желе гледати и дистрибуирати „дечју порнографију".[294]

[294] П2П мрежа (https://sr.wikipedia.org/sr-ec/P2P) приступљено 19.09.2019.год.

Због чега је П2П мрежа погодна? Да би приступили П2П мрежи, корисници једноставно преузимају и инсталирају погодну апликацију за П2П корисника. Апликација П2П корисника повезује с његовом специфичном П2П мрежом и на тај начин повезује кориснике једне са другима. Једном када се корисници повежу, могу да отпремају или преузимају датотеке једни од других без откривања ичега од личних података. Веб сервери П2П који преносе те датотеке су довољно велики да складиште милионе датотека и називају се „дивљим западом интернета". Извршиоци су подстакнути огромном количином активности у овим мрежама и чињеницом да примена закона једноставно не може да обухвати милионе људи који учествују у овој трговини. Психологија масе има великог удела у мотивацији корисника да изабере баш овај начин преузимања и дељења података.

10.3.7. Софтвер и хардвер

Навешћемо само пар најпопуларнијих софтвера за коришћење П2П мреже.

- "**eMule**" је бесплатна апликација за дељење датотека за Microsoft Windows. Покренут у мају 2002. године као алтернатива „eDonkei2000", па се „еМуле" сада повезује и на " eDonkei " мрежу и на мрежу „Кад". Препознатљиве карактеристике „еМуле-а" су да га често користе клијенти који траже изузетно ретке садржаје, директна размена датотеа између клијента, брз опоравак оштећених фајлова и употреба кредитног система за награђивање учесталих корисника. [295]
- **"LimeWire**" је П2П програм за размену података, који омогућава корисницима да поделе с другима своје фајлове или да пронађу жељене фајлове, укључујући песме, филмове, слике, игрице, текстуалне фајлове и програме. Од осталих опција издваја се могућност прегледања фајла током његовог скидања. LimeWire је програм отвореног кода који користи „Gnutella" мрежу за размену фајлова и без проблема функционише чак и ако се налазите иза firewalla, а доступан је у верзијама за Windows, Mac и Linux.[296]
- **"Ares galaxy"** је п2п апликација за дељење датотека која користи сопствену децентрализовану мрежу супернода. Била је издвојена из „Gnutella" мреже 2002. године и хостована је на SourceForge.net. Ares galaxy има једноставан интерфејс за брз приступ са уграђеним аудио / видео прегледачем.[297]

[295] eMule (https://en.wikipedia.org/wiki/EMule) приступљено 19.09.2019.год.

[296] LimeWire (https://en.wikipedia.org/wiki/LimeWire) приступљено 19.09.2019.год.

[297] Ares Galaxy (https://en.wikipedia.org/wiki/Ares_Galaxy) приступљено 19.09.2019.год.

- **"Torrent":** је датотека која делује као кључ за покретање преузимања стварног садржаја. Када је неко заинтересован да прими заједничку датотеку (filmove, fotografije, документе итд.), прво мора да добије одговарајућу торрент датотеку - било преузимањем .торрент датотеке директно или коришћењем везе „магнетом". Тада је потребан БитТоррент софтвер за отварање ове датотеке / везе. Једном када БитТоррент софтвер скенира торрент датотеку / везу, тада ће морати да нађе локације „сејача" који деле одговарајућу датотеку, тј. који је поседују у рачунару и пристају да је деле. Да би то учинио, покушаће да се повеже на листу дефинисаних пратилаца (из метаподатака торрент датотеке) и покушаће директно повезивање. Ако буде успешан, одговарајући садржај ће почети да се преноси.[298]

Што се тиче улоге хардвера у извршењу овог и сличних кривичних дела, међу одузетим предметима у истрази најчешће се налазе рачунари, мобилни телефони, хард дискови, меморијске картице, УСБ меморије, ЦД и ДВД дискови (данас ређе). Стручњаци се слажу да је битно познавање основних појмова хардвера и софтвера као и функционисања интернета и мрежа од стране правосудних органа, како би се рационално и компетентно одлучивало у сваком сегменту поступка. Наведени уређаји служе за складиштење фотографија, видео снимака и осталог недозвољеног садржаја, од стране учиниоца.

10.3.8. Друштвене мреже

Последњих година интернет друштвене мреже као што су Фејсбук, Твитер, Инстаграм, постају глобални масовни феномен. Фејсбук, због своје природе наметнуте корисницима од почетка свог постојања, јесте платформа која најчешће садржи највећи број личних података о кориснику на његовом профилу, почев од фотографија, локације, запослења, статуса везе па некада и до броја телефона. Сви ови подаци нису увек истинити и када гледате профил другог корисника можете се само поуздати у срећу и веровати му на реч да су сви подаци које о себи приказује, тачни.

Једно од главних питања која се тичу прикупљања података на мрежи су проблем лажних корисничких података или чак у потпуности лажних профила. Разлози за пружање лажних корисничких података могу бити резултат стратегије побољшања приватности због конфликтне конфигурације приватности и политике заштите података које проузрокује платформа, тако да циљ не мора увек бити малициозан. Међутим, док многи

[298] Торент фајл (https://en.wikipedia.org/wiki/Torrent_file) приступљено 19.09.2019.год.

корисници Фејсбука делимично дају лажне податке у својим профилима, неки профили чак представљају особу која не постоји у стварном животу. Такви профили се широко користе за злонамерне нападе на приватност корисника.[299] Фејсбук је примио критике на свој рачун у вези ове теме и покушао да сачини „имуни систем" који би препознавао лажне профиле и брисао их. Међутим, резултати истраживања из 2012. године показали су да је стварање и одржавање лажних профила лак задатак и да Фејсбуков имуни систем није успео да препозна лажне профиле који су направљени у току истраживања, како би тестирали успешност овог начина одбране.[300]

Већина лажних профила се користи туђим фотографијама одређене особе коју познаје или прати на некој од друштвених мрежа, или фотографија преузетим са интернета на којима може бити нека славна и позната личност или нека потпуно непозната особа из друге државе. Профил може имати само лажне фотографије, а праве личне податке или и они могу бити потпуно лажни. Када говоримо о лажним профилима сачињеним од стране пунолетних особа које желе да ступе у контакт са малолетницима, говоримо о фотографијама на којима је млађе лице, подацима који говоре да особа има мање година него у стварности, да похађа неку основну или средњу школу итд. На таквим профилима је најчешће све од података лажно, те особа на тај начин ступа у комуникацију са малолетном особом којој никада не открије идентитет, или га касније кроз разговор открије. У данашње време, интернет корисници су много освешћенији о томе како препознати лажан Фејсбук профил, како да пријавити и избећи потенијалну опасност, међутим деца и малолетници који тек почињу да користе интернет, у жељи да поседују што већи број пратилаца на друштвеним мрежама, а са мањком знања и искуства, и даље представљају лаку мету за оне који се крију иза лажних профила. Због тога је освешћеност и едукација о овим темама кључна, када је заштита деце и малолетника у питању, јер се све своди на лични суд и процену. То ће и данас бити пресудно када дођемо у ситуацију да треба проценити да ли је особа са друге стране екрана заиста онаква каквом се представља, с обзиром на то да још увек не постоји ефективан софтвер и апликација која ће ту процену обављати уместо нас. Кривична дела која се врше на овим платформама су бројна и то је коначно препознато од стране законодавца, те по први пут у Кривичном законику имамо дела као што су Прогањање и Полно узнемиравање.

[299] Katharina K., Dieter M., Edgar W., Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model, The Society of Service Science and Springer 2012, 170-172.

[300] *Ibid.*

Иако нису нужно везани за сајбер простор, услед напретка технологије и све већег коришћења виртуалних начина комуникације, начин извршења им је у великом броју случајева везан управо за употребу интернета и технологије. Ово је нарочито везано управо за наведена два кривична дела, јер извршилац више не мора физички да прати особу и константно се против њене воље налази у њеној близини како би добили квалификацију овог дела, већ је довољно да пошаље велики[301] број порука или позива на телефон особе, или неку њену друштвену мрежу и да јавни тужилац има основа да квалификује управо Прогањање. Ако су ови позиви или поруке са непримереном сексуалном конотацијом која жртву узнемирава, постојаће елементи кривичног дела Полно узнемиравање. У активној онлајн комуникацији, која различитим помагалима доприноси њеној живости, долази до уплетања више кривичних дела и тешко је раздвојити њихове радње. Због тога ћемо касније у наставку обратити посебну пажњу на наведена кривична дела, као и на кривично дело Принуда, које се такође често јавља заједно са кривичним делом из чл. 185 КЗ-а.

Инстаграм је достигао вртоглаву популарност због изостанка текста на овој друштвеној мрежи. Управо због овога је најпопуларнији међу најмлађом популацијом, којима фотографије и видео снимци окупирају пажњу, без потребе за писаним изражавањем и читањем. Инстаграм такође не поседује неки посебан вид заштите, већ садржи класичну и устаљену опцију пријављивања лажних профила. Због свега овога је постао јако погодан као средство комуникације, проналажења малолетних особа којима је лако представити се као неко други, са лажним фотографијама и без осталих личних података које Инстаграм при креирању профила и не захтева. Тиме је онима који креирају лажне профиле посао олакшан, те не морају долазити у ситуацију да њихови лажни лични подаци буду очигледно лажни, већ је довољно да у своје име поставе туђе фотографије.

Остале друштвене мреже и апликације, поготово оне које су наменски настале за упознавање, такозване „дејтинг“ апликације, углавном имају забрану коришћења особама млађим од 18 година, али малолетно лице лако може дати лажне податке и на тај начин се нађе изложено и на мети оних који управо малолетна лица и траже.

Која год друштвена мрежа или апликација била у питању, контрола од стране родитеља и одраслих особа генерално је неизбежна. Такође, едукација на ове теме мора постати нешто што је свакодневица, јер су управо

[301] Довољан број порука/позива упућених жртви од стране извршиоца је остављен на слободну процену Јавног тужиоца.

друштвене мреже постале део свакодневне рутине и деце и одраслих. Деца морају бити свесна свега што се може десити када ступе на интернет платформу, да су самим придруживањем друштвеној мрежи постали потенцијалне жртве, али такође фокус треба бити на томе како паметно користити све предности интернета, које неминовно постоје.

10.3.9. Трка нових технологија и законодавца

Најновијим изменама и допунама Кривичног законика које су објављене у Службеном гласнику РС, бр.94/2016, а примењују се од 01. јуна 2017.године, дефинисана су нова кривична дела Прогањање (чл.138а КЗ) и Полно узнемиравање (чл. 182а КЗ). Потреба за овим кривичним делима је постојала и у време када технологије нису у оволикој мери окупирале свакодневицу и комуникацију, али свакако да су са доласком таквог времена и радње ових кривичних дела нашле своје плодно тло на интернету. С обзиром на то да су кривична дела нова, са мало судске праксе и теоријске подршке, битно је што боље упознати се са њима, препознати радњу извршења и све начине на које се може остварити.

Прогањање

(Члан 138а)

(1) Ко у току одређеног временског периода:
   1) друго лице неовлашћено прати или предузима друге радње у циљу физичког приближавања том лицу противно његовој вољи;
   2) противно вољи другог лица настоји да са њим успостави контакт непосредно, преко трећег лица или путем средстава комуникације;
   3) злоупотребљава податке о личности другог лица или њему блиског лица ради нуђења робе или услуга;
   4) прети нападом на живот, тело или слободу другог лица или њему блиског лица;
   5) предузима друге сличне радње на начин који може осетно да угрози лични живот лица према коме се радње предузимају, казниће се новчаном казном или затвором до три године.

(2) Ако је делом из става 1. овог члана изазвана опасност по живот, здравље или тело лица према коме је дело извршено или њему блиског лица, учинилац ће се казнити затвором од три месеца до пет година.

(3) Ако је услед дела из става 1. овог члана наступила смрт другог лица или њему блиског лица, учинилац ће се казнити затвором од једне до десет година.

За кривично дело Прогањање законодавац таксативно наводи више могућих радњи извршења овог кривичног дела, при чему као радње наводи и све друге сличне радње на начин који може осетно да угрози лични живот лица према коме се радње предузимају.[302] Средства комуникације шире свој опус и свакога дана имамо неку нову апликацију, платорму и сл. те то мора бити узето у обзир приликом одређивања законске квалификације одређеног догађаја. Према дефиницији кривичног дела, Прогањање чини онај који у току одређеног временског периода другу особу без њеног пристанка прати, уходи, злоупотребљава њене податке, врши узнемиравање телефоном, било директном комуникацијом било слањем смс порука, слањем мејлова, путем друштвених мрежа, фејсбука, инстаграма и др., при чему за постојање кривичног дела није битно да ли се прогонилац и жртва познају и да ли су били у некој вези.

Поставља се и питање доказивања ових кривичних дела. Препорука је да жртве чувају све преписке и поруке које су примале, али и да се у вези свега поверавају блиским особама, пријатељима које би, након подношења кривичне пријаве, могле да сведоче у поступку. [303]

Полно узнемиравање

(Члан 182а)

(1) Ко полно узнемирава друго лице, казниће се новчаном казном или затвором до шест месеци.
(2) Ако је дело из става 1. овог члана учињено према малолетном лицу, учинилац ће се казнити затвором од три месеца до три године.
(3) Полно узнемиравање јесте свако вербално, невербално или физичко понашање које има за циљ или представља повреду достојанства лица у сфери полног живота, а које изазива страх или ствара непријатељско, понижавајуће или увредљиво окружење.
(4) Гоњење за дело из става 1. овог члана предузима се по предлогу.

За кривично дело Полно узнемиравање, Кривични законик каже да је то свако вербално, невербално или физичко понашање које има за циљ или представља повреду достојанства лица у сфери полног живота, а које за последицу има да код жртве изазива страх или ствара непријатељско, понижавајуће или увредљиво окружење. Циљ овог кривичног дела је превенција, али и да поред жртве штити јавни морал и нормалну атмосферу

[302] Нова кривична дела – Прогањање и Полно узнемиравање, (https://www.pravniportal.com/nova-krivicna-dela-proganjanje-polono-uznemiravanje/), приступљено 11.10.2019.године.
[303] *Ibid.*

у нашем друштву. Закон дефинише основни облик овог кривичног дела, као и тежи облик уколико је оштећени малолетно лице. Учинилац овог кривичног дела, дакле може бити свако лице без обзира на пол, а исто се односи и на жртву. По дефиницији кривичног дела могуће је да је учинилац мушкарац, а жртва жена или обрнуто, али такође и да су учинилац и жртва истог пола. Могуће је да учнилац буде један од супружника, а други супружник жртва, дечко, девојка, ванбрачни партнери и сл. Према законском опису кривичног дела, потребно да се деси више радњи којима се ствара непријатна и увредљива атмосфера. Радња извршења је свако вербално, невербално или физичко понашање, дакле било које понашање учиниоца које мора бити такво да има за циљ или представља повреду достојанства лица у сфери полног живота. [304]

[304] Нова кривична дела – Прогањање и Полно узнемиравање, (https://www.pravniportal.com/nova-krivicna-dela-proganjanje-polono-uznemiravanje/), приступљено 11.10.2019. године.

Литература

1. Accenture, „Accenture Cybersecurity Report“ https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf приступљено 01.09.2020
2. Al Islam, A., Sabrina, T.: Detection of various denial-of-service and distributed denial-of-service attacks using RNN ensemble, *Proceedings of the Twelfth International Conference on Computers and Information Technology*, 2009, стр. 604.
3. Алексић, Ж., Шкулић М.: *Криминалистика*, Службени гласник, Београд, 2007.
4. Aljazeera, http://balkans.aljazeera.net/vijesti/steta-od-cyber-napada-do-2022-godine-10000-milijardi-dolara? последњи пут приступљено 20.08.2022.
5. Al-Laham, Mohamad; Al-Tarawneh, Haroon; Abdallat, Najwan (2009). „Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy“ (PDF). *Issues in Informing Science and Information Technology*. **6**: 339–349. последњи пут приступљено 12 May 2021.
6. APG Yearly Typologies Report (2018); *Methods and Trends of Money Laundering and Terrorism Financing;* APG Secretariat, New South Wales
7. Ares Galaxy (https://en.wikipedia.org/wiki/Ares_Galaxy) приступљено 19.09.2019.год.
8. Arvicco, 'A Crypto-Decentralist Manifesto' (Ethereum Classic Blog, 11 July, 2016), https://ethereumclassic.github.io/blog/2016-07-11-manifesto/ (accessed on 25 October, 2017).
9. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder: Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction (Princeton University Press, 2016) ch 10.7
10. Avast, „What is a VPN“, https://www.avast.com/c-what-is-a-vpn последњи пут приступљено 27.10.2022.год.
11. Assets publishing service, „Cryptoassets Taskforce Final Report“, доступно на https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf; приступљено 25.07.2020.
12. Бошковић, М.: *Криминологија*, Правни факултет за привреду и правосуђе, Нови Сад, 2020.
13. B 92, „Teror: Više od 150 mrtvih, Pariz pod opsadom“, доступно на https://www.b92.net/info/vesti/index.php?yyyy=2015&mm=11&dd=14&nav_category=78&nav_id=1062857, приступљено 29.04.2020. године.
14. Baesystems, „Financial Crime Survey“, доступно на https://www.baesystems.com/en/cybersecurity/financial-crime-survey-2016# последњи пут приступљено 21.08.2022.
15. Bank in for security https://www.bankinfosecurity.asia/government-mulls-banning-cryptocurrencies-a-12628; приступљено 15.08.2020.
16. Bankinfosecurity, „Cybercrime Black Markets RDP Access Remains Cheap“, https://www.bankinfosecurity.eu/cybercrime-black-markets-rdp-access-remains-cheap-easy-a-13054?highlight=true последњи пут приступљено 21.08.2022.
17. Bankinfosecurity, „Suspected Hacker Faces Money Laundering Conspiracy Charges“, https://www.bankinfosecurity.eu/suspected-hacker-faces-money-laundering-conspiracy-charges-a-14359?highlight=true; приступљено 26.08.2020.
18. BBC, „Breaking Bad fan jailed over Dark Web ricin plot“, https://www.bbc.com/news/uk-england-34288380, приступљено 01.05.2020. године.

19. Berton, Beatrice, „The dark side of the web: ISIL's one-stop shop?". Report of the European Union Institute for Security Studies, 2015., доступно на Bitmixer, https://www.bitmixer.co/ приступљено 15.06.2020.
20. Brenner, S. W.: *Cybercrime: criminal threats from cyberspace*, An Inprint ABC-CLIO, LLC, Santa Barbara, USA, 2010, стр. 9.
21. Вилић, В.: *Повреда права на приватност злоупотребе друштвених мрежа као облик компјутерског криминалитета - докторска дисертација*, Ниш, 2016.
22. Вујаклија М., Лексикон страних речи и израза, Просвета-Београд, 1980.
23. Вулетић, Д.: *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011.
24. Вулетић, Д.: *Сајбер безбедност. Интегрална безбедност Републике Србије*, Факултет за пословне студије и право, Факултет за стратешки и оперативни менаџмент, Универзитет '"Унион-Никола Тесла'", Београд, 2017, стр. 176-181.
25. Вучуровић М., Порнографија- од пећине до сајбер простора, Либерто Београд 2014.
26. Van Valkenburgh et al., 'Distributed Collaborative Organisations: Distributed Networks and Regulatory Frameworks', Working Paper (2015), http://bollier.org/sites/default/files/misc-fileupload/ files/DistributedNetworksandtheLaw%20report,%20Swarm-Coin%20Center-Berkman.pdf, at 11 et seq.
27. Visual Capitalist, „What Happens in an Internet Minute in 2019?", доступно на https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/, приступљено 18.04.2020. године.
28. Gabriel Weimann, „Terrorist Migration to the Dark Web", Terrorism Research Initiative, 2016.
29. Gabriel Weimann: „Going Darker? The challenge of dark net terrorism", Woodrow Wilson Center, Washington.
30. Garrick Hileman, Michel Rauchs, „Global Cryptocurrency Benchmarking Study", 2017., стр. 13, доступно на https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf, приступљено 02.05.2020. године.
31. Global social media stats counter, доступно на https://gs.statcounter.com/social-media-stats, приступљено 18.04.2020. године
32. Globalincidentmap, Доступно на https://www.globalincidentmap.com/, приступљено 05.05.2020. године.
33. Grabosky, P.: The evolution of cybercrime, 2006-2016, In T. J. Holt (Ed.), *Cybercrime Through an Interdisciplinary Lens*. Routledge, NewYork, 2017.
34. Graphical Address Generator (royalforkblog.github.io) последњи пут приступљено 11.10.2022.год.
35. Guha, R., Furqan, Z., Muhammad, S: Discovering man-in-the-middle attacks on authentication protocols, *Proceedings of the IEEE Military Communications Conference*, 2007, 1-7.
36. Dailyfintech, „Follow the money crypto laundering" https://dailyfintech.com/2020/08/10/follow-the-money-crypto-laundering/ приступљено 16.08.2020.
37. Davoodalhosseini, M., Rivadeneyra, F., & Zhu, Y. (2020). CBDC and monetary policy (No. 2020-4). Bank of Canada. https://www.banqueducanada.ca/2020/02/note-analytique-personnel-2020-4/. последњи пут приступљено 12 May 2022.
38. Doek J., Greijer S., Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Luxembourg, 2016.

39. Ducas, E., & Wilner, A.S. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. International Journal, 72, pp. 538 - 562.
40. Ђукић, А. (2018) Организовани високотехнолошки криминал – појам, развој и основне карактеристике, Универзитет у Београду, Факултет безбедности
41. Ђукић, А. (2018) Организовани високотехнолошки криминал – појам, развој и основне карактеристике, Универзитет у Београду, Факултет безбедности
42. Eur-lex.europa https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=uriserv:OJ.C_.2015.414.01.0006.01.HRV&toc=OJ:C:2015:414:TOC; приступљено 10.09.2020.
43. eMule (https://en.wikipedia.org/wiki/EMule) приступљено 19.09.2019.год.
44. Енциклопедија британика: https://www.britannica.com/technology/P2P последњи пут приступљено 20.09.2022.год.
45. Ериксен, Т.: *Тиранија тренутка: брзо и споро време у информационом друштву*, Библиотека XX века, Београд, 2003.
46. +Euro Parlament, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf; приступљено 18.07.2020.
47. Europarlament, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf; приступљено 04.06.2020.
48. European Central Bank (October 2012). „1". *Virtual Currency Schemes* (PDF). Frankfurt am Main: European Central Bank. p. 5. . последњи пут приступљено 19 June 2021.
49. European Union: Framework Decision on attacks against information systems of the Commission of the European Communities, (Оквирна одлука о нападима на информационе системе Комисије европских заједница), 2005, доступно на: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN [05.04.2024]EUROPOL 2015.
50. EUROPOL 2017 Internet Organised Crime Threat Assessment (IOCTA), доступно на https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017, приступљено 03.05.2020.
51. Европол, *Internet Organised Crime Threat Assessment* 2018.
52. Закон о ауторским и сродним правима, *Службени гласник РС*, бр. 104/2009, 99/2011, 119/2012, 29/2016 – одлука УС и 66/2019 Више о томе на https://base.garant.ru/70414158/ или на https://en.wikipedia.org/wiki/Hash_function последњи пут приступљено 21.09.2022.год.
53. Закон о електронској трговини, *Службени гласник РС*, бр. 41/2009, 95/2013 и 52/2019.
54. Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, *Службени гласник РС*, бр. 94/2017 и 52/2021.
55. Закон о електронском потпису, *Службени гласник РС*, бр.135/2004.
56. Закон о играма на срећу, *Службени гласник РС*, бр. 18/2020.
57. Закон о кривичном поступку, *Службени гласник РС*, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – одлука УС и 62/2021 – одлука УС.
58. Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица, *Службени гласник РС*, бр. 85/2005
59. Закон о оптичким дисковима, *Службени гласник РС*, 52/2011.
60. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, *Службени гласник РС*, бр.61/2005 и 104/2009.

61. Закон о порезу на додату вредност, *Службени гласник РС*, бр.84/04, 86/04, 61/05 и 61/07)
62. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе малолетних лица, *Службени гласник РС*, бр. 32/2013
63. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе према малолетним лицима, *Службени гласник РС*, бр. 32/2013.
64. Закон о посебним мерама за спречавање вршења кривичних дела против полне слободе малолетних лица, *Службени гласник РС*, бр. 32/2013
65. Закон о посебним овлашћењима ради ефикасне заштите права интелектуалне својине, *Службени гласник РС*, бр. 46/2006, 104/2009 – др. закони и 129/2021.
66. Закон о потврђивању конвенције о високотехнолошком криминалу, *Службени гласник РС,* бр.19, 2009.
67. Закон о спречавању прања новца и финансирања тероризма, *Службени гласник РС*, број 91/2019.
68. Zirojević Mina, Ivanović Zvonimir Cyber law – Serbia**,** Institut za uporedno pravo, 2022.
69. Zhang, Y., Deng, F.,. Chen, Z., Xue, Y., Lin, C.: UTM-CM: A practical control mechanism solution for UTM systems, *Proceedings of the IEEE International Conference on Communications and Mobile Computing*, 2010.
70. *Zhou Xiaochuan (*2018): *Future Regulation on Virtual Currency Will Be Dynamic, Imprudent Products Shall Be Stopped for Now,* Xinhuanet.
71. IACA, „Cryptocurrency Crime Versus Control or the future of Money" https://www.iaca.int/iaca-alumni/blog-view-magazine/402-cryptocurrency-crime-versus-control-or-the-future-of-money.html приступљено 01.08.2022.
72. IBM, https://www.ibm.com/ibm/history/ibm100/us/en/icons/ebusiness/transform/ последњи пут приступљено 10.07.2022.
73. Ивановић, З. Криминалистички аспекти високотехнолошког криминала, КПУ, Београд, 2021.
74. IMF, http://www.imf.org/;
75. International Center for Counter-Terrorism (ICT),"The Telegram Chat Software as an Arena of Activity to Encourage the 'Lone Wolf' Phenomenon", 2016., доступно на https://www.ict.org.il/Article/1673/the-telegram-chat-software-as-an-arena-of-activity-to-encourage-the-lone-wolf-phenomenon#gsc.tab=0, приступљено 02.05.2020. године.
76. International Monetary Fond, „The Truth about the Dark Web", доступно на https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm последњи пут приступљено 20.08.2022.
77. Internet Organised Crime Threat Assessment (IOCTA), доступно на https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015, приступљено 01.05.2020. године.
78. Internetworldstats, https://www.internetworldstats.com/europa2.htm#links, ажурирано у децембру 2018. године, приступљено 20.04.2020. године.
79. Investopedia, https://www.investopedia.com/terms/g/genesis-block.asp последњи пут приступљено 07.10.2022.год.
80. ISS, „Alert_30_The_Dark_Web", https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf, приступљено 29.04.2020. године.
81. Jacob K., The Verge: „Twitter keeps loosing monthly users, so it's going to stop sharing how many", 2019., доступно на https://www.theverge.com/2019/2/7/18213567/

twitter-to-stop-sharing-mau-as-users-decline-q4-2018-earnings, приступљено 16.06.2020. године.
82. Jared G., Miami Herald: „Photo proves therapist lied about helping disabled kids and stole $41,000, prosecutors say“, доступно на https://www.miamiherald.com/news/nation-world/national/article219529365.html, приступљено 21.06.2020. године.
83. Joint Publication 1-02: *DoD Dictionary of Military Terms*, DC: Joint Staff, Joint Doctrine Division, Washington, J-7, USA, 2008.
84. Јонев: „Сајбер тероризам и употреба сајбер простора у терористичке сврхе“, Безбедност 2/2016.
85. JSTOR, https://www.jstor.org/stable/pdf/26297596.pdf?refreqid=excelsior%3A85c-63cb404e3dede02d74b93b6e77f6e, приступљено 02.05.2020. године
86. Justice, „New York City Man Charged Hacking Credit Card Trafficking And Money Laundering“, Достуно на: https://www.justice.gov/usao-ma/pr/new-york-city-man-charged-hacking-credit-card-trafficking-and-money-laundering последњи пут приступљено 22.08.2022.
87. Kartaltepe, E., Xi, S.: Towards blocking outgoing malicious impostor emails, Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006.
88. Kaspersky, „What is Cryptocurrency“, https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency последњи пут приступљено 05.10.2022.год.
89. Kaspersky, https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn, последњи пут приступљено 27.10.2022.год.
90. Katharina K., Dieter M., Edgar W., Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model, The Society of Service Science and Springer 2012.
91. Kollock, P., Smith, M.: *Communities in cyberspace*, Routledge, New York, 2001.
92. Kopecký, K: Cyber grooming danger of cyberspace (study), In: *Dangerous communication phenomena for teachers with a focus on cyberbullying, cyberstalking, cybergrooming and other socio-pathological phenomena,* 2010, 1-18.
93. Kostić Jelena, Stevanović Aleksandar, (ur.) *Finansijski kriminalitet*, Institut za uporedno pravo, Institut za kriminolška I sociološka istraživanja,, 2018.
94. Клаић Б, Велики рјечник страних ријечи, Зора Загреб, 1974.
95. Конвенција Савета Европе о заштити деце од сексуалног узнемиравања и сексуалног злостављања-незванични превод, (http://arhiva.mup.gov. rs/) приступљено 17.09.2019.године.
96. Константиновић Вилић, С., Николић Ристановић, В., Костић, М.: *Криминологија*, Ниш, 2012.
97. Кривични Законик, *Службени гласник РС,* бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019*)*
98. Кривични законик Републике Србије, *Службени гласник РС*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019.
99. Кривични законик, *Службени гласник РС*, бр. 85/2005, 88/2005 -ispr., 107/ 2005 -ispr., 72/ 2009, 111/ 2009, 121/2012, 104/2013 и 108/2014
100. Lagazio, M., Sherif, N., & Cushman, M.: A multi-level approach to understanding the impact of cyber crime on the financial sector, *Computers & Security*, 2014.

101. Lexisnexis, „Financial Institution Uplift Detection Money Mule Accounts“, https://risk.lexisnexis.com/global/en/insights-resources/case-study/financial-institution-uplift-detection-money-mule-accounts; приступљено 23.7.2020.
102. Li, P., Wang, Z., Tan, X.: Characteristic analysis of virus spreading in *ad hoc* networks, *Proceedings of the International Conference on Computational Intelligence and Security Workshops*, 2007.
103. Li, Xianghia. (2015). Transnational Organized Crime in the Context of Internet.; University of Vienna, Vienna
104. LimeWire (https://en.wikipedia.org/wiki/LimeWire) приступљено 19.09.2019.год.
105. LOC, „Cryptocurrency World Survey“, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf; приступљено 01.08.2020.
106. Malik, N. „Terror in the Dark“, a report by the the Henry Jackson Society, London, 2018., доступно на https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf, приступљено 01.05.2020. године.
107. McCusker, R. (2012). Organised cybercrime: myth or reality, malignant or benign? In S. Manacorda (Ed.) Cybercriminality: finding a balance between freedom and security Milano, Italy:ISPAC.
108. Mckinsey, „Financial Crime and Fraud in the Age of Cybersecurity“, https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity; приступљено 11.07.2020.
109. Mckinsey, „Financial Crime and Fraud in the Age of Cybersecurity“, https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity; приступљено 25.05.2020.
110. Mersch, Yves (16 January 2017). *Digital Base Money: an assessment from the ECB's perspective* (Speech). Farewell ceremony for Pentti Hakkarainen, Deputy Governor of Suomen
111. Metapicz, Доступно на http://metapicz.com/, приступљено 05.05.2020. године.
112. Milutinović, Monia (2018). „Cryptocurrency“. *Ekonomika*. 64 (1): 105–122.
113. Милан Манчевић, Дечја порнографија као облик високотехнолошког криминала-мастер рад, Правни факултет Универзитета у Нишу, 2017., стр.12.
114. Миленковић, Ј.: Криминална виктимизација деце, *Зборник радова студената докторских студија права* (ур. В. Ђурђић, М. Лазић), Ниш, 2014, стр. 43.
115. Министарство финансија Републике Србије (2017); билтен бр. 11; службена објашњења и стручна мишљења за примену финансијских прописа, Београд.
116. N. A. Hassan, R. Hijazi, *Open Source Intelligence Methods and Tools,* 2018. 1
117. Nai Fovino, I., Masera, M., Guidi, L., Carpi, G.: An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. *IEEE 3rd Conference on Human System Interactions (HSI)*, 2010, 679-686.
118. Народна банка Србије, „Надзор над финансијским инситуцијама“, https://nbs.rs/sr_RS/ciljevi-i-funkcije/nadzor-nad-finansijskim-institucijama/digital-imo/ последњи пут приступљено 22.09.2022.год.
119. National defense authorization Act for fiscal year 2006, Public Law 109-163, доступно на https://www.govinfo.gov/content/pkg/PLAW-109publ163/html/PLAW-109publ163.htm, приступљено 18.04.2020. године.
120. NATO Open source Intelligence handbook, доступно на NATO OSINT Handbook V 1.2: Free Download, Borrow, and Streaming: Internet Archive.

121. NATO OSINT Intelligence reader, доступно на NATO OSINT Reader FINAL Oct2002.pdf (cyberwar.nl)
122. NCPC, „Media_Release_on_Money_Mules", https://www.ncpc.org.sg/downloads/mediarelease/22-Nov-2013_Media_Release_on_Money_Mules.pdf; приступљено 23.7.2020.
123. NDTV, „the First Bitcoin Transaction", https://www.ndtv.com/business/the-first-bitcoin-transaction-was-for-buying-pizzas-more-interesting-tidbits-inside-2512643 последњи пут приступљено 07.10.2022.год.
124. Николић-Ристановић, В., Константиновић Вилић, С.: *Криминологија*, Прометеј, 2018, стр. 175.
125. Нова кривична дела – Прогањање и Полно узнемиравање, (https://www.pravniportal.com/nova-krivicna-dela-proganjanje-polono-uznemiravanje/), приступљено 11.10.2019. године
126. Nytimes, „cyber attacks temporarily cripple 2 israeli web sites", https://www.nytimes.com/2012/01/17/world/middleeast/cyber-attacks-temporarily-cripple-2-israeli-web-sites.html, приступљено 29.04.2020. године.
127. Onemilliontweetmap, Доступно на https://onemilliontweetmap.com/, приступљено 05.05.2020. године.
128. Open Source Initiative website, стална интернет адреса: https://opensource.org/osd.
129. Pankki – Finlands Bank. Helsinki: European Central Bank. последњи пут приступљено 19 June 2021.
130. Paccsresearch, https://www.paccsresearch.org.uk/wp-content/uploads/2019/06/WEIS_2019_paper_25.pdf последњи пут приступљено 05.08.2022.
131. Павловић, М.: *Борба против високотехнолошког криминала у Србији, достигнућа и изазови*, Београдски центар за безбедносну политику, Београд, 2022.
132. Parker, D. B.: *Computer Crime: Criminal Justice Resource,* National Institute of Justice, Washington, 1989.
133. PBC, http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html; приступљено 14.08.2020.
134. П2П мрежа (https://sr.wikipedia.org/sr-ec/P2P) приступљено 19.09.2019.год.
135. Петровић, С.: *Компјутерски криминал*, Војно-издавачки завод, Београд, 2004.
136. Портал отворених података Р. Србије, доступно на https://data.gov.rs/sr/posts/meta-podatsi/, приступљено 18.04.2020. године.
137. Ponemon, https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf; приступљено 26.08.2020.
138. Прља, Д., Кораћ, В: Малолетници и сајбер криминал, У: *Малолетници као учиниоци и жртве кривичних дела и прекршаја*, Институт за криминолошка и социолошка истраживања, 2015.
139. Rezaee Z., Riley R., (2009); *Financial Statement Fraud: Prevention and Detection,* JOHN WILEY & SONS PUBLISHING, New Jersey.
140. Републички завод за статистику, доступно на https://www.stat.gov.rs/sr-cyrl/, приступљено 18.04.2020. године.
141. Rotman, S., „Bitcoin versus electronic money", CGAP, Вашингтон, 2014., доступно на https://www.cgap.org/sites/default/files/Brief-Bitcoin-versus-Electronic-Money-Jan-2014.pdf, приступљено 02.05.2020. године.
142. Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System", доступно на https://bitcoin.org/bitcoin.pdf, приступљено 02.05.2020. године.

143. Савет Европе, (2016); *Истрага и процесуирање кривичних дела корупције идентификованих кроз ревизорске извештаје,* практикум за припаднике правосуђа и полиције, Београд.
144. Сергар Т., Врањеш С., (2013); *Откривање и спречавање финансијских превара у циљу јачања финансијских перформанси предузећа у Републици Српској,* ACTA ECONOMICA, број 19.
145. Спасојевић, Ђ., Миладиновић Боговац, Ж.: Малолетници као жртве кривичних дела учињених злоупотребом рачунарске мреже, *Научно-стручни часопис – Трендови у пословању*, 2018, VI(12).
146. Стакић, Б., Бараћ, С. (2007): Међународне финансије, ФФМО, друго измењено и допуњено издање, Београд.
147. Стевановић З.: Интернет зависност - од игре до патологије, *Ревија за криминологију и кривично право*, 1/2013, 66-67.
148. Стојановић З., Делић Н., (2013): *Кривично право посебни део,* Правни факултет универзитета у Београду.
149. Sciencedaily, https://www.sciencedaily.com/releases/2020/01/200116123805.htm приступљено 10.09.2020.
150. Shiri, F. I., Bharanidharan S., Norbik B. I.: A parallel technique for improving the performance of signature-based network intrusion detection system, *IEEE 3rd International Conference on Communication Software and Networks*, 2011.
151. Start, Доступно на https://start.me/p/wMdQMQ/tools, приступљено 05.06.2024. године.
152. Start, Доступно на https://www.start.umd.edu/, приступљено 05.05.2020. године.
153. Start, Доступно на https://www.start.umd.edu/gtd/, приступљено 05.05.2020. године.
154. Statista, „Global market share held by mobile operating systems since 2009", https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/ последњи пут приступљено 27.10.2022.год.
155. Tails boum, https://tails.boum.org/ последњи пут приступљено 28.10.2022.год.
156. Takanori Isobe, Kazuhiko Minematsu, „Breaking Message Integrity of an End-to-End Encryption Scheme of LINE", доступно на https://eprint.iacr.org/2018/668.pdf, приступљено 01.05.2020. године.
157. Тасић, В., Бауер, И.: *Речник комјутерских термина*, Микро књига, Београд, 2003.
158. TechLifestyle,„top5listanajboljiimejlklijentzaandroidu2021godini",https://www.tech-lifestyle.com/top-5-lista-najbolji/top-5-najbolji-imejl-klijent-za-android-u-2021-godini/
159. Techblog, доступно на https://techblog.comsoc.org/2016/03/09/idc-directions-2016-iot-internet-of-things-outlook-vs-current-market-assessment/, приступљено 18.04.2020. године..
160. Techbullion, „How the Bitcoin atms work and their advantages", https://techbullion.com/how-the-bitcoin-atms-work-and-their-advantages/ приступљено 28.07.2020
161. Telegraph, „Bitcoin Crackdown Amid Fears Money Laundering Tax Dodging", https://www.telegraph.co.uk/news/2017/12/03/bitcoin-crackdown-amid-fears-money-laundering-tax-dodging/, приступљено 03.05.2020. године.
162. The Institute for National Security Studies (INSS), „Backdoor Plots: The Darknet as a Field for Terrorism", 2013., доступно на https://www.files.ethz.ch/isn/170411/INSSInsights464.pdf, приступљено 29.04.2020. године.

163. The Journal, „Housing Market Ireland Cash Buyers Funds“ https://www.thejournal.ie/housing-market-ireland-cash-buyers-funds-2-2895200-Jul2016/ последњи пут приступљено 25.08.2022.
164. The New York Times, Isabel Kershner: „2 Israeli Web Sites Crippled as Cyberwar Escalates“, доступно на The Washington post, Sarah Kaplan: „Founder of app used by ISIS once said „We shouldn't feel guilty.“ On Wednesday he banned their accounts.“, доступно на Tineye, Доступно на https://tineye.com/, приступљено 05.05.2020. године.
165. Torproject, https://stem.torproject.org/faq.html последњи пут приступљено 27.10.2022. год.
166. Torproject, https://www.torproject.org/about/history/ последњи пут приступљено 24.10.2022.год.
167. Торент фајл (https://en.wikipedia.org/wiki/Torrent_file) приступљено 19.09.2019.год.
168. Treasury, доступно на https://www.treasury.gov/about/organizational-structure/offices/pages/office-of-foreign-assets-control.aspx последњи пут приступљено 22.05.2022.
169. Tulane University, „Everything you should know about dark web“, Стална интернет адреса: https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web.
170. United Nations: Crimes related to computer networks: background paper for the Workshop on Crimes related to the Computer Network, 2000, доступно на: https://digitallibrary.un.org/record/432653?v=pdf [10.04.2024]
171. United Nations: Manual on the Prevention and Control of Computer-related Crime, (Приручник УН о спречавању и контроли компјутерског криминала), 1994, доступно на: http://www.uncjin.org/Documents/EighthCongress.html [05.04.2024]
172. United Nations: Resolution 2007/20 of July 26, 2007, (Резолуција 2007/20 од 26. 07. 2007. године), 2007, доступно на: http://www.un.org/.../ecosoc/.../2007 [05.04.2024]
173. United Nations: Resolution on Missuse of the Internet for the Purpose of Sexual Exploatation, (Резолуција Уједињених Нација (тзв. Женевска резолуција) о злоупотреби интернета у сврху сексуалне експлоатације), 1998, доступно на: http://www.uri.edu/artsci/wms/hughes/ppr.htm [05.04.2024]
174. United Nations: UN General Assembly resolution 65/230, (Резолуција Уједињених Нација 65/230), 2010, доступно на: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [05.04.2024]
175. United Nations: UN resolution A/res/55/63 on combating the criminal misuse of information technologies, (Резолуција Уједињених Нација A/res/55/63 о борби против злоупотребе информационих технологија), 2000, доступно на: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [05.04.2024]
176. United Nations: UN resolution on computer crime legislation, (Резолуција Уједињених Нација о законодавству у области компјутерског криминалитета), доступно на: http://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.14 [05.04.2024]
177. UNODC, UN_Convention_Against_Corruption, https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf пут приступљено 05.10.2022.
178. Урошевић В., Ивановић З., Уљанов С., (2012), *Mač u world wide web-u, izazovi visokotehnološkog kriminala,* Enternal mix, Београд.
179. Устав Републике Србије, *Службени ɡласник РС*, бр. 98/2006.
180. UK Government Office for Science (2016): Distributed Ledger Technology: beyond blockchain. A report by the UK Government Chief Scientific Adviser, London, UK, 2016.

181. Facebook Investor relations, доступно на https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx приступљено 18.04.2020. године
182. FATF, https://www.fatf-gafi.org/ последњи пут приступљено 20.10.2022.год.
183. FATF, „FATF recommendations" http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html; приступљено 03.10.2022.
184. FATF, Glossary, https://www.fatf-gafi.org/glossary/u-z/ последњи пут приступљено 04.10.2020.
185. FATF, https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate); приступљено 28.08.2020.
186. FATF, Recomenation, https://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf последњи пут приступљено 22.09.2022.год.
187. Focus Group on Digital Currency including Digital Fiat Currency". *ITU*. http://www.itu.int/en/ITU-T/focusgroups/dfc/Pages/default.aspx. последњи пут приступљено 19 June 2021.
188. Forbes, „How the Darknet can be Used by Terrorists to Obtain Weapons" https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/#7c3a90be62cd, приступљено 02.05.2020. године.
189. Forbes, „Technology Psilocybin bitcoins" доступно на https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html?sh=2ab1e3f3353e последњи пут приступљено 05.10.2022.год.
190. Forbes, Nikita Malik: „How Criminals And Terrorists Use Cryptocurrency: And How To Stop It", доступно на https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#26f895623990, приступљено 02.05.2020. године.
191. Forbes, Nikita Malik: „How The Darknet Can Be Used By Terrorists To Obtain Weapons", доступно на https://www.forbes.com/sites/nikitamalik/2019/01/15/how-the-darknet-can-be-used-by-terrorists-to-obtain-weapons/ последњи пут приступљено 20.12.2024.
192. Freenetproject, https://freenetproject.org/pages/about.html последњи пут приступљено 26.10.2022.год.
193. Hacker, Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision
194. Harman D., „U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests", доступно на https://www.haaretz.com/.premium-isis-uses-bitcoin-for-fundraising-1.5366305,приступљено 02.05.2020. године.
195. Hacker, Philipp Chris Thomale: Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law, European Company and Financial Law, 2018, pp. 645-696.
196. Hacker, Philipp Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich edited by „Regulating Blockchain. Techno-Social and Legal Challenges", Oxford University Press, 2019.
197. Chainalysis, „Money Laundering Cryptocurrency 2019", https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019 приступљено 24.05.2020.
198. Checkpoint, „What is hacktivism", https://www.checkpoint.com/definitions/what-is-hacktivism/#, приступљено 29.04.2020. године.

199. Checkpoint, „What is Hacktivism", доступно на Internet filter, http://internetfilter-review.toptenreviews.com/internet-pornography-statistics. html
200. Cimaglobal, „The dark web and finance, The threat is real", https://www.cimaglobal.com/Members/Insights/The-dark-web-and-finance-The-threat-is-real/ последњи пут приступљено 18.08.2020.
201. Ciphertrace, „Cryptocurrency Anti Money Laundering Report" https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/; приступљено 22.05.2022.
202. Ciphertrace, https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/; приступљено 22.05.2020.
203. CISCO Community, https://community.cisco.com/t5/other-network-architecture-subjects/lan-switching-routing-ip-mac-stripping/td-p/534743 последњи пут приступљено 08.06.2024.год.
204. Cityam, „Foreign Criminals Laundering Money Drive London House Prices" http://www.cityam.com/220931/foreign-criminals-launderingmoney-drive-london-house-prices последњи пут приступљено 21.08.2022.
205. Claus Dierksmeier и Peter Seele, Cryptocurrencies and Business Ethics, у Journal of Bussiness Ethics, Springer Science+Business Media Dordrecht 2016 и 2018 Vol. 152, No. 1 (September 2018), pp. 1-14
206. Coinatmradar, https://coinatmradar.com/bitcoin_atm/15150/bitcoin-atm-general-bytes-szeged-change-valutavaltas/ приступљено 10.09.2020.
207. Coindesk, „US Congress Announce Study Virtual Currency Link Terrorism Today", https://www.coindesk.com/us-congress-announce-study-virtual-currency-link-terrorism-today,приступљено 03.05.2020. године.
208. CoinSchedule, 'Cryptocurrency ICO Stats 2017', https://www.coinschedule.com/stats.php (последњи пут приступљено 28.09.2022.
209. Cointelegraph, „What can I buy with bitcoins", https://rs.cointelegraph.com/bitcoin-for-beginners/what-can-i-buy-with-bitcoins; приступљено 23.09.2020.
210. Coursera, https://www.coursera.org/learn/cryptocurrency; приступљено 14.08.2020.
211. Coursera, https://www.coursera.org/specializations/wharton-fintech; последњи пут приступљено 22.06.2022.
212. Cvetković, Liability in the context of blockchain-smart contract nexus: introductory considerations, UDK: 347.4:[004.7:336.74 004.7 336.74, International Scientific Conference „Responsibility in the Legal and Social Context", held at the Faculty of Law, University of Nis, on 18 September 2020, pp.82-100.
213. Шкулић М., (2015); *Нормативна анализа положај жртве кривичног дела/оштећеног кривичним делом у кривичноправном систему србије,* Правни факултет, Београд.
214. Walker, J., Williams, B., Skelton, G.: Cyber security for emergency management, Proceedings of the *IEEE International Conference on Technologies for Homeland Security*, 2010.
215. Wall, D. S.: *Cybercrime: The transformation of crime in the information age*, Polity Press, Cambridge, UK, 2007.
216. Wall, D.S. (2017) Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing, University of Leeds, UK
217. Washington post, „Founder of app used by ISIS once said we shouldn't feel guilty on Wednesday", https://www.washingtonpost.com/news/morning-mix/wp/2015/11/19/

founder-of-app-used-by-isis-once-said-we-shouldnt-feel-guilty-on-wednesday-he-banned-their-accounts/, приступљено 02.05.2020. године.
218. WEFORUM, „Here Are The Biggest Cybercrime Trends Of 2019", https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/; приступљено 05.08.2022.
219. Weforum, „How AI can knock the starch out of money laundering", https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/; приступљено 02.06.2020.
220. Wellman, B., Gulia, M.: Virtual communities as communities – Net surfers don't ride alone, In Kollock P., Smith M., (ed) *Communities in cyberspace*, Routledge, New York, 2001.
221. Wen, W.: An improved intrusion detection system, *Proceedings of the International Conference on Computer Applications and System Modeling*, 2010.
222. Wikipedia, „Computational hardness assumption" https://en.wikipedia.org/wiki/Computational_hardness_assumption
223. Wilsoncenter, „Going Darker Challenge Of Dark Net Terrorism", https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf, приступљено 01.05.2020. године.
224. Wimmer, Andreas, „Dark net, Social Media and Extremism: Addressing Indonesian Counter terrorism on the Internet", доступно на https://www.academia.edu/20813843/Dark_net_Social_Media_and_Extremism_Addressing_Indonesian_Counter_terrorism_on_the_Internet, приступљено 02.05.2020. године.
225. Wimmer, Andreas, Aulia Nastiti, „Darknet, Social Media, and Extremism: Addressing Indonesian Counterterrorism on the Internet." Deutsches Asienforschungszentrum Asian Series Commentaries, Vol. 30-2015.
226. Yu, W., Nargundkar, S., Tiruthani, N.: A phishing vulnerability analysis of web-based systems, *Proceedings of the IEEE Symposium on Computers and Communications*, 2008, 326–331.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

007:004]:34(497.11)
339:004.738.5
343.53:004

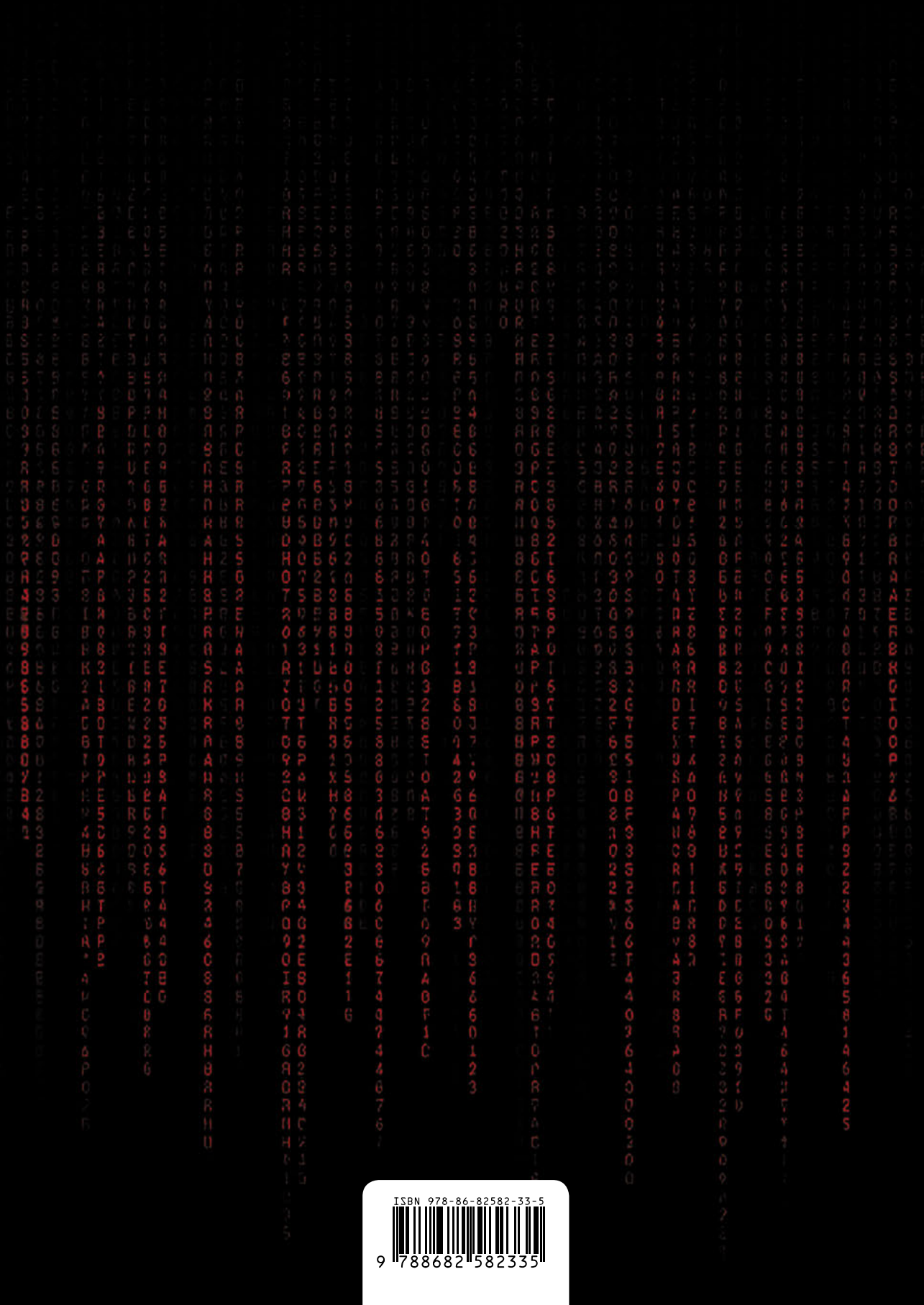
ЗИРОЈЕВИЋ, Мина, 1975-
Сајбер законодавство Србије. 2. део / Мина Зиројевић, Звонимир Ивановић. - Београд : Институт за упоредно право, 2025 (Београд : Birograf Comp). - 212 стр. : илустр. ; 24 cm
Тираж70. - Напомене и библиографске референце уз текст. - Библиографија: стр. 201-212.

ISBN 978-86-82582-33-5

1. Ивановић, Звонимир, 1976- [аутор]

а) Електронска трговина -- Правни аспект б) Високотехнолошки криминал в) Информационо-комуникационе технологије -- Тржиште -- Правни аспект -- Србија

COBISS.SR-ID 170947081



ISBN 978-86-82582-33-5