.

УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

# Dark Web – дигитални простор извршења кривичних дела

(Мастер рад)

Ментор

Проф. др Дарко Димовски

Студент

Ана Станојевић

Број индекса: М005/24-ИТ

Ниш, 2026.

.

# САДРЖАЈ

**УВОД……..5**

**1. ПОЈАМ И КАРАКТЕРИСТИКЕ DARK WEB-A……...8**

1.1. Интернет као глобални информациони систем……...8

1.2. Разграничење појмова: Surface Web, Deep Web и Dark Web……10

1.3. Darknet vs. Dark Web…….13

1.4. Техничке и организационе карактеристике Dark Web-a……...14

1.4.1. Анонимност, енкрипција и децентрализација……14

1.4.2. Функционисање кроз Tor мрежу и друге алате……..15

1.4.3. Улога криптовалута и псеудонимност трансакција……..…….18

**2. КРИМИНОЛОШКО ПОИМАЊЕ DARK WEB-A……..20**

2.1. Теоријска објашњења појаве криминалитета на Dark Web-у……...20

2.1.1. Теорија аномије и девијације……21

2.1.2. Теорија рационалног избора и опортунитета……..23

2.1.3. Теорије социјалног учења и субкултура……..26

2.1.4. Теорија ниске самоконтроле…….29

2.1.5. Теорија неутрализације…….31

2.2. Друштвени и психолошки аспекти коришћења Dark Web-a……33

2.3. Типови корисника на Dark Web- у……..35

**3. DARK WEB КАО ОКРУЖЕЊЕ ИЗВРШЕЊА КРИВИЧНИХ ДЕЛА…….38**

3.1. Категорије Dark Web сајтова……...38

3.1.1. Dark Web маркети ( илегална и полуилегална тржишта)……..38

3.1.2. Хакерски и syber crime сајтови……40

3.1.3. Leak и data-dump сајтови……...41

3.1.4. Форуми и online заједнице……....42

3.1.5. Dark Web претраживачи и дирекотријуми……..43

3.1.6. Платформе за узбуњиваче (Whistleblower platforms)…….43

3.1.7. Крипто услуге и миксери……..44

3.2. Настанак и еволуција Dark Web маркета ……...45

3.2.1. Прва генерација – појава Silk Road-a (2011–2013)…….46

3.2.2. Silk Road 2.0 (2013-2014)……..….49

.

3.2.3. AlphaBay (2015-2017)……....50
3.2.4. AlphaBay 2.0 (2021-2023)……..……54
3.2.5. Hansa Market (2015-2017)……..……55
3.2.6. Dream Market (2013-2019)…….57
3.2.7. Hydra Market (2015-2022)…….60
3.2.8. Савремена Dark Web тржишта……....63
**4. ТИПОЛОГИЈА КРИВИЧНИХ ДЕЛА НА DARK WEB-У…….65**
4.1. Неовлашћена производња и ствљање промет опојних дрога……...66
4.2. Секусална екпслоатација деце и дечија порнографија……..70
4.3. Трговина људима……..73
4.4. Трговина оружјем и експлозивним материјама…….76
4.5. Сајбер криминал као услуга (Cyber crime as a service - CaaS)…….78
4.5.1. Ransomware-as-a-Service (RaaS)……..….79
4.5.2. Phishing as a servise……....82
4.5.3. Zero-day експлоатације……..85
4.5.4. Украдени акредитиви (корисничка имена и лозинке)-Credential Theft.....89
4.5.5. Ботнети и DDoS услуге за изнајмљивање……...93
4.5.6. Алати засновани на Dark AI ( Мрачна вештачка интелигенција)……96
4.6. Прање новца путем криптовалута……...…99
**5. ОРГАНИЗАЦИЈА И СТРУКТУРА КРИМИНАЛНИХ МРЕЖА НА DARK WEB-У.....……101**
5.1. Мрежа ћелија као модел организације криминалних активности на Dark Web –у.....101
5.2. Организација криминалних мрежа на Dark Web –у……....103
5.3. Процес извршења кривичних дела на Dark Web–у (фазе, улоге и дистрибуција задатака)……..105
**6. КРИМИНОЛОШКИ АСПЕКТИ ОТКРИВАЊА И ПРЕВЕНЦИЈЕ DARK WEB КРИМИНАЛА……...…108**
6.1. Дигитална виктимологија и специфичности жртава на Dark Web-у……108
6.2. Дигитални отисак (Digital footprint) и његов значај……111
6.3. Методе праћења криминалаца на Dark Web-у……113

.

6.4. Праћење Dark Web-a (Dark Web monitoring)……...116
6.5. Криминолошки приступи превенцији криминала на Dark Web-у…….118
6.5.1. Примарна, секундарна и терцијарна превенција…….119
6.5.2. Улога образовања и дигиталне писмености у као фактори превенције кривичних дела на Dark Web-у…….120
6.5.3.Улога полиције, тужилаштва и међународних организација у борби против криминала на Dark Web-у…….122
**7. НОРМАТИВНИ И ИНСТИТУЦИОНАЛНИ ОКВИР СУЗБИЈАЊА DARK WEB КРИМИНАЛА……..125**
7.1. Међународни правни оквир (конвенције УН, Савет Европе – Будимпештанска конвенција)…….125
7.1.1. Конвенција УН против транснационалног организованог криминала из 2000. године- Палермска конвенција ……126
7.1.2. Резолуције генералне скупштине Уједињених нација 74/247 из 2019. године и 75/282 из 2021. године……...128
7.1.3. Конвенција Уједињених нација против сајбер криминала 2024. године…….....129
7.1.4. Конвенција Савета Европе о сајбер криминалу ( Будимпештанска конвенција, 2001)……....130
7.2. Национални законодавни оквир Републике Србије……132
7.3. Проблеми и изазови у правној квалификацији дела извршених на Dark Web-у……137
**8. ЗАКЉУЧАК……..139**
**Литература……141**
**Сажетак и кључне речи…….....147**
**Abstract and key words..... 148**
**Биографија студента…….....149**

.

## Увод

Савремено друштво карактерише интензиван развој информационо-комуникационих технологија, који је довео до дубоке дигитализације готово свих сфера друштвеног живота. Интернет је постао једна од кључних инфраструктура модерног света, омогућавајући брзу размену информација, глобалну комуникацију и развој нових економских и друштвених односа. Истовремено, овај технолошки напредак довео је и до појаве нових облика криминалитета који се прилагођавају дигиталном окружењу. Сајбер криминал, као један од најдинамичнијих облика савременог криминалитета, све чешће се испољава у комплексним и транснационалним облицима, што представља значајан изазов за традиционалне механизме кривичноправне заштите.

Посебно место у том контексту заузима такозвани Dark Web – део дигиталног простора који је намерно скривен од уобичајених претраживача и индексационих система, на коме су развијена илегална дигитална тржишта, позната као Dark Web маркети. На овим тржиштима врши се трговина опојним дрогама, оружјем, украденим подацима, малверима и другим незаконитим производима и услугама.

Предмет овог рада јесте свеобухватно криминолошко и правно сагледавање Dark Web-а као специфичног сегмента интернет простора који, услед својих техничких карактеристика, омогућава висок степен анонимности и представља погодно окружење за вршење различитих облика кривичних дела. У том смислу, рад обухвата анализу појма и основних карактеристика Dark Web-а, његово разграничење у односу на друге сегменте интернета – Surface Web и Deep Web – као и техничке механизме (енкрипција, децентрализација, Тор мрежа, криптовалуте) који условљавају његово функционисање.

Посебна пажња посвећена је криминолошком објашњењу овог феномена кроз релевантне теоријске приступе, као и друштвеним и психолошким аспектима коришћења Dark Web-а. Такође, анализирају се облици и структура кривичних дела која се на њему врше, као и начини организовања њихових извршилаца.

Значај теме огледа се у чињеници да Dark Web представља један од најдинамичнијих, недовољно регулисаних и тешко контролисаних дигиталних простора, у

.

коме се одвијају бројне илегалне активности, као што су трговина наркотицима, оружјем и људима, сексуална експлоатација деце, као и различити облици сајбер криминала. Поред тога, интензиван развој информационо-комуникационих технологија праћен је појавом нових облика криминалитета, познатих као „криминал као услуга“ (cybercrime-as-a-service), све широм употребом криптовалута и растућом софистицираношћу технолошких алата, што додатно отежава откривање и сузбијање ових појава.

Сходно томе, разумевање механизама функционисања Dark Web-а има посебан значај за унапређење криминолошке теорије, али и за проналажење ефикаснијих механизама откривања, доказивања и гоњења кривичних дела извршених у дигиталном окружењу, уз истовремено поштовање основних људских права и слобода.

Циљ рада је да се кроз интердисциплинарни приступ анализирају узроци, облици и механизми криминалитета на Dark Web-у, као и да се идентификују ефикасни начини његовог откривања и превенције. Такође, циљ је да се утврди у којој мери постојећи нормативни оквири, како на међународном тако и на националном нивоу, одговарају изазовима које доноси овај облик дигиталног криминалитета, као и да се идентификују кључни недостаци у правној регулативи и пракси и укаже на могуће правце њиховог унапређења.

Основне хипотезе рада полазе од претпоставке да кључне карактеристике Dark Web-а (анонимност, енкрипција и децентрализованост) значајно доприносе развоју и ширењу криминалних активности, као и да традиционални облици криминалитета у дигиталном окружењу добијају нове, софистицираније форме, што додатно отежава примену постојећих правних норми и ефикасно сузбијање криминалитета. Такође, претпоставља се да постојећи нормативни и институционални механизми, како на националном тако и на међународном нивоу, нису у потпуности усклађени са динамиком развоја Dark Web-а, те да је неопходно њихово даље унапређивање. Посебна хипотеза односи се на значај превентивних мера, укључујући развој дигиталне писмености и јачање институционалних капацитета, као кључних фактора у сузбијању овог облика криминалитета.

.

У раду ће бити примењене следеће научне методе: нормативно-правни метод за анализу међународних и националних правних аката који регулишу област сајбер криминала; криминолошки метод за анализу узрока, облика и структура криминалитета на Dark Web-у, уз ослањање на релевантне теорије (аномија, рационални избор, социјално учење и др.); компаративни метод за поређење различитих правних и институционалних решења; као и дескриптивно-аналитички метод за систематизацију постојећих сазнања и емпиријских података, уз примену методе анализе садржаја научне и стручне литературе, извештаја међународних организација и релевантних статистичких података.

.

# 1. ПОЈАМ И КАРАКТЕРИСТИКЕ DARK WEB-A

## 1.1. Интернет као глобални информациони систем

Интернет представља најзначајнији глобални информациони систем савременог доба, који омогућава размену података, комуникацију и приступ информацијама без просторних и временских ограничења. Као мрежа међусобно повезаних рачунарских мрежа, Интернет функционише на основу заједничких техничких стандарда и протокола, пре свега TCP/IP протокола, који омогућавају интероперабилност различитих уређаја и система широм света [1].

Основна карактеристика Интернета као глобалног информационог система огледа се у његовој децентрализованој структури. Не постоји јединствени центар управљања, већ се систем заснива на великом броју аутономних мрежа које добровољно прихватају заједничка правила комуникације. Оваква архитектура доприноси високом степену отпорности система, његовој стабилности и континуираном развоју [2]. Интернет обухвата различите сервисе и апликације који омогућавају приступ и обраду информација, као што су World Wide Web (WWW), електронска пошта, друштвене мреже, сервиси за размену датотека, видео конференције, cloud сервиси и платформе за електронско пословање. Посебан значај има World Wide Web као хипертекстуални систем који омогућава лако претраживање и повезивање информација путем веб-страница [3].

Интернет функционише по концепту клијент/сервер. Сервери су моћни рачунари који 24 сата обрађују велике количине података, док клијенти (корисници) постављају упите серверима и траже информације. За правилан проток података задужен је TCP/IP протокол, а сваки рачунар добија јединствену IP адресу, која се састоји од четири скупа бројева од 0 до 255, одвојених тачкама (нпр. 55.66.90.190). Због лакшег памћења уведен је DNS (Domain Name Server) систем, који преводи текстуална имена сервера у бројеве,

[1] V. Cerf, R. Kahn, „A Protocol for Packet Network Intercommunication“, *IEEE Transactions on Communications*, Vol. 22, No. 5, 1974

[2] A. S. Tanenbaum, D. J. Wetherall, *Computer Networks*, 5th ed., Pearson Education, Boston, 2011.

[3] T. Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*, HarperCollins, New York, 2000.

.

омогућавајући лак приступ ресурсима (нпр. https://www.prafak.ni.ac.rs/)[5]. Интернет такође користи различите протоколе и технологије за пренос података, укључујући HTTP/HTTPS (за web комуникацију), FTP (за размену датотека), SMTP и IMAP (за електронску пошту), VoIP (за гласовне позиве) и модерне cloud технологије које омогућавају складиштење и обраду података у реалном времену.

Градња интернет инфраструктуре у Југославији започета је 1992. године на основу пројекта Министарства за науку и технологију, којим су дефинисана тела, изглед, услуге и задаци Интернета. Планом је било предвиђено да држава оформи агенцију за управљање интернетом, али су немили догађаји у региону успорили планирани развој. Улагања у инфраструктуру и приступну мрежу настављена су од 1992. године, док је непрекидан приступ интернету за већину корисника остао недостижан до средине 1996. године. Након увођења интернета на српско тржиште, број корисника растао је просечном годишњом стопом од 150%, али је Србија по броју корисника и даље била на зачетку европских земаља, са приступом који је имало тек око 10% становништва[6].

Као глобални информациони систем, Интернет има кључну улогу у образовању, науци, привреди, култури, здравственом систему и јавним службама. Омогућава брз пренос знања, приступ научним базама података, дигиталним библиотекама и платформама за учење на даљину. У привреди омогућава електронско пословање, маркетинг, глобалну трговину и развој дигиталне економије, док у култури и друштвеним мрежама олакшава размену информација, креативност и глобалну сарадњу [7]. Интернет такође има значајан утицај на иновације и развој нових технологија, као што су вештачка интелигенција, IoT (Internet of things - Интернет ствари), 5G мреже и blockchain технологија, што додатно шири његову примену и комплексност[8].

[4] D. Comer, *Internetworking with TCP/IP*, Vol. 1, 6th ed., Pearson, 2013.
[5] Ibid.
[6] Министарство науке и технологије Југославије, Извештај о развоју Итернета 119-1996, Београд, 1997
[7] M. Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press, Oxford, 2001
[8] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge, 2007.

.

Глобални карактер Интернета носи бројне изазове и ризике у техничкој, друштвеној и правној сфери. Лакоћа приступа, анонимност и огромна количина података омогућавају бројне злоупотребе, као што су:

- Сајбер криминал: крађа идентитета, phishing, ransomware и хаковање система
- Малициозни софтвер и вируси: тројанци, spyware и други програми који могу украсти податке или омогућити неовлашћени приступ
- Подреда приватност података, као што је ризик од цурења поверљивих информација и нежељеног профилисања
- Дезинформације и лажне вести, односно ширење пропаганде и манипулација јавним мњењем.
- Психолошки ризици: зависност од интернета, смањење социјалних интеракција, нарушавање менталног здравља .
- Кибернетички напади на државе и критичну инфраструктуру: енергетски системи, банкарски сектор, транспорт.
- Правни изазови: отежана примена националних закона и међународних регулатива због глобалне природе Интернета.

Сви ови ризици захтевају мултидисциплинарни приступ: техничка решења (енкрипција, firewall, antivirus), едукацију корисника, правне оквире и међународну сарадњу.

### 1.2. Разграничење појмова: Surface Web, Deep Web и Dark Web

Интернет се састоји од различитих слојева информација који се могу класификовати према доступности и индексацији[9] од стране претраживача. Основни слојеви интернета обухватају ***Surface Web*** (површински веб), ***Deep Web*** (дубоки веб) и ***Dark Web*** (тамни веб). Сваки од ових слојева има своје специфичне карактеристике, намену и ниво приступачности.

[9] Индексација је процес којим претраживачи (као што су Google, Bing или Yahoo) организују и чувају информације са веб страница у својим базама података, како би их касније могли брзо и прецизно приказати у резултатима претраге. Извор: IBM. *What is Indexing?* IBM Knowledge Center, 2026.

.

### 1. Surface Web (Површински веб)

Површински веб представља део интернета који је индексиран и доступан јавним претраживачима као што су Google Chrome, Safari, Mozilla Firefox, Bing и Yahoo. Укључује јавне веб странице, блогове, новинске портале, интернет продавнице, видео садржаје на YouTube-у, странице друштвених медија и друге отворене информације. Површински веб чини мањи део укупног интернет садржаја, само око 4–5% укупног интернет садржаја, али је најчешће доступан и највише коришћен од стране обичних корисника интернета.[10] Други термини за површински веб укључују видљиви веб, lightnet или индексирани веб[11].

### 2. Deep Web (Дубоки веб)

Deep Web (Дубоки веб), познат као и невидиви или скривени веб, [12]обухвата огроман део интернета који није индексиран претраживачима, што значи да садржај не може бити пронађен преко Google-а или Bing-а без одговарајућег приступа[13]. У овај слој спадају приватне базе података, интернет банкарство, е-пошта, кориснички налози заштићени лозинком, финансијске, медицинске и научне архиве, полицијски и владини ресурси, сајтови за онлајн игре, веб странице са захтевом за регистрацију, услуге засноване на претплати као што су Netflix, HBO Max, Apple TV+, Amazon Prime и Spotify, корпоративни интернет системи и складиштење у облаку као што су Dropbox или iCloud. Deep Web укључује и друге садржаје који захтевају аутентификацију или специјалан приступ.

Велики део Deep Web-а је легалан и безбедан, и широко се користи за приватну и корпоративну комуникацију, али је недоступан јавности због природе садржаја и ограничења приступа. Технички је сложенији од површинског веба јер информације нису индексиране; приступ се обично остварује познавањем тачних URL адреса или

---

[10] IBM. *Understanding the Dark Web*. IBM Research, 2026.

[11] McAfee. *The Dark Web: A Definitive Guide***.** (преузето: 31. 01. 2025) https://www.mcafee.com/learn/the-dark-web-a-definitive-guide/.

[12] Термин „Дубоки веб“ сковао је 2001. године рачунарски научинк Мајкл. К. Бергман, који га је разликовао од термина „површинкси веб“

[13] Britannica, *Deep Web*, (преузето: 31.01.2025). https://www.britannica.com/technology/deep-web

.

коришћењем специфичних платформи[3]. Процењује се да дубоки веб садржи око 96% онлајн садржаја и да је приближно 500 пута већи од површинског веба[4].

Садржај који се налази на површини веба доступан је јер га софтверски роботи, познати као „пауци“[14] или претраживачи, хватају и индексирају, додељујући му рангирање. Ови системи обично скенирају веб странице са доменима као што су .com, .org, .net, као и неке податке на сајтовима друштвених медија. Пауци прате уграђене линкове како би открили додатни садржај. Касније, када корисници претражују одређени садржај, резултати се појављују у претраживачу и постају јавно доступни[15].

Само око 4% целокупног online садржаја је слободно доступан на површинском, веб-у, остатак је скривен у дубоком вебу. То значи да јавност нема директан начин да претражи огромну количину неиндексираног садржаја. Веб странице често користе методе за спречавање индексације, као што су CAPTCHA**,** више IP адреса за исти садржај, садржај који није у HTML формату, заштита лозинком и садржај без линкова[6]. Иако претраживање дубоког веба није инхерентно ризично, постоје потенцијалне дигиталне опасности као што су злонамерни софтвер, вируси, шпијунски софтвер и кејлогери[16]. Поред тога, могуће је наћи осетљиве податке који се могу злоупотребити, а корисници се могу сусрести са појединцима који се баве сајбер криминалом или другим неетичким активностима[7].

### 3. Dark Web (Тамни веб)

Dark Web (Тамни веб) [17] је потпуно скривен део дубоког веба, који је доступан само кроз специјализоване мреже и софтвер као што је Tor (The Onion Router) или I2P[18].

---

[14] Паук, такође назван веб-бот или crawler, је софтверски програм који аутоматски прелиста веб странице, прати линкове и прикупља садржај ради индексације од стране претраживача, TechTarget. *Web Crawlers Explained: How Search Engines Work*, 2026, ( преузето дана 07.01.2026. године) https://www.techtarget.com/whatis/definition/crawler

[15] Ibid

[16] Keyloggeri (keyloggers) су софтверски или хардверски алати за дигитално прислушкивање који прате и снимају све што корисник откуца на тастаури. Често се користе као шпијунска средства за крађу лозинки, личних података и кредита, а могу служити и за надзор запослених. Заштита од ових алата укључује ажуриран антивирус и опрез при отварању сумњивих линкова.

[17] Најранији облик модерног Dark Web-а насто је у марту 2000. године, када је ирски студент Ијан Кларк развио и објавио Freenet, који је нудио анонимну комуникацију на мрежи путем децентрализоване мреже корисника Freenet.

.

Карактерише га висок ниво анонимности, што омогућава приватну комуникацију и размену информација, али и потенцијал за илегалне активности, као што су трговина забрањеним материјалима, хакерске услуге и трговина дрогом[19].

На Dark Web- у се не може приступити кроз стандардне веб прегледаче попут Firefox-a или Chrome-a. Приступ се остварује само преко шифрованих peer-to-peer мрежа или преклапајућих анонимизујућих мрежа као што је Tor. Tor обезбеђује потпуну анонимност коришћењем више слојева шифровања, мреже релеја и механизма за усмеравање саобраћаја који насумично усмерава интернет саобраћај, чиме се практично онемогућава праћење IP адресе корисника. Tor прегледач је бесплатан за преузимање и ради на свим главним оперативним системима. Поред Tor-a, корисници могу додатно заштитити свој идентитет коришћењем виртуелне приватне мреже (VPN).

Иако је Dark Web део Deep Web-a, он чини само мали сегмент интернета и технички је сложенији од површинског и дубоког веба. URL-ови на Dark Web-у обично користе домен *.onion*, што их чини тешко доступним и невидљивим за стандардне претраживаче. Поред илегалних активности, Dark Web се користи и за легитимне сврхе, као што су заштита приватности, комуникација новинара, активиста или корисника који желе анонимност на интернету[2].

### 1.3. Darknet vs Dark Web

Dark Web и Darknet су појмови који се често користе као синоними, али међу њима постоји јасна разлика. Darknet представља затворену мрежну инфраструктуру која функционише путем специјализованих протокола и софтвера, попут Tor-a, омогућавајући анонимну и енкриптовану комуникацију између корисника. Насупрот томе, Dark Web представља садржај који се налази унутар darknet-a, односно означава скуп web-страница i online сервиса ( на пример .onion domeni), који су хостовани унутар таквих мрежа и којима се може приступити искључиво преко Darknet мрежа. Док је Darknet технички оквир који

[18] TechTarget, *Dark Web definition*, (преузето 12.01.2026. године ) https://www.techtarget.com/whatis/definition/dark-web
[19] DarknetSearch. *Dark Web Overview and Security Risks*. DarknetSearch Reports, 2026.

.

омогућава приватност и заштиту идентитета, Dark Web представља садржајни слој те инфраструктуре, који може укључивати како легитимне, тако и незаконите активности.

### 1.4. Техничке и организационе карактеристике Dark Web –а

#### 1.4.1. Анонимност, енкрипција и децентрализација

Висок ниво анонимности представља једну од кључних техничких карактеристика Dark Web-a, која се и остварује се применом напредних техника за сакривање идентитета корисника и метаподатака комуникације, пре свега употребом специјализованих анонимизујућих мрежа, пре свега Tor (The Onion Router). Анонимност подразумева онемогућавање идентификације корисника, његове IP адресе и географске локације током комуникације на интернету. За разлику од класичног интернета, где су IP адреса, локација и обрасци саобраћаја често лако доступни провајдерима и трећим лицима, анонимизујуће мреже настоје да онемогуће повезивање корисника са конкретним активностима. Tor мрежа функционише као преклапајућа (overlay) мрежа која усмерава интернет саобраћај кроз низ насумично одабраних релеја, при чему ниједан појединачни чвор нема увид и у извор и у одредиште комуникације, чиме се значајно смањује могућност идентификације корисника и праћења његових активности.[20]

Техничка основа анонимности на Dark Web-у јесте onion routing, механизам који подразумева вишеслојну енкрипцију података и њихово прослеђивање кроз више независних релеја. Сваки релеј у мрежи дешифрује само један слој енкрипције и располаже искључиво ограниченим информацијама – зна само адресу претходног и наредног чвора, али не и комплетан пут комуникације. Овај вишеслојни механизам спречава централни надзор и значајно отежава саобраћајну анализу, чак и у условима напредних техника масовног електронског надзора.[21].

Поред анонимности, енкрипција представља суштински безбедносни механизам Dark Web-a. Комуникација унутар анонимних мрежа заштићена је снажним криптографским алгоритмима, који обезбеђују поверљивост, интегритет и аутентичност

[20] Encyclopaedia Britannica. (n.d.). *Tor (network).* ( преузето 15.01.2026)https://www.britannica.com/technology/Tor-encryption-network

[21] Dingledine, R., Mathewson, N., Syverson, P., *Tor: The Second-Generation Onion Router*, US Naval Research Laboratory, 2004.

.

података. Енкрипција спречава неовлашћени приступ, пресретање или измену садржаја и представља суштински елемент заштите приватности корисника, што је од посебног значаја за новинаре, активисте, узбуњиваче и друге кориснике који делују у репресивним политичким окружењима. Истовремено може бити злоупотребљена за прикривање илегалних активности, што представља значајан изазов за органе кривичног гоњења и отвара сложена правна и етичка питања у вези са балансом између права на приватност и јавне безбедности.

Трећа важна карактеристика Dark Web-a јесте децентрализација**.** За разлику од класичних веб сервиса који се ослањају на централне сервере и провајдере, анонимне мреже попут Tor-a, I2P-a или Freenet-a су дизајниране су тако да не поседују централни сервер или управљачко тело. Оваква архитектура значајно повећава њихову отпорност на цензуру, гашење сервиса и техничке нападе, али и и контролу од стране државних или корпоративних актера. Децентрализована структура омогућава континуирано функционисање мреже чак и у случају уклањања појединих чворова, што је уједно и један од разлога зашто је правно регулисање и контрола Dark Web-a изузетно сложена[4].

Комбинација анонимности, енкрипције и децентрализације чини Dark Web технички сложеним и функционално специфичним делом интернета и указује на његову изражену дуалну природу. Са једне стране може служити као простор за остваривање легитимних сврха, као што је заштита слободе говора, приватности и људских права у дигиталном окружењу, док са друге стране представља простор за развој различитих облика сајбер криминала, укључујући трговину илегалном робом, прање новца и организоване криминалне активности.

### 1.4.2. Функционисање кроз Tor мрежу и друге алтернативне мреже

Назив „Tor“ је скраћеница од *The Onion Router* („слојевити усмеривач“)[22]. Tor обезбеђује анонимност корисника тако што шифрује саобраћај у више слојева. Саобраћај пролази кроз три насумично изабрана Tor чвора, при чему се на сваком чвору дешифрује

[22] The Onion Router је првобитно развијен у америчкој истераживачкој лабораорији морнарице САД-а средином деведесетих говина прошлог века као начин заштите преноса обавештајних података путем интернета, коришћењем вишеструких слојева шифровања одатле и назив „onion“ – лук).

.

један слој, а трећи чвор шаље поруку ка одредишту. На овај начин Tor прикрива трагове корисника и отежава праћење комуникације.

Основу Tor мреже чине Tor чворови (*nodes* или *relays*), које постављају и одржавају волонтери. Постоје различите улоге чворова:

- **Улазни заштитни чворови (*entry guards*)** – обезбеђују да нападач не надгледа оба краја комуникације. Чворови који имају ову улогу бирају се на основу стабилности и саобраћаја.
- **Мостни чворови (*bridge relays*)** – користе се када провајдер или држава блокира Tor. Њихове IP адресе нису јавне, што отежава цензору да спречи приступ.
- **Излазни чворови (*exit nodes*)** – шаљу саобраћај ван Tor мреже ка одредишту на интернету. Саобраћај излазног чвора је откодован, па постоји ризик да излазни чвор може видети садржај порука ако није шифриран (HTTPS).

Корисник Tor мреже мора знати који чворови постоје. То обезбеђују именички сервиси (*directory authorities*), који дигитално потписују списак чворова. Софтвер Tor користи списак само ако већина именичких сервера потврди његову валидност, што спречава компромитовање мреже. Именички сервиси се редовно ажурирају и одржавају их поуздани чланови Tor заједнице.

Уклопни превозници (*pluggable transports*) маскирају Tor саобраћај као обичан интернет саобраћај, тако да цензори не могу открити да корисник користи Tor. Они раде заједно са мостним чворовима како би омогућили приступ Tor мрежи у условима цензуре.

Tor омогућава анонимност и за сервере који желе да остану невидљиви на интернету. Скривени сервиси *(*hidden/onion services*)* користе *.onion* домене и доступни су искључиво кроз Tor. Саобраћај иде кроз шест чворова (три од стране корисника и три од стране сервиса), што обезбеђује анонимност обе стране. Скривени сервиси се користе за: анонимне веб сајтове и блогове, форуме и платформе за слободу говора у цензурисаним

.

земљама и безбедне комуникационе сервисе. Због додатних чворова, веза је спорија од уобичајеног интернета, али нуди виши ниво приватности.[23]

Поред Tor мреже, постоје и друге технологије које омогућавају анониман приступ интернету и Darkweb-у. Међу најпознатијим су I2P, Freenet и VPN. Ове мреже функционишу по различитим принципима, а њихова заједничка особина је обезбеђивање приватности и анонимности корисника.

**I2P (Invisible Internet Project)** представља анонимну overlay мрежу намењену комуникацији и размену података унутар саме мреже. За разлику од Tor мреже, која омогућава анониман приступ интернету, I2P је фокусиран на анонимност унутар мреже. Сваки чвор у I2P мрежи делује као једнак учесник, шифрујући и прослеђујући саобраћај других чворова, чиме се онемогућава праћење порука до њиховог оригиналног пошиљаоца. Мрежа се одржава кроз добровољне чворове који међусобно размењују информације и креирају тунеле кроз које се саобраћај шаље. Коришћењем Garlic routing технике, где се више порука шифрује и шаље заједно, додатно се повећава сигурност и отежава анализа саобраћаја. У I2P мрежи сваки корисник комуницира преко inbound и outbound тунела, а идентификација чворова се одвија кроз дистрибуирану базу података, што елиминише потребу за централизованим сервером[24].

**Freenet** је дистрибуирана peer-to-peer мрежа чији је циљ анонимно објављивање и преузимање садржаја. Мрежа не користи централне сервере, већ свако чвориште учествује у складиштењу и прослеђивању података, при чему чворови не знају идентитет пошиљаоца или примаоца. Садржај се у мрежи складишти помоћу хеш кључева за мутабилне или непокретне податке, што омогућава трајно и безбедно чување информација. Freenet подржава два режима рада: Opennet, који омогућава повезивање са било којим чворовима, и Darknet, који повезује само проверене и поверењем одабране партнере, чиме се повећава сигурност. Мрежа је дизајнирана тако да наставља да

[23] CERT.hr. (2018). *Tor mreža – tehnička pozadina i napredno korištenje* (Verzija 1.00). Nacionalni CERT. (преузетдо дана 17.01.2026. гоидне)https://www.cert.hr/wp-content/uploads/2018/02/tor_tehnicka_pozadina_i_napredno_koristenje.pdf
[24] I2P. (n.d.a). *I2P documentation: Introduction to I2P*. ( преузето 17.01.2026), https://beta.i2p.net/en/docs/overview/intro/

.

функционише и ако појединачни чворови буду искључени, што јој даје високу отпорност на цензуру[25].

**VPN (Virtual Private Network)** представља технологију која обезбеђује шифровану комуникацију преко јавног интернета. За разлику од I2P и Freenet-а, VPN користи клијент-сервер архитектуру и централисан приступ. Подаци се шифрују на корисниковом уређају, затим се шаљу кроз VPN тунел до сервера који их дешифрује и прослеђује ка одредишту. VPN замењује стварну IP адресу корисника својом, што прикрива локацију и идентитет. Технологија користи различите протоколе тунелирања као што су IPsec, OpenVPN и WireGuard, који обезбеђују стабилну и безбедну везу. Иако VPN омогућава приватност саобраћаја, његова анонимност зависи од политике провајдера, а мрежа је мање отпорна на нападе у поређењу са децентрализованим решењима попут I2P и Freenet-а[26] [27].

Свака од ових технологија има своје предности и мане. I2P је идеалан за анонимну комуникацију унутар мреже, али је приступ интернету ограничен. Freenet омогућава трајно и анонимно складиштење података, али функционише искључиво унутар своје дистрибуисане мреже. VPN пружа брз и једноставан приступ интернету са заштитом саобраћаја, али захтева поверење у провајдера и није потпуно децентрализован. У пракси, ове мреже се често комбинују за постизање највећег нивоа анонимности и приватности.

### 1.4.3. Улога криптовалута и псеудонимност трансакција

Криптовалуте[28] представљају облик дигиталне, односно виртуелне имовине који се заснива на примени криптографских метода ради обезбеђивања сигурности трансакција, контроле емисије нових јединица и верификације преноса вредности. За разлику од

[25] Freenet Project. (n.d.). *Freenet manual: Introduction*. (преузето 19.01.2026.), https://freenet.org/resources/manual/introduction/

[26] Cisco Systems. (n.d.). *How VPN works*. Retrieved (преузето 19.01.2026.), https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

[27] GeeksforGeeks. (n.d.). *What is VPN? How it works & types of VPN*. Retrieved (преузето 20.01.2026.), https://www.geeksforgeeks.org/computer-networks/what-is-vpn-how-it-works-types-of-vpn

[28] Bitcoin представља прву модерну криптовалуту са ограничењем од 21 милион Биткоина. Први пут је објављена у White paper-у 2008. godine, коју је објавио Satoshi Nakamoto, псеудоаонимна особа или група. Bitcoin је данас највећа светска криптовалута која се најчешће користи и све се више посматра као легитимно средство оразмене.

.

традиционалних валута које издају централне банке, криптовалуте функционишу у оквиру децентрализованих система, без постојања централног ауторитета или посредника, као што су банке или друге финансијске институције.

Основу функционисања криптовалута чини технологија **блокчејн** (*blockchain*), која представља дистрибуирану и јавну дигиталну књигу у којој се хронолошки бележе све извршене трансакције. Сваки блок у ланцу садржи скуп потврђених трансакција, временски жиг и криптографски хеш претходног блока, чиме се обезбеђује интегритет података и онемогућава њихова накнадна измена без сагласности већине учесника у мрежи.

Потврђивање трансакција у криптовалутним системима врши се применом механизама консензуса, који омогућавају децентрализованим учесницима да постигну сагласност о валидности података. Најпознатији механизам је *Proof of Work* (PoW), у оквиру којег тзв. рудари користе значајне рачунарске ресурсе ради решавања комплексних математичких проблема, док се у савременијим системима све чешће примењује *Proof of Stake* (PoS), као енергетски ефикаснији модел. Као награду за успешно верификовање новог блока, учесници мреже добијају одређену количину криптовалуте.

Трансакције криптовалутама реализују се посредством дигиталних новчаника, који функционишу на основу асиметричне криптографије и садрже пар криптографских кључева: јавни кључ, који служи као адреса за пријем средстава, и приватни кључ, који омогућава располагање криптовалутом и дигитално потписивање трансакција[5]. Иако идентитет корисника није непосредно видљив, све трансакције су јавно доступне на блокчејну, због чега се криптовалуте у стручној литератури најчешће дефинишу као псеудоанонимне, а не као потпуно анонимне.

Захваљујући наведеним техничким карактеристикама, криптовалуте налазе примену у различитим областима, као што су електронско плаћање, међународни трансфери новца, паметни уговори (*smart contracts*) и децентрализоване финансијске услуге (*DeFi)*. Истовремено, њихова примена отвара значајна правна, економска и

.

безбедносна питања, нарочито у контексту спречавања прања новца, финансирања криминалних активности и потребе за адекватном регулативом дигиталне имовине.[29]

## 2. КРИМИНОЛОШКО ПОИМАЊЕ ДАРК WEБА

### 2.1. Теоријска објашњења појаве криминалитета на Dark Web-у

Разумевање криминалитета који се одвија на Dark Web-у захтева мултидисциплинарни приступ, јер овај облик криминала обухвата елементе класичних, технолошких и психолошких девијација. У савременој криминологији, неколико теоријских концепата пружа најадекватнији оквир за анализу мотивације, услова и динамике извршења кривичних дела у дигиталном окружењу, међу којима се издвајају: теорија аномије и девијације, теорија рационалног избора и опортунитета, теорија социјалног учења и субкултура, теорија ниске самоконтроле и теорија неутрализације .

Примена ових теорија у анализи криминалитета на Dark Web-у омогућава свеобухватан приступ који повезује структурне, индивидуалне, социјалне и моралне факторе. Теорија аномије објашњава друштвене узроке и притиске који подстичу девијантно понашање; теорија рационалног избора и опортунитета анализира свесне одлуке и услове који олакшавају извршење кривичних дела; теорија социјалног учења и субкултура приказује процес учења и нормализацију криминала унутар дигиталних заједница; теорија ниске самоконтроле истиче диспозиције и импулсивност починилаца; док теорија неутрализације разоткрива моралне рационализације и психолошке механизме оправдања девијантоног понашања.

Истовремено, ове теорије чине интегративни модел разумевања криминалитета на Dark Web-у, који повезује повезујући друштвену структуру, индивидуалне карактеристике и специфичности дигиталног окружења савременог криминала.

[29] Урошевић, У. (н.д.). Шта су крипто валуте – како функционишу, Електонско пословање, Универзитет Црне Горе, ( преузето 21.01.2026.)
https://www.ucg.ac.me/skladiste/blog_22181/objava_56875/fajlovi/EP%20_%207.pdf

.

### 2.1.1. Теорија аномије и девијације

Реч аномија потиче од грчке речи ***anomía*** *(ἀνομία),* где префикс *a-* значи „без“, а nomos *(νόμος)* „закон, што значи „без закона“[30]. Концепт аномије први су разматрали антички филозофи, укључујући Плутарха и Платона, који су уочавали везе између моралог реда и стабилности друштва. Почетком двадесетог века аномија је постала повезана са идејом недостатка друштвених норми. У савременој социологији, француски социолог Жан Мари Гијо (*Jean-Marie Guyau*) је у својој књизи „Скица моралности без обавезе и санкције (1884. године) користио је термин аномија да опише друштвено безакоње и одсуство моралних правила[31].

Аномија је стање друштвене нестабилности које настаје када норме, вредности и очекивања друштва постану нејасни или неефикасни у регулисању понашања појединаца. Концепт аномије је увео француски социолог Émile Durkheim 1893. године у својој књизи „Подела рада у друштву“,  како би описао осећај одвојености, без сврхе и несигурности у односу на оно што је друштвено прихватљиво. Он је указао да аномија често настаје у периоду брзих друштвених промена, када старе норме више не важе, а нове још нису усвојене, остављајући људе без јасног моралног водича.

Диркем је повезивао аномију са различитим облицима друштвене кризе, укључујући економске потресе, технолошке промене и распад традиционалних заједница. У таквим условима људи могу да осете губитак смисла, изолацију или фрустрацију, а друштво као целина постаје подложно повећаном нивоу девијантног понашања. Један од најпознатијих примера који је Диркем истраживао је феномен самубиства[32], који је показивао као последицу аномије, када људи губе осећај припадности и контроле над својим животом.

Роберт Мертон је касније развио и проширио идеју аномије у оквиру своје теорије напетости (*strain theory или means-end theory).*[33] Он је указао да аномија настаје као

[30] Simply Psychology. (n.d.). *Anomie: Definition, theory, & examples*. Simply Psychology. (преузето 28.01.2026.) https://www.simplypsychology.org/anomie.html/
[31] Guyau, J.-M. (1884). *Esquisse d’une morale sans obligation ni sanction*. Paris: Félix Alcan.
[32] Durkheim, É. (1897). *Suicide: A study in sociology*. London: Routledge
[33] Merton, R. K. (1938). *Social structure and anomie.* American Sociological Review, 3(5), 672–682.

.

резултат конфликта између друштвено прописаих циљева, као што су богатство и успех, и ограничених легитимних средстава за њихово постизање. Када људи нису у могућности да легитимним путем остваре друштвене стандарде успеха, јавља се напетост која може водити ка девијантном понашању, као што су криминал или одбацивање друштвених норми. Мертонов модел показује да аномија није само питање индивидуалне моралне конфузије, већ и структурни проблем друштва који утиче на понашање великих група људи. Ова теорија повезује друштвене промене, недостатак норми и осећај отуђености са појавом девијантног понашања и криминала.

Примери девијантног понашања у условима аномије укључују кривична дела против имовине као средство за остваривање финансијских циљева, кривична дела са елементима насиља као реакцију на друштвену фрустрацију, развој зависности од алкохола и опојних дрога као механизма суочавања са осећајем безнађа, као и економски криминал, попут проневера и корупције, нарочито код појединаца изложених притиску друштвених очекивања успеха[7].

У савременом друштву, у којем велики број појединаца тежи материјалној добити, моћи и друштвеном статусу које реално не може да постигне легалним путем, Dark Web се појављује као алтернативна платформа за остваривање тих циљева. Захваљујући високом степену анонимности и одсуству ефикасног институционалног надзора, Dark Web омогућава појединцима да путем незаконитих активности, као што су трговина опојним дрогама, оружјем и финансијске преваре, настоје да компензују структурна ограничења са којима се суочавају.

Деловање у дигиталном окружењу, а нарочито у простору Dark Web-а који функционише изван стандардних друштвених и моралних норми, може допринети слабљењу личне одговорности и деградацији моралних вредности. У таквом окружењу појединци лакше занемарују последице сопствених поступака, што олакшава прибегавање криминалним активностима, јер се она не доживљавају као озбиљно кршење правила која важе у свакодневном друштвеном животу. Поред тога, појединци који се осећају економски, социјално или културно маргинализовано могу развити осећај фрустрације и отуђености, што их мотивише да траже алтернативне заједнице, идентитете и циљеве

.

управо у анонимном дигиталном простору Dark Web-a. На тај начин, Dark Web може створити привид алтернативне једнакости и доступности ресурса, али се тај осећај равноправности остварује кроз девијантне и илегалне активности, што додатно продубљује аномију и подрива друштвене норме.

### 2.1.2. Теорија рационалног избора и опортунитета

Теорија рационалног избора (*Rational Choice Theory – RCT*) има своје корене у класичној школи кривичног права, пре свега у делима Чезареа Бекарије (1738–1794) и Џеремија Бентама (1748–1832). Бекарија је у делу О злочинима и казнама (*Dei delitti e delle pene*, 1764) је први јасно формулисао идеју да је криминал резултат рационалног избора, заснованог на процени користи и штете и истакао да људи делују рационално и да ће се уздржати од криминала ако су казне извесне, брзе и пропорционалне делу, док је Бентам развио концепт хедонистичког калкулуса, према којем људи при доношењу одлука мере задовољство (корист) у односу на бол (трошак), што је утемељило утилитаристички приступ рационалности[34].

У савременој криминологији, Гари Бекер (1930–2014), сматра се оснивачем савремене теорије рационалног извора у криминологији. У чланку *Crime and Punishment: An Economic Approach* (1968) он је формализовао криминал као рационалну економску одлуку и примњнио економски модел на криминално понашање, у коме је предложио да потенцијални учиниоци процењују очекиване користи и трошкове пре извршења кривичног дела[35].

Рационални избор подразумева да потенцијални учиниоци пре извршења дела процењују могуће користи (нпр. материјалну добит, друштвени статус) и трошкове (нпр. вероватноћу откривања и хапшења, тежину казне). Када очекиване користи превазилазе перципиране трошкове, криминално понашање постаје рационална опција. Важно је нагласити да ови „трошкови“ и „користи“ нису ограничени искључиво на новчане добитке или губитке, већ обухватају и друштвени статус, психолошко задовољство, као и

[34] Fiveable. (n.d.). *Rational Choice Theory of Criminology*. ( преузето 26.01.2026.), https://fiveable.me/crime-human-development/unit-1/rational-choice-theory/study-guide/
[35] Becker, G. S. (1968). *Crime and punishment: An economic approach*. Journal of Political Economy, 76(2), 169–217.

.

емоционалне награде или одвраћајуће факторе. Овај приступ је тесно повезан са теоријом рутинских активности, према којој до криминала долази када мотивисани учиниоци налете на погодне мете у одсуству способних чувара[36].

Дерек Корниш и Роналд Кларк су током осамдесетих година XX века додатно развили овај приступ, уводећи концепт ситуационог доношења одлука, наглашавајући да непосредни фактори, као што су привлачност мета, присуство чувара, безбедносне мере и дизајн окружења, утичу на доношење одлука у конкретним околностима.[37]

Теорија рационалног избора има значајне импликације за кривичну политику. Она заговара повећање перципираних трошкова кривичног дела путем брзих, извесних и пропорционалних казни, као и примену мера ситуационе превенције, укључујући промене у дизајну окружења (нпр. боље осветљење, видео-надзор) контролу приступа и мере „очвршћавања“ мета, које смањују могућности за извршење кривичних дела мењањем калкулације трошкова и користи код потенцијалних учинилаца. Сходно томе, креатори политика треба да обликују кривичноправне системе тако да криминал постане мање привлачан избор. Теорија рационалног избора указује и на значај награђивања законитог понашања. Стварање подстицаја за легитимне изборе – као што су могућности запослења, социјална подршка и програми у заједници – може учинити конформне животне путеве рационалнијим и привлачнијим.

Теорија рационалног избора тесно је повезана са теоријом опортунитета и теоријом рутинских активности. Теорија опортунитета наглашава да криминално понашање зависи од присутности погодних прилика (opportunities)**.** Чак и мотивисани учиниоци неће починити кривично дело ако нема приступ мети или ако околности не дозвољавају извршење.[3] На основу ове логике развијена је ситуациона превенција криминала, која

[36] Wikipedia. (2023). *Rational choice theory (criminology)*. (преузето 02.02.206. године) https://en.wikipedia.org/wiki/Rational_choice_theory_(criminology)

[37] Soztheo. (n.d.). *Rational Choice Theory*. (преузето 02.02.206. године) https://soztheo.com/theories-of-crime/classical-rational-choice/rational-choice-theory

.

укључује дизајн окружења, контролу приступа и очвршћавање мета, како би се смањила привлачност кривичних радњи[38].

Теорија рутинских активности, развијена од стране Lawrence Cohen и Marcus Felson (1979), прецизира механизам појаве прилика, указујући да криминал настаје када се сусретну три елемента: мотивисан учинилац, погодна мета и недостатак способног чувара[39]. Овај приступ објашњава како свакодневне рутине и активности појединаца формирају прилике за криминал. Теорија рутинских активности је у суштини „операционализована“ верзија теорије опортунитета, јер објашњава како се прилике јављају у свакодневном животу.

Комбиновањем ових три теорије добијамо свеобухватан оквир за разумевање криминала на Dark Web-у. Теорија рационалног избора објашњава психолошки и економски процес доношења одлуке код учиниоца. Потенцијални учиниоци процењују добит од илегалних активности, као што су трговина дрогом, оружјем или хакерским услугама, у односу на ризик откривања, хапшења и губитка анонимности. Криптовалуте и специјализоване анонимне мреже, попут Tor или I2P, обезбеђују висок степен анонимности и смањују ризик од индентификације, чиме се криминал чини рационално привлачним, јер учинилац види већу очекивану корист него потенцијалне трошкове. Починиоци свесно бирају дигитални простор, јер он макимизује корист и минизује могућност откривања. Теорија опортунитета показује структурне и ситуационе факторе који омогућавају или блокирају извршење кривичних дела. Форуми на Dark Web платформи представљају средину у којој су прилике за криминал стално присутне, а недостатак способног чувара, обезбеђен високим степеном анонимности и употребом криптовалута, омогућава понављање илегалних радњи[40]. Теорија рутинских активности објашњава како свакодневне навике и понашање учинилаца и корисника формирају сталне прилике. Мотивисани учинилац који редовно користи анонимне мреже, као што је

[38] Wikipedia. (2023). *Opportunity theory (criminology)*; *Routine activity theory*. (преузето 03.02.206. године) https://en.wikipedia.org/wiki/Opportunity_theory_(criminology) и https://en.wikipedia.org/wiki/Routine_activity_theory

[39] Cohen, L. E., & Felson, M. (1979). *Social change and crime rate trends: A routine activity approach*. American Sociological Review, 44(4), 588–608.

[40] Clarke, R. V., & Cornish, D. B. (1985). *Modelling offenders' decisions: A framework for research and policy*. Crime and Justice, 6, 147–185

.

Dark Web, свакодневно прегледа специјализоване форуме и учествује у трансакцијама, стално се сусреће са погодним метама које траже илегалне услуге[41]. Ова комбинација високог мотива, погодних прилика и слабог надзора објашњава зашто је криминал на Dark Web-у толико присутан.

### 2.1.3. Теорија социјалног учења и субкултура

Теорија социјалног учења *(Social learning theory - SLT)* представља један од најзначајнијих теоријских приступа у савременој криминологији, јер криминално и девијантно понашање објашњава као резултат нормалних друштвених процеса учења. Уместо да криминал тумачи као последицу биолошких предиспозиција или индивидуалних психопатолошких особина, ова теорија полази од претпоставке да се криминал усваја, одржава и репродукује кроз друштвене интеракције, нарочито у оквиру примарних група и субкултурних окружења[42].

Теорија социјалног учења је интегрисана торија, у смислу да уједињује елементе више криминолошких и психолошких приступа. Њени теоријски темељи социјалног учења налазе се у теорији диференцијалне асоцијације Едвина Садерленд-а (*Edwin Hardin Sutherland-a),* који је први систематски тврдио да се криминал учи кроз комуникацију са другима, при чему појединци усвајају мотиве, технике и рационализације које погодују кршењу закона[43]. Садерленд је нагласио да учесталост, трајање, интензитет и приоритет друштвених односа имају пресудан значај за формирање криминалних образаца понашања. Иако није развио прецизне механизме учења, његова теорија поставила је основу за касније, теоријски разрађенија објашњења.

Полазећи од уоченог недостатка Садерлендове теорије у погледу јасне разраде механизама учења, Роберт Л. Бурџес и Роналд Л. Акерс су 1966. године формулисали теорију диференцијалне асоцијације–појачања. У овом приступу, Садерлендове пропозиције су преформулисане у бихејвиоралним терминима, уз увођење принципа

[41] Cohen, L. E., & Felson, M. (1979). *Social change and crime rate trends: A routine activity approach*. American Sociological Review, 44(4), 588–608
[42] Akers, R. L. (2017). *Social learning and social structure: A general theory of crime and deviance* (2nd ed.). London: Routledge.
[43] Sutherland, E. H. (1947). *Principles of criminology* (4th ed.). Philadelphia: J. B. Lippincott

.

оперантног условљавања и појачања, чиме је криминално понашање концептуализовано као облик понашања који се учи на исти начин као и свако друго, кроз интеракцију, али и одржава путем награда и казни.

Према Акерсу, социјално учење криминала одвија се кроз четири међусобно повезана процеса: диференцијалну асоцијацију, дефиниције, диференцијално појачање и имитацију[44]. Диференцијална асоцијација односи се на обрасце друштвених односа у којима појединац долази у контакт са особама које већ испољавају криминална понашања или изражавају ставове повољне према криминалу. Ови односи не подразумевају само искључиво учење техника извршења кривичних дела, већ и усвајање вредности и норми које криминал легитимишу.

Други кључни елемент теорије чине дефиниције, односно ставови, уверења и вредносне оријентације појединца према законима и друштвеним нормама. Криминално понашање је вероватније када појединац усваја дефиниције које су повољне према кршењу закона или које неутралишу моралну осуду криминала. Такве дефиниције могу укључивати рационализације, оправдања или умањивање тежине последица криминалног понашања[45].

Централни механизам одржавања криминалног понашања представља диференцијално појачање, које се заснива на равнотежи између награда и казни. Понашање које доноси материјалне, друштвене или симболичке награде, а не бива доследно санкционисано, има већу вероватноћу да се понавља. Акерс наглашава да награде не морају бити непосредне или формалне; често су то признање вршњачке групе, статус у субкултури или осећај припадности[46].

Четврти елемент теорије је имитација, која подразумева учење понашања путем посматрања других, нарочито када су ти други перципирани као успешни, ауторитативни

[44] Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press.
[45] Akers, R. L. (2011). *Social learning theory*. In F. T. Cullen, J. P. Wright, & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 230–240). New Brunswick, NJ: Transaction Publishers.
[46] Akers, R. L. (2009). *Social learning and social structure: A general theory of crime and deviance* (Rev. ed.). New Brunswick, NJ: Transaction Publishers.

.

или награђени за своја дела. Овај процес је посебно изражен код младих и у субкултурним групама у којима криминални модели понашања имају висок симболички значај.

У каснијој фази развоја, Акерс је формулисао концепт теорије социјалне структуре и социјалног учења, чиме је теорију проширио на макросоциолошки ниво[7]. У овом моделу, фактори попут сиромаштва, друштвене неједнакости, дезорганизације заједнице или маргинализације не делују директно на криминално понашање, већ посредно, кроз обликовање друштвених односа и процеса социјалног учења. Другим речима, друштвена структура утиче на то са ким се појединци повезују, које дефиниције усвајају и какве облике појачања доживљавају.

У том контексту, теорија социјалног учења има снажну везу са субкултурним теоријама криминала. Субкултуре представљају друштвене групе са релативно стабилним вредносним системима који се разликују од доминантних друштвених норми. У криминалним субкултурама, понашања која су у ширем друштву санкционисана могу бити позитивно вреднована, чиме се стварају услови за интензивно социјално учење криминала. Акерс наглашава да субкултуре не производе криминал саме по себи, већ функционишу као окружења у којима се криминално понашање учи, нормализује и награђује[47].

Теорија социјалног учења објашњава криминално понашање на Dark Web-у као резултат друштвеног учења у окружењима високог нивоа анонимности и приступа илегалним тржиштима. Овај виртуелна платформа ствара окружење које омогућава корисницима кроз диференцијлне асоцијације на форумима, тржиштима и затвореним заједницама интерагују са другим појединцима који већ учествују у кривичним активностима, као што су трговина наркотицима, оружјем или крађа података, и при том усвајају ставове, вредности и рационализације које легитимишу та дела. Виртуелне заједнице и форуми делују као примарне групе у којима се формирају ове асоцијације, а време проведено у међусобном размењивању искустава са искуснијим криминалцима о хаковању, енкрипцији, продаји забрањених супстанци и другим облицима криминалних

[47] Akers, R. L. (2017). *Social learning and social structure: A general theory of crime and deviance* (2nd ed.). London: Routledge.

.

активности повећава вероватноћу учења и репродукције криминалних модела. Понашање које је у „реалном свету“ санкционисано, у Dark Web окружењу може бити перципирано као прихватљиво или чак похвално, што илуструје дигиталну улогу дефиниција. На пример, хакерски успеси или успешна трговина илегалним робама могу се рационализовати као „вештине“ или „пословне могућности“, што смањује осећај кривице и нормализује девијантно понашање.

Диференцијално појачање је у виртуелном окружењу индиректно, социјално и симболичко. Учесници добијају награде кроз репутацију на форумима, статус у online заједницама, приступ бољим изворима илегалних добара или социјалну потврду од других корисника, док су казне благе или ретке због анонимности мреже, што додатно појачава понављање криминалних активности. У том смислу, појачање није само материјално већ и социјално и психолошко, што је типично за дигиталне субкултуре.

На крају, имитација игра значајну улогу на Dark Web-у. Нови учесници уче од искуснијих актера, посматрају успешне трансакције, технике хаковања и начине избегавања полицијских контрола, који модели постају стандарни обрасци понашања којима се руководе нови чланови  и имају велики симболички значај у онлајн субкултурама.

### 2.1.4. Теорија ниске самоконтроле

Теорију ниске самоконтроле *(Self-Control Theory – SCT)* је формулисао Мајкл Р. Готфредсон *(Michael R. Gottfredson*) заједно са Трависом Хиршијем *(Travis Hirschi)* 1990. године у делу A General Theory of Crime.[48][49] Иако нису били први који су истраживали улогу интерне контроле у криминалу или улогу самоконтроле у понашању Готфредсон и Хирши су поставили концепт самоконтроле у први план као главни фактор криминалног понашања. Они су указали на недостатак индивидуалне самоконтроле као кључни фактор криминалног понашања, полазећи од претпоставке да је људско понашање у великој мери

[48] Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford University Ppess.
[49] Hirschi, T. (2004). *Self-Control and Crime*. In *Criminological Theory* (pp. 536–544). Roxbury Publishing.

.

усмерено ка тражењу тренутних задовољстава и избегавању бола, што је у складу са хедонистичким рационалним приступом класичне криминологије[50].

Иако је корист од криминала обично пролазна и мала, док су негативне последице одложене, појединац са ниском самоконтролом, због недостатка предвиђања и пажње према дугорочним последицама упушта се у криминал. Главна теза теорије ниске самоконтроле је да ниска самоконтрола резултује кратковидошћу и импулсивним понашањем, па лице са високим самоконтролом процењује дугорочне последице и одустаје од преступа, док лице са ниском самоконтролом следи тренутни импулс без узимања у обзир будућих ризика и казни.

Самоконтрола је дефинисана као тенденција појединца да тежи краткорочном задовољству без узимања у обзир дугорочних последица својих дела, што чини низак ниво самоконтроле главним предиктором криминала. Готфредсон и Хирши истичу да људи са ниском самоконтролом обично делују импулсивно, имају малу осетљивост на потребе других, више се ослањају на физичка него на ментална решења, ризикују, доносе кратковиде одлуке, имају слабу вербалну комуникацију. Ове особине се обично јављају заједно и имају тенденцију да перзистирају кроз живот, чинећи самоконтролу стабилном конструкцијом у објашњењу криминала.

SCT као кључни фактор у развоју самоконтроле истиче ефикасно родитељство током првих 8–10 година живота. Ефикасно родитељство обухвата праћење понашања детета, идентификацију и санкционисање непримереног понашања, уз показивање наклоности према детету[51]. Теорија тврди да је након детињства ниво самоконтроле фиксиран: особе које нису развиле самоконтролу остају предиспониране за импулсивно и криминално понашање, док особе са високим нивоом самоконтроле имају стабилну способност одлагања задовољстава. SCT такође минимизира значај каснијих социјалних утицаја као што су вршњаци или животне околности, сматрајући да они углавном само одражавају већ формирану самоконтролу[29]. Теорија предвиђа да криминалност након детињства остаје стабилна, али да постоји вишеструкост облика криминала, јер све

[50] Felson, M., & Osgood, D. W. (2008). *Crime and everyday life* (4th ed.). Sage.
[51] Hirschi, T. (2004). *Self-control and crime*. In *Criminological theory* (pp. 536–544). Roxbury Publishing

.

криминалне активности пружају тренутно задовољство на штету дугорочних последица. SCT тако представља „мотивисаног преступника“, где је низак ниво самоконтроле кључна детерминанта криминала, а не само присуство мотива за криминал[56].

Током последњих 30 година SCT је била предмет стотина емпиријских студија које су у великој мери потврдиле главну тврдњу да је ниска самоконтрол један од најјачих предиктора криминалног понашања[52][53]. Мета-анализе су показале да самоконтрола значајно предвиђа криминалитет, чак и када се контролишу други фактори, као што су социјални утицаји и економски услови.

Примена теорије ниске самоконтроле може се проширити и на дигитални контекст, посебно на Dark Web, где прилике за анонимно деловање и привидна неухватљивост појачавају склоност ка импулсивним поступцима. Особине које су карактеристичне за SCT, као што су импулсивност, кратковидост и тежња ка тренутном задовољству, могу се уочити код појединаца који користе Dark Web за обављање нелегалних трансакција без разматрања дугорочних последица по сопствену безбедност или социјални статус[54]. Пошто свака илегална активност на Dark Web-у пружа одређену краткорочну корист, било да је реч о финансијском профиту, приступу забрањеним информацијама или задовољавању личних интереса, особе са ниском самоконтролом имају тенденцију да учествују у различитим облицима дигиталног криминала, што је у складу са концептом “мотивисаног преступника”. На пример, трговина дрогом путем криптовалута омогућава тренутно задовољство у виду финансијске користи или приступа супстанцама, али истовремено носи ризик од будућег кривичног гоњења.

### 2.1.5. Теорија неутрализације

Теорију неутрализације развили су Дејвид Матза (*David Matza*) и Грешам Сајкс (Gresham Sykes) током 1950-их и 1960-их година, а коју су представили у кључном раду

[52] Hay, C., & Meldrum, R. (2016). The general theory of crime: A meta-analysis of the relationship between low self-control and criminal offending. *Criminal Justice and Behavior, 43*(4), 489–513.
[53] Burt, C. H. (2015). Low self-control and crime: A review of the literature. *Journal of Criminal Justice, 43*(4), 211–221.
[54] Wall, D. S. (2015). *Dark web: Exploring and mitigating criminal opportunities*. Routledge

.

*Techniques of Neutralization: A Theory of Delinquency*[55]. Ова теорија објашњава начин на који појединци који чине кривична дела оправдавају своје поступке како би ублажили осећај кривице и избегли одговорност. Хипотеза Матзе и Сајкса је била да појединци увек имају свест о својој моралној обавези да се придржавају закона и у себи носе обавезу да избегавају илегалне радње. Они су ову идеју повезали са концептом drift-a (*померање или „дрфтовање")*[56] — појединци прелазе између легитимног и нелегитимног понашања, јер задржавају везу са конвенционалним вредностима, али у одређеним околностима неутралишу своје моралне уздржавајуће механизме како би извршили преступ и потом се поново вратили конформизму[57]. Ово одваја теорију неутрализације од претходних теорија које су тврдиле да преступници стварају потпуно одвојен морални систем супротан друштвеним нормама.

Матза и Сајкс су идентификовали пет специфичних техника неутрализације које преступници користе да би оправдали ,односно неутрализовали свој однос према нормама друштва:

1. **Негирање одговорности *(Denial of responsibility)*** – преступник тврди да је био приморан спољним околностима да почини злочин и стога не осећа личну одговорност.
2. **Порицање штете (*Denial of injury)*** – преступник инсистира да његови поступци нису нанијели штету, па се не ради о истинском преступу. На пример, илегално преузимање филмова или музике може бити оправдано тиме што штета није очигледна.
3. **Негирање жртве *(Denial of the victim*)** – преступник тврди да жртва заслужује оно што јој се догодило или да није стварна жртва.
4. **Осуђивање оних који осуђују (*Condemnation of the condemners)*** – преступник преусмерава критику на оне који га осуђују, инсистирајући да су они неправедни или лицемерни

[55] Sykes, G. M., & Matza, D. (1957). *Techniques of Neutralization: A Theory of Delinquency*. American Sociological Review, 22(6), 664–670
[56] Matza, D. (1964). *Delinquency and Drift*. Wiley.
[57] Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review, 22*(6), 664–670.

.

5. **Позивање на више циљеве *(Appeal to higher loyalties)*** – преступник оправдава незаконите поступке тврдећи да служе вишем циљу, нпр. крађа да би се помогло болесном детету.

Посматрајући примену ове торије на починиоце кривичних дела на Dark web-у можемо закључити да су овакве рационализације својствене овој теорији често присутне, посебно међу починиоцима сајбер превара, пиратерије, дистрибуције забрањеног садржаја и дигиталног насиља У овом контексту, теорија неутрализације пружа снажан оквир за разумевање психолошких и моралних оправдања која корисници ове платформе користе за уклапање илегалних активности у свој систем вредности**,** омогућавајући опстанак криминалног понашања у условима где друштвени надзор изостаје.

### 2.2. Друштвени и психолошки аспекти коришћења Dark Web –а

Друштвени и психолошки фактори у коришћењу Dark Web-а су често испреплетени. Друштвена околина, online заједнице и економски притисци обликују изборе појединца, док психолошке потребе за анонимношћу, контролом, узбуђењем и припадношћу појачавају мотиве за укључивање у скривени интернет.

Друштвени фактори играју кључну улогу у обликовању понашања корисника Dark Web-а. Online заједнице и форуми делују као простори социјалног учења, у којима се криминалне технике, норме и вредности преносе са искуснијих на мање искусне чланове. Жеља за прихватањем и статусом унутар ових група може подстаћи појединце да се укључе у све ризичније активности. Истовремено, искуства друштвене искључености и отуђености у реалном животу повећавају вероватноћу тражења припадности у дигиталном подземљу.

Поред наведног анонимност доприноси феномену online деинхибиције, при чему појединци испољавају понашања која би у реалном окружењу избегавали. Смањени осећај одговорности и перципирана некажњивост олакшавају кршење закона и моралних норми. Спољни фактори, попут економских притисака и доступности алата за сајбер криминал, додатно снижавају праг уласка у ове активности. На крају, ограничене могућности органа за спровођење закона, услед децентрализоване природе Dark Web-а и употребе напредних

.

криптографских технологија, доприносе перципираном ниском ризику од откривања[1]. Овај фактор такође може нормализовати и продужити девијантно понашање корисника.

За разлику од друштвених фактора један од кључних психолошких мотива за коришћење Dark Web-а јесте потреба за анонимношћу и приватношћу. У условима масовне дигитализације, корисици Dark Web доживљавају као простор слободе, у којем могу учествовати у online активностима без страха од идентификације или санкција. Перципирана безбедност, заснована на енкрипцији и децентрализованој структури мреже, често доводи до повећаног осећаја контроле и смањене свести о потенцијалним ризицима.

Поред приватности, значајан мотив представља и приступ такозваном „забрањеном знању“. Dark Web омогућава доступност садржајима који су на површинском интернету цензурисани или правно ограничени, укључујући хакерске технике, илегална тржишта и екстремистичке идеологије. Овај феномен привлачи радознале појединце, али и оне који намерно трагају за знањем изван институционалних и друштвено прихваћених оквира, тако да забрањени карактер садржаја додатно појачава његову привлачност.

Један од најизраженијих аспеката Dark Web-а јесте могућност учешћа у забрањеним трансакцијама. Анонимна тржишта омогућавају куповину и продају илегалних добара и услуга, као што су наркотици, оружје, фалсификована документа, украдени подаци и хакерски алати. Употреба криптовалута додатно олакшава овакве трансакције, смањујући ризик од откривања. Потенцијална финансијска добит, у комбинацији са осећајем некажњивости, представља снажан мотивациони фактор за укључивање у ове активности.

За одређени број корисника, Dark Web представља и простор неконвенционалне забаве. Скривени форуми и затворене online заједнице окупљају појединце заинтересоване за екстремне садржаје, алтернативне идеологије и имерзивне дигиталне улоге[58]. Овакви садржаји могу задовољити потребу за узбуђењем, адреналином и бекством од

[58] Реч „имерзивно“ долази од енглеског *immersive* и значи потапајуће, урањајуће – нешто што корисника у потпуности увлачи у искуство. Имерзивне дигиталне улоге су улоге које корисници преузимају у дигиталном окружењу тако да се снажно „уживе“ у њих, као да су део виртуелног света или приче.

.

свакодневице, али истовремено могу довести до нормализације насиља и девијантних облика понашања.

Посебно значајан психолошки аспект коришћења Dark Web-a јесте осећај моћи и слободе. Појединци који се у реалном животу осећају маргинализовано или друштвено искључено могу у овом дигиталном простору пронаћи осећај контроле и самопотврђивања. Dark Web им омогућава да изразе ставове и понашања која би у стварном окружењу била санкционисана, чиме се задовољавају одређене психолошке потребе за аутономијом и припадношћу. Финансијска добит представља доминантан покретач бројних сајбер криминалних активности, укључујући онлајн преваре, крађу података и ransomware нападе[7]. Међутим, поједини актери делују из мотива личне или политичке освете, настојећи да наруше углед или функционисање одређених институција и држава. Dark Web се такође користи као платформа за сајбер шпијунажу и прикупљање обавештајних података, нарочито у контексту државно спонзорисаних напада и напредних дуготрајних претњи[59].

### 2.3. Типови корисника на Dark Web-u

Иако сам по себи није илегалан, легалност Dark Web-a зависи од начина коришћења и активности корисника. На њему се могу налазити легитимни ресурси, попут форума о приварности, истражвачких платформи или сајтова за слободно новинарство у земљама са репресивним режмом. Такође, може бити и простор где се обављају незаконите активности, као што су трговина наркотицима, оружјем или крађа података, и учествовање у таквим активностима представља кривично дело. Овакво окружење погодно је за испољавање специфичних образаца понашања, укључујући и маладаптивне црте личности описане у Алтернативном моделу поремећаја личности DSM-5[60], који обухвата пет основних домена:

[59] Gray, A. (2024). *The thrill-seekers of the digital underworld: A review of research into the psychological motivations of Dark Web users and cybercriminals*. Asia Pacific Institute of Information Technology (APIIT). (преузето 07.02.2026.) https://www.researchgate.net/publication/382742239_The_Thrill%E2%80%91Seekers_of_the_Digital_Underworld_A_Review_of_Research_into_the_Psychological_Motivations_of_Dark_Web_Users_and_Cybercriminals

[60] Алтернативни модел поремећаја личности (AMP) уведен је 2013. године од стране Америчке психијатријске асоцијације (APA), у петом издању „Дијагностичког и статистичког приручника за менталне поремећаје (DSM-5)

.

- негативни афект - склоност ка искуствовању негативних емоција као што су анксиозност, туга, љутња, осећај кривице,
- дистанцираност - избегавање људи, повлачење из друштвених интеракција, смањено уживање у позитивним емоцијама,
- антагонизам - онкурентност, манипулативност, супротстављање другима, склоност ка непријатељству,
- дезинхибиција - импулсивност, неопрезност, недостатак самоконтроле и
- психотицизам - необичне, ексцентричне или ирационалне мисли и понашања, склоност ка фантазији или параноидности.[61]

Dark Web не представља узрок маладаптивних црта личности, већ окружење које омогућава њихово јасније испољавање. Истраживања указују да популација корисника Dark Web-a није хомогена, те да различити типови корисника показују различите психолошке профиле и нивое ризика од девијантног понашања. Могу се извојити следеће и групе:

**1. Радознали и повремени корисници** чине групу код које се Dark Web користи епизодно, најчешће из знатижеље и без активног учешћа у заједницама или илегалним активностима. Код ових појединаца не уочава се стабилан образац маладаптивних црта личности, мада се у појединим случајевима може регистровати блага дезинхибиција у виду експериментисања и ризичног понашања, нарочито код млађих корисника[1]. Овакво понашање има контекстуални, а не патолошки карактер[62].

**2. Корисници усмерени на заштиту приватности и анонимности,** Dark Web користе као средство очувања личне и професионалне безбедности. У ову групу спадају новинари, активисти и појединци изложени политичкој или друштвеној репресији. Иако код њих може бити присутна извесна интерперсонална дистанца, она не представља маладаптивну црту, већ функционалну стратегију прилагођавања[2]. У оквиру DSM-5

[61] American Psychiatric Association. *Diagnostic and Statistical Manual of Mental Disorders, 5th Edition (DSM-5)*. American Psychiatric Publishing, 2013.
[62] Nightingale, S. et al. "Understanding User Behavior on the Dark Web." *Journal of Cybersecurity*, 2020.

.

модела, њихово понашање не показује клинички значајну повезаност са антагонизмом или дезинхибицијом[63].

**3. Информациони трагачи** користе Dark Web ради приступа цензурисаним или недоступним садржајима. Код ових корисника чешће се уочава домен дистанцираности, који се испољава кроз смањену потребу за социјалним интеракцијама и наглашену когнитивну аутономију. Иако ова црта сама по себи није патолошка, њено дуготрајно присуство може допринети социјалној изолацији[64].

**4. Чланови Dark Web форума и заједница** представљају психолошки комплекснију групу. Ове заједнице карактеришу високи нивои неповерења, строга правила понашања и наглашена улога репутације. Код појединих чланова уочавају се антагонистичке црте личности, као што су манипулативност, подозривост и непријатељски стил комуникације[4]. Идентитет се не гради на социјалној припадности, већ на инструменталној вредности и позицији унутар заједнице[65].

**5. Конзументи илегалног садржаја и услуга** показују израженије маладаптивне обрасце, пре свега у доменима дезинхибиције и антагонизма. Код њих су чести импулсивност, морална неутрализација и смањена емпатија, што омогућава рационализацију незаконитог понашања. Анонимност Dark Web-а значајно доприноси редукцији перципиране одговорности и повећава толеранцију према ризику.[66]

**6. Криминално активни корисници Dark Web-а**, укључујући сајбер криминалце и организаторе илегалних тржишта, показују највиши степен маладаптивних црта личности. Код њих доминирају антагонизам, дезинхибиција и психотицизам, уз изражену манипулативност, ниску емпатију и склоност ка „ризику/узбуђењу”[6]. Психотицизам се може испољити кроз параноидне интерпретације стварности, прецењивање сопствене контроле и искривљену перцепцију последица[67].

[63] Omer, T., “Privacy Activism and Dark Web Utilization.” *Information Security Journal*, 2019.
[64] Lee, A., & Chen, Y., “Cognitive Autonomy and Online Information Seeking.” *Cyberpsychology Review*, 2021.
[65] Johnson, M., “Community Dynamics in Dark Web Forums.” *Social Computing Journal*, 2022.
[66] Smith, R., & Kumar, P., “Illegal Content Consumption and Internet Behavior.” *Deviant Behavior*, 2018.
[67] Garcia, D., “Personality Traits of Cybercriminals.” *Psychological Reports*, 2019.

.

7. Посебну ризичну групу чине **корисници са постојећим психосоцијалним тешкоћама**, код којих доминира негативни афект, осећај усамљености и емоционална нестабилност. Dark Web у овом контексту може функционисати као механизам избегавања, али истовремено повећава ризик од даље изолације и проблематичне употребе интернета[68].

## 3. DARK WEB КАО ОКРУЖЕЊЕ ИЗВРШЕЊА КРИВИЧНИХ ДЕЛА

### 3.1. Категорије Dark Web сајтова

Dark Web није само једна врста веб-сајта, већ представља хетерогено дигитално окружење у оквиру анонимизационих мрежа. Реч је о комплексу различитих мрежа, платформи и сервиса, у којем коегзистирају легитимни, квазилегални и отворено криминални садржаји. Сајтови на Dark Web-у могу се систематизовати у неколико кључних категорија, на основу намене, структуре, типа активности и социјалне функције.[69] [70]

#### 3.1.1. Dark Web маркети (илегална и полуилегална тржишта)

Dark Web маркети су најпознатији и најистраживанији тип Dark Web сајтова. Они функционишу по моделу класичних e-commerce платформи, али у условима потпуне или високе анонимности. Корисници приступају овим сајтовима путем Tor мреже, док се плаћања врше искључиво криптовалутама, најчешће Bitcoin-ом или Monero-ом. Основне карактеристике ових сајтова је постојање система корисничких налога са псеудонимима, систем оцене и рецензије продаваца, механизме посредничког чувања новца тзв. escrow, као и енкриптована комуникација између купца и продавца. Dark web тржишта обухватају широк спектар понуде добара и услуга, као што су:

[68] Brown, L. & Davis, S., "Psychosocial Difficulties and Internet Use." *Journal of Behavioral Addictions*, 2021.
[69] CyberArrow. (n.d.). *Types of dark web*. (преузето 8.01.2026.), https://www.cyberarrow.io/blog/types-of-dark-web/?utm_source=chatgpt.com
[70] Norton. (n.d.). *Dark web websites*. (преузето 8.01.2026.), https://us.norton.com/blog/digital-life/dark-web-websites?utm_source=chatgpt.com

.

- **Украдени подаци и дигитални идентитети**

Обухватају украдене податке о клијентима, бројеве кредитних картица, податке за пријаву на налоге (email, друштвене мреже, финансијске платформе), комплетне пакете личних података (*Personally Identifying Information – PII*), бројеве социјалног осигурања и сличне идентификационе податке. Ови подаци се често користе за крађу идентитета и финансијске преваре.

- **Фалсификати и кривотворине**

На овим тржиштима се могу наћи: фалсификовани лични документи, лажни сертификати и дипломе, кривотворена роба познатих брендова, као и лажни новац и финансијски инструменти, што директно подрива правне, образовне и економске системе.

- **Пословне тајне и поверљиве информације**

Ова категорија обухтвата украдене корпоративне податке, интерне документације компанија, индустријске и технолошке тајне, а често је повезана и са индустријском шпијунажом и сајбер-нападима на велике организације.

- **Нелегалан и експлоатативан садржај**

Један од најтежих и најпроблематичнијих аспеката Dark Web маркета јесте присуство илегалног порнографског материјала, укључујући садржаје који представљају тешка кривична дела, попут секусалне експлоатације деце.

- **Malware, хакерске услуге и сајбер-оружје**

Dark Web тржишта служе и као платформе за продају злонамерног софтвера (malware), ransomware алата, услуга хаковања, DDoS напада по наруџбини, exploit комплета и других сајбер-оружја. Ова понуда представља основу модерног сајбер криминала и омогућава развој модела *Cybercrime-as-a-Service* и снижава праг уласка у сајбер криминал, односно омугућава улазак у криминалне активности чак и технички мање вештим појединцима.

.

- **Насилне и екстремне услуге**

Иако су често преварантског карактера, на darkweb маркетима су се појављивали огласи за наводне „услуге плаћених убица“ и друге облике тешког криминала, што додатно доприноси перцепцији Dark Web-а као високоризичног окружења

- **Дроге и фармацеутски производи**

Ово је једна од најзаступљенијих категорија и обухвата: илегалне наркотике, психоактивне супстанце, лекове без рецепта и фалсификоване фармацеутске производе. Dark Web marketи су значајно утицали на трансформацију глобалне трговине дрогом, премештајући је у дигитални простор.

- **Књиге, образовни материјали и алати за приватност**

Поред илегалних садржаја, поједини маркети нуде: образовне и техничке материјале, туторијале и алате за приватност и дигиталну безбедност. Ова понуда показује да Dark Web тржишта нису искључиво једнодимензионално криминална, већ понекад укључују и легалне или неутралне ресурсе.

Dark Web тржишта су изузетно нестабилна, често имају кратак „животни век“ због полицијских интервенција, интернационалних истрага или унутрашњих тзв. *exit scam* превара, где администратори нестају са средствима корисника. Адресе се често мењају, а читави маркети нестају преко ноћи. Иако постоје директоријуми који помажу у проналажењу Dark Web сајтова, њихова поузданост је ограничена, а ризици значајни. Најпознатији примери Dark Web тржишта су:  Silk Road, AlphaBay, Dream Market, Hansa Market, Hydra, Agora, Archetyp, Atlantis, Black Market reloaded, Evolution, Sheep Marketplace, The Farmer`s Market, TheRealDeal, Utpoia, White Housse Market, сви тренутно непостојећи и угашени.

### 3.1.2. Хакерски и cyber-crime сајтови

Ова категорија обухвата сајтове и форуме који су фокусирани на сајбер криминал као услугу (*Crime-as-a-Service*), који подразумева комерцијализацију сајбер криминалних

.

активности и њихово нуђење као готових производа или услуга крајњим корисницима. За разлику од класичних Dark Web маркета који су често оријентисани ка масовној продаји илегалне робе, хакерски форуми су јасно сегментисани, технички специјализовани и намењени корисницима са одређеним нивоом знања и искуства. Основна функција ових платформи обухвата продају и размену различитих врста злонамерног софтвера (malware), exploit алата, ransomware пакета, као и услуга извођења DDoS напада по наруџбини, трговина украденим корисничким налозима, приступима корпоративним системима (RDP, VPN), компромитованим серверима, као и базама података са осетљивим информацијама.

Често су организовани као затворени форуми, где је приступ могућ само путем позива, препоруке постојећих чланова или након процеса верификације који може укључивати доказивање техничких вештина, претходних „успешних послова“ или финансијског улога, што указује на висок ниво унутрашње контроле и неповерења према новим члановима. Поред криминалних трансакција, хакерски и cyber-crime форуми служе и као центри знања и обуке. На њима се одвијају техничке дискусије о рањивостима софтвера, новим техникама заобилажења безбедносних механизама, методама анонимизације, као и анализе актуелних сајбер напада. Туторијали и водичи могу бити намењени почетницима, али и напредним корисницима, чиме се омогућава континуирана репродукција и ширење сајбер криминалних вештина.

### 3.1.3. Leak и data-dump сајтови

Leak сајтови служе чија је примарна функција јавна објава украдених, компромитованих или неовлашћено прибављених података. За разлику од Dark Web маркета, где се подаци продају као роба, ови сајтови служе као простор за њихово јавно излагање, чиме се штета за појединце, организације и институције значајно увећава.

Најчешћи типови података који се објављују су лични подаци грађана (име, адреса, контакт информације, бројеви докумената), базе података компанија, дипломатски и државни документи и интерни корпоративни фајлови, као и дипломатске и државне документе. У појединим случајевима, објављени материјал садржи осетљиве информације од значаја за националну безбедност, што овим сајтовима даје и јаку политичку димензију. Мотиви за објављивање ових информација могу бити различите природе од

.

финансијске уцене, преко идеолошког активизма, до чистог злонамерног излагања личних података (doxxing). Ови сајтови су често повезани са ransomware групама, које користе објављивање података као средство такозване двоструке или вишеструке уцене (double или triple extortion). У овом моделу, жртве се не суочавају само са губитком приступа својим подацима, већ и са претњом њиховог јавног објављивања, чиме се притисак значајно интензивира и проширује на клијенте, партнере и ширу јавност. Са социолошког аспекта, они представљају облик дигиталне моћи и контроле путем информација.

### 3.1.4. Форуми и online заједнице

Dark Web форуми и онлајн представљају социјалну и интеракциону димензију Dark Web екосистема. За разлику од тржишта и техничких платформи, ови простори служе као места комуникације, размене знања, формирања идентитета и изградње неформалних друштвених структура у условима анонимности. Њихов садржај и намена могу бити криминалног, политичког, идеолошког, активистичког или искључиво техничког карактера.

Типолошки, Dark Web форуми могу се поделити на више подкатегорија. Форуми усмерени на приватност и криптографију баве се темама дигиталне анонимности, енкрипције, безбедне комуникације и заштите од надзора, често уз размену техничких савета и алата. Криминалне дискусионе заједнице функционишу као места размене искустава, техника и ресурса међу актерима сајбер криминала, укључујући финансијске преваре, хаковање и трговину илегалним добрима. Поред њих, присутни су и форуми екстремистичких и радикалних група, који служе за идеолошку индоктринацију, ширење пропаганде и мобилизацију присталица, као и политички активистички простори, нарочито у контексту ауторитарних режима где је слобода говора ограничена.

Идентитети корисника на Dark Web форумима су флуидни, нестабилни и краткотрајни**,** најчешће засновани на псеудонимима који се лако напуштају и мењају, где се репутација се формира искључиво кроз активност, техничку компетентност и корисност за заједницу. Поверење је минимално и увек условно, што резултира културом сталне сумње и опреза.Ови форуми често функционишу као центри социјализације, учења и регрутовања, посебно за нове чланове који постепено усвајају норме, језик и вредности

.

заједнице. Процес регрутовања је обично неформалан, али ефикасан, заснован на доказивању знања, лојалности и спремности на сарадњу. На тај начин, Dark Web форуми играју кључну улогу у одржавању и репродукцији криминалних, идеолошких и активистичких мрежа и представљају алтернативне јавне сфере које функционишу ван домета традиционалних институција надзора и контроле.

### 3.1.5. Dark Web претраживачи и директоријуми

Због специфичне техничке архитектуре Dark Web-а и употребе анонимизационих мрежа, класични интернет претраживачи не индексирају .onion домене нити омогућавају приступ садржајима који се налазе ван Surface Web-а. Из тог разлога развијени су специјализовани Dark Web претраживачи и директоријуми**,** који служе као основни навигациони механизми у овом затвореном дигиталном окружењу. Најпознатији примери укључују The Hidden Wiki, Ahmia и NotEvil, који функционишу као комбинација претраживача, каталога и референтних листа Dark Web ресурса. Ови сервиси имају улогу индексирања .onion сајтова, њихове основне категоризације, као и пружања основне оријентације у мрежи. За разлику од површинских претраживача, Dark Web претраживачи имају ограничен домет и капацитет индексирања, што је последица честих промена адреса, кратког животног века сајтова и намерног избегавања видљивости од стране администратора илегалних платформи. Као резултат тога, садржаји које ови сервиси приказују често су непотпуни, застарели или нетачни. Ови сервиси су често нестабилни, непотпуни и подложни злоупотребама, али су кључни за функционалност Dark Web-а као екосистема.

### 3.1.6. Платформе за узбуњиваче (Whistleblower platforms)

Иако се Dark Web често повезује са криминалом, значајан број сајтова има потпуно легитимну и друштвено корисну сврху. Платформе за узбуњиваче (whistleblower platforms) показују да Dark Web представља и алтернативну инфраструктуру приватности**,** која омогућава безбедан и анониман приступ информацијама и комуникацију у условима високог ризика. Ове платформе омогућавају узбуњивачима да без страха од откривања идентитета деле поверљиве или компромитоване документе са новинарима, истражним тимовима и организацијама које се баве јавним интересом. Најпознатији пример је

.

SecureDrop[71], који користи Tor мрежу како би обезбедио потпуну анонимност пошиљаоца, као и сигурну доставу података редакцијама и невладиним организацијама. Кроз ову платформу, корисници могу слати документе, белешке и друге врсте информација без могућности праћења или компромитовања њихове приватности. Ове платформе користе и реномирани медији, укључујући The Guardian, ProPublica и The New York Times, чиме се обезбеђује континуитет истраживачког новинарства у контекстима где би класични канали комуникације били ризични или неприкладни. Поред новинарских организација, платформе за узбуњиваче пружају и могућност анонимне комуникације и размене порука, као и приватне претраге, што значајно доприноси заштити слободе говора и приступа информацијама у ауторитарним или репресивним срединама.

### 3.1.7. Крипто услуге и „mixери“

Криптовалуте представљају кључни елемент финансијских трансакција на Dark Web-у, обезбеђујући брзе, дигитално-сигурне и релативно анонимне механизме плаћања. Најчешће коришћене валуте укључују Bitcoin, због његове распрострањености, као и Monero и Zcash, који пружају виши ниво приватности и практично скривање података о пошиљаоцу и примаоцу трансакције[72].

Један од кључних изазова за кориснике Dark Web-а је сакривање историје трансакција и обезбеђивање анонимности финансијских токова. За ову сврху користе се такозвани „mixери“ *(tumbling сервиси),* који раздвајају и мешају криптовалуте корисника са валутама других учесника система, чиме се нарушава директна веза између пошиљаоца и примаоца. Ови сервиси омогућавају да се трансакције на блокчејну чине нечитљивим или тешко праћењим, што је критично за учеснике у илегалним трговинама, али и за легитимне кориснике који желе додатну приватност.

Поред mixera, неки сервиси нуде додатне функционалности, као што су: Escrow услуге, где платни износ остаје депонован код посредника све док обе стране не потврде трансакцију, што обезбеђује већу сигурност у трговини илегалним или ризичним добрима;

[71] SecureDrop. (n.d.). *About SecureDrop*. ( преузето 19.02.2026.), https://securedrop.org
[72] Zola, F., et al. (n.d.). *Topological analysis of mixer activities*. arXiv. (преузето 20.02.2026.) https://arxiv.org/abs/2504.11924

.

Peer-to-peer (P2P) размена и замена криптовалута, која омогућава директну трговину између корисника без посредника; Децентрализоване финансијске платформе (*DeFi)*, које се све више користе за анонимно управљање средствима и кредитне/залог трансакције унутар Dark Web-a.

### 3.2. Настанак и еволуција Dark Web маркета

Dark Web маркети постали су важан фактор у савременој глобалној трговини, омогућавајући приступ широком спектру различитих производа и услуга, најчешће илегалних. Током година они су се развили у алтернативне канале трговинске размене који комбинују технолошке иновације, висок степен анонимности и изразито транснационални карактер. Од свог настанка, у последњих петнаестак година, ови маркети прошли су кроз више развојних фаза – од експерименталних платформи ограниченог домета до глобалног, фрагментираног и изузетно адаптабилног екосистема.

Два предуслова била су кључна за настанак првих Dark Web тржишта:

**1. Анонимна инфраструктура** – Развој анонимне мреже Tor (The Onion Router), која је постала јавно доступна почетком 2000-их година, омогућио је стварање дигиталног простора у коме је идентитет учесника релативно заштићен. Tor функционише тако што усмерава интернет саобраћај кроз више слојева енкрипције и различите чворове у мрежи, чиме се прикрива IP адреса корисника. Поред анонимног приступа, Tor омогућава и хостовање „.onion“ сајтова, односно скривених сервиса који нису доступни преко класичних претраживача и стандардног веба[73].

**2. Децентрализована валута** – Појава криптовалуте Bitcoin 2009. године представљала је други кључни елемент. Заснован на блокчејн технологији, Bitcoin омогућава директне трансакције између корисника без посредовања банака или других финансијских институција[74]. Иако трансакције нису потпуно анонимне већ псеудонимне, у комбинацији са Tor мрежом омогућиле су довољан степен приватности да се развију онлајн тржишта изван регуларних институционалних оквира.

[73] Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The Second-Generation Onion Router.* Proceedings of the 13th USENIX Security Symposium.
[74] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

.

Комбинација анонимне комуникационе инфраструктуре и децентрализованог система плаћања створила је техничке и функционалне услове за настанак првих Dark Web маркета, који су убрзо почели да функционишу по моделу легалних e-commerce платформи, али у оквиру скривеног и слабо регулисаног дигиталног простора.

### 3.2.1. Прва генерација – појава Silk Road (2011–2013)

Први велики Dark Web маркет био је Silk Road, покренут у фебруару 2011. године, чији је развој започео шест месеци раније. Оснивач, Ross Ulbricht, користио је псеудоним *Dread Pirate Roberts*, инспирисан измишљеним ликом из филма Принцеза невеста. Улбрихт је имао визију анонимне, либертаријанске трговине, где корисници могу слободно да тргују робом и услугама ван контроле државе[75]. Назив платформе „Silk Road“ потиче од историјске мреже трговачких путева започетих током династије Хан (206. п. н. е. – 220. н. е.), која је повезивала Европу, Индију, Кину и друге делове Афро-Евроазије.[76]

Silk Road је функционисао као e-commerce платформа слична Amazon-у или eBay-у, али у потпуно анонимном окружењу Tor мреже и уз плаћања искључиво у криптовалути Bitcoin. Главне иновације платформе укључивале су систем оцена и рецензија продаваца, escrow механизам за заштиту купаца[77], строго организовану понуду производа и ограничење одређених врста робе. Највећи део понуде чиниле су дроге, чак 70%, које су биле подељене у категорије: стимуланси, психоделици, лекови на рецепт, прекурсори, опиоиди, екстази, дисоцијативи, стероиди и ПЕД-ови. Унутар категорије стимуланси, налазили су се кокаин, амфетамини и метамфетамини, који су чинили приближно 20% укупне понуде и били су најпопуларнији међу корисницима из Сједињених Држава и Европе. Психоделици, као што су LSD, псилоцибинове печурке и DMT, чинили су око 10% понуде и били су посебно атрактивни младој популацији корисника глобално. Лекови на рецепт, попут опиоида (оксикодон), бензодиазепина и стимуланаса за ADHD, заузимали су око 15% понуде и често су се користили у рекреативне, али и медицинске

[75] Greenberg, A. (2013, April 29). *Collected Quotations of the Dread Pirate Roberts, Founder of the Underground Drug Site Silk Road and Radical Libertarian.* Forbes.
[76] Martin, J. (2014). *Lost on the Silk Road: Online drug distribution and the "cryptomarket".* Criminology & Criminal Justice, 14(3), 351–367
[77] **Escrow механизам** је сигуран начин плаћања где трећа страна привремено задржава средства док се уговорени услвои трансакције не испуне, односно средства су задржавана на рачуну платформе док купац не потврди пријем наруџбине, смањујући ризик од преваре.

.

сврхе. Silk Road је такође продавао прекурсоре и хемикалије, потребне за синтезу других супстанци, који су чинили око 5% укупне понуде и били су намењени искључиво искусним продавцима који сами припремају дроге. Екстази и дисоцијативи, као што су MDMA и кетамин, заузимали су око 10% понуде, док су стероиди и лекови за побољшање перфоманишти (PED - Performance Enhancing Drugs) за бодибилдере чинили око 5%. Продавци су добијали упутства о вакуумском запечаћивању робе како би избегли откривање од стране поште или царине.

Поред наркотика, Silk Road је нудио и фалсификоване документе, попут лажних возачких дозвола и пасоша, који су чинили око 2–3% понуде. Остала нелегална роба, укључујући порнографију и оружје (које се продавало на сестринском сајту *The Armoury*), чинила је око 5% понуде, док је легална роба као што су одећа, књиге, накит, порнографски материјал и софтвер заузимала око 5%. Такође су се на платформи нудиле и дигиталне услуге, као што су писање или дизајн, али су чиниле мањи удео, око 1–2%[78][79].

Silk Road је био један од ретких Dark Web маркета који је имао јасно дефинисане услове коришћења, чији је циљ био да тржиште буде „безбедно“, односно дозвољавали су продају робе која је релативно безбедна и која није директно штетна по друге људе, а забрањивали све што би могло да нанесе физичку, правну или финансијску штету. У оквиру забрањених активности и робе били су: продаја дечје порнографија, Атентати, претње и насиље, оружје и експлозиви (осим на посебним сестринским сајтовима), украдене кредитне картице и банкарски подаци, као и остала роба која може нанети штету људима или финансијске преваре.

Silk Road је веома брзо постао популаран. Чланак Gawker-a из јуна 2011. године повећао је видљивост платформе и број корисника[80]. Током рада платформе, било је више од 3.800 продаваца и преко 100.000 купаца. Током 2,5 година, на сајту је обављено приближно 1.229.465 трансакција укупне вредности око 9,5 милиона Bitcoin-a, што је у то

[78] Martin, J. (2014). *Lost on the Silk Road: Online drug distribution and the "cryptomarket".* Criminology & Criminal Justice, 14(3), 351–367. https://doi.org/10.1177/1748895813505234
[79] UNODC. (2020). *World Drug Report 2020 – Booklet 4: Drugs and the darknet.* United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/data-and-analysis/wdr2020.html
[80] Gawker. (2011, October 17). *The underground website where you can buy any drug imaginable*. https://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

.

време износило око 1,2 милијарде долара, а провизије платформе биле су око 614.000 Bitcoin-a[81]. Корисници су долазили са различитих континената: 30% из Сједињених Држава, 27% непријављено, а остали из Велике Британије, Аустралије, Немачке, Канаде, Шведске, Француске, Русије, Италије и Холандије[7].

Технички, Silk Road је користио Tor мрежу за анонимност и Bitcoin као валуту са escrow механизмом, уз могућност фиксирања вредности трансакција у доларима да би се ублажила волатилност Bitcoin-a[8]. Платформа је имала и систем приватних порука (од 24. маја до 23. јула 2013. године послато је преко 1,2 милиона порука), аутоматизовани систем рецензија и оцене, који је одржавао поверење купаца и продаваца. У мају 2013. године платформа је кратко обустављена због DDoS напада[7].

Платформа Silk Road је угашена 2. октобра 2013. године након вишегодишње истраге коју је предводио Federal Bureau of Investigation (FBI), у сарадњи са другим америчким и међународним агенцијама. Кључни моменат у истрази било је повезивање раних интернет објава о Silk Road-у са личним дигиталним идентитетом оснивача, Ross Ulbricht-a[2], на тај начин што су истражитељи наводно идентификовали адресу електронске поште која је коришћена у раној промоцији сајта.[82]

Гашење Silk Road-а није довело до нестанка Dark Web маркета. Напротив, убрзо су се појавили „наследници“ као што су Silk Road 2.0, AlphaBay и Hansa, који су преузели исти модел функционисања, анонимност путем Tor мреже, плаћање у Bitcoin-у, escrow механизам и систем рецензија, који су постали стандард за све наредне генерације darknet маркета. Она је поставила темеље модерног Dark Web екосистема, демонстрирајући да је могуће организовати глобалну анонимну економију у којој су трансакције релативно сигурне, структурисане и вођене механизмима саморегулације, без директног надзора државних институција. Управо та комбинација технолошке анонимности и тржишних механизама постала је образац који ће касније платформе даље развијати и усавршавати.

[81] Christin, N. (2013), op. cit.

[82] Хапшење Роса Улбрихта извршено је 2. октобра 2013. године у јавној библиотеци у Сан Франциску. Судски поступак против Улбрихта вођен је пред Окружним судом Сједињених Држава за јужни дистрикт Њујорка (*United States v. Ross Ulbricht*). Током 2015. године проглашен је кривим по више тачака оптужнице, укључујући дистрибуцију наркотика, прање новца и компјутерску хакерску заверу[2]. Осуђен је на доживотну казну затвора без могућности условног отпуста

.

### 3.2.2.Silk Road 2.0 (2013-2014)

Након гашења оригиналног Silk Road у октобру 2013. године, већ 6. новембра исте године бивши сарадници и администратори су поново покренули платформу под истим именом Silk Road, додајући ознаку „2.0“, са циљем да очувају кориничку базу и наставе модел анонимне онлајн трговине засноване на криптовалутама. Нови псеудонимни администратор користио је исто име „*Dread Pirate Roberts*“, настојећи да симболички настави традицију оригиналног сајта. Као додатну меру безбедности, дистрибуиране су шифроване копије изворног кода платформе како би се омогућило брзо поновно покретање у случају уклањања са сервера приликом нове полицијске интервенције, што је представљало важну стратешку меру у Dark Web окружењу[83].

Као и претходна верзија, Silk Road 2.0 је функционисао преко Tor мреже, што је омогућавало прикривање идентитета корисника и локације сервера. Плаћања су се вршила у Bitcoin-у, а примењиван је и escrow механизам, као и систем рецензија и оцена продаваца доприносио је стварању поверења међу корисницима.

Ипак, платформа се убрзо суочила са озбиљним изазовима. Крајем 2013. године ухапшено је више лица повезаних са администрацијом, што је довело до привремене нестабилности у управљању сајтом, а фебруара 2014. године Silk Road 2.0 је претрпео велики хакерски напад. Искористивши рањивост познату као „transaction malleability“, нападачи су успели да преусмере значајну количину средстава из escrow система. Украдено је око 4.400 биткоина, што је тада представљало милионски износ у америчким доларима. Иако је администрација покушала да надокнади губитке корисницима користећи сопствене провизије од продаје, поверење у платформу било је озбиљно нарушено[84].

Коначно, у новембру 2014. године, у оквиру међународне полицијске акције под називом Operation Onymous, сајт је угашен. Акцију су координисали Federal Bureau of

[83] Greenberg, A. (2013, November 6). *Silk Road 2.0 Launches, Promising a Resurrected Black Market for the Dark Web.* Forbes.(преузето 21.02.2026) www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web

[84] Wired. (2014, February 28). Bitcoin 'transaction malleability' exploit hits Silk Road 2.0 escrow accounts. (преузето 21.02.2026) https://www.wired.com/2014/02/bitcoin-transaction-malleability-silk-road-2

.

Investigation и Europol, уз учешће више европских служби. Том приликом ухапшен је Blake Benthall, који је наводно управљао платформом под псеудонимом „*Defcon*“. Истовремено је процесуиран и британски програмер Thomas White, повезан са радом обновљене верзије сајта[85].

Иако је Silk Road 2.0 трајао релативно кратко, од новембра 2013. до новембра 2014. године, његов значај у историји darknet трговине је велики. Он је показао да модел анонимних криптомаркета није везан за једног појединца, већ да се може релативно лако реплицирати захваљујући технологијама које омогућавају анонимност и децентрализовано плаћање.

### 3.2.3.AlphaBay (2015-2017)

AlphaBay био је једно од највећих и најзначајнијих Dark Web тржишта у историји. Платформа је први пут најављена у септембру 2014. године, а званично је почела са радом 22. децембра 2014. године. Оснивач и администратор био је канадски држављанин Alexandre Cazes, познат под псеудонимом „Alpha02“.

Током периода функционисања, AlphaBay је надмашио свог претходника, Silk Road, како по броју корисника тако и по обиму понуде. Према подацима објављеним након међународне истраге, у тренутку гашења 2017. године платформа је имала више од 400.000 корисника и преко 40.000 активних продаваца, са стотинама хиљада огласа. Процењено је да је укупан промет платформе премашио више стотина милиона америчких долара.

AlphaBay је функционисао као анонимно тржиште доступно путем Tor мреже, што је омогућавало прикривање IP адреса и идентитета корисника. Плаћања су се вршила криптовалутама, пре свега Bitcoin-ом, а касније су уведени и Monero и Ethereum, при чему је Monero временом постао посебно популаран због већег степена анонимности трансакција. Једна од кључних карактеристика платформе био је њен escrow систем који је

[85] Europol, & U.S. Department of Justice. (2014, November 6). *Operation Onymous: Silk Road 2.0 shutdown press releases*. (преузето 28.02.2026.) https://www.europol.europa.eu/newsroom/news/operation-onymous-silk-road-20-shutdown

.

подразумевао задржавање средства купца након обављене куповине на посредничком (escrow) рачуну под контролом платформе све до испоруке и потврде пријема производа. Тек након верификације испоруке средства су пребацивана продавцу. Овај механизам је имао за циљ да смањи ризик од преваре и повећа поверење између страна у трансакцији. Ипак, постојала је и опција „finalize early“ (рани завршетак трансакције), која је носила већи ризик за купце и често је коришћена код продаваца са високим рејтингом.

Поред escrow система, AlphaBay је имплементирао више безбедносних механизама:

- **Шифрована комуникација** – поруке између купаца и продаваца биле су PGP-шифроване, што је спречавало треће стране да пресретну и читају садржај комуникације.
- **Двофакторска аутентификација (2FA)** – додатни ниво заштите налога, који је значајно отежавао неовлашћени приступ.
- **Multisignature (вишеструки потпис)** – код одређених трансакција било је потребно одобрење више страна за ослобађање средстава, чиме се додатно смањивао ризик од злоупотребе.

Платформа је имала релативно строга интерна правила. Продавци који нису испуњавали поруџбине, кршили правила или добијали велики број негативних оцена могли су бити санкционисани, суспендовани или трајно уклоњени са тржишта. Систем репутације, заснован на оценама и коментарима купаца, играо је кључну улогу у одржавању поверења и тржишне динамике. Интерфејс AlphaBay-а био је дизајниран по узору на легалне платформе електронске трговине. Сајт је садржао:

- детаљне листинге производа са описима, ценама и фотографијама,
- систем оцена и рецензија продаваца,
- категорије и поткатегорије производа,
- систем корпе за куповину,
- падајуће меније и филтере за претрагу.

Овај степен функционалности и корисничке приступачности допринео је масовности платформе и њеној професионализацији. AlphaBay је у том смислу

.

представљао еволутивни корак у односу на раније Dark Web маркете, комбинујући технолошку софистицираност, механизме поверења и висок степен анонимности.

Платформа је угашена у јулу 2017. године у оквиру међународне полицијске операције „Operation Bayonet“, координисане од стране америчких, канадских и тајландских власти. Хапшење администратора и заплена серверске инфраструктуре означили су крај једног од највећих darknet тржишта, али и показали да, упркос високом нивоу анонимности, потпуна недодирљивост у дигиталном простору није могућа[86].

У понуди платформе AlphaBay налазио се изузетно широк спектар нелегалних производа и услуга. Према емпиријском истраживању које су спровели Levi Baravalle и Christine Lee (2018)[87], а које је засновано на анализи великих узорака огласа прикупљених применом технике веб-скрепинга („spider web“ метода), тржиште је било структурисано у 12 главних категорија робе и услуга**.**

Највећу категорију чинила је „Drugs & Chemicals“ (Дрога и хемикалије), која је према процени вредности трансакција обухватала приближно 85–87% укупне економске вредности тржишта. Иако је у појединим анализама, заснованим на броју огласа, њен удео био нижи (око 40–50%), подаци о финансијском обиму показују да су наркотичке супстанце представљале убедљиво доминантан економски ресурс платформе. Ова категорија обухватала је канабис, кокаин, хероин, MDMA, LSD, синтетичке психоактивне супстанце, као и лекове на рецепт и различите хемијске прекурсоре.

Друга категорија по економској вредности била је „Weapons“ (Оружје), са приближно 4–5% укупне процењене вредности**,** иако је по броју огласа чинила мањи проценат. Она је обухватала ватрено оружје, муницију и делове оружја. Ови подаци указују на несразмеру између медијске перцепције и стварног удела оружја у структури тржишта.

---

[86] NordStellar, „AlphaBay – Историја највећег Darknet тржишта“, *NordStellar Blog*, (преузето 15. 02.2026).https://nordstellar.com/blog/alphabay/

[87] Baravalle, A., & Lee, S. W. (2018). *Dark web markets: Turning the lights on AlphaBay*. In *Web Information Systems Engineering – WISE 2018: 19th International Conference, Dubai, United Arab Emirates, November 12–15, 2018, Proceedings, Part II* (pp. 502–514). Springer. (преузето 16.02.2026.) https://doi.org/10.1007/978-3-030-02925-8_35

.

Категорија „Fraud“ (Превара) чинила је око 2% укупне економске вредности, али је по броју огласа била значајнија. Обухватала је украдене податке са платних картица (carding), банковне рачуне, лажне идентитете и услуге финансијских превара. Слично томе, категорија „Carded items“ (посебно издвојена у анализи) односила се на продају украдених финансијских података. Категорија „Counterfeit items“ (Фалсификована роба и документи) обухватала је лажне пасоше, личне карте, возачке дозволе, дипломе, али и реплике брендова и луксузне производе, са уделом од приближно 2% у укупној процењеној вредности. „Digital Products“ (Дигитална добра) и „Software & Malware“ (Софтвер и малвер) заједно су чинили око 1–2% укупне вредности. Ове категорије укључивале су украдене налоге (PayPal, Netflix, Steam), базе података, дигиталне кључеве, приступе серверима, ransomware, spyware, DDoS услуге и ботнете. Иако релативно мањег финансијског обима у односу на трговину наркотицима, ове категорије су биле значајне у контексту сајбер-криминала. Категорија „Services“ (Услуге) обухватала је различите „криминалне услуге“, укључујући програмерске, техничке и логистичке услуге, док су „Guides & Tutorials“ (Водичи и туторијали) садржали упутства за извођење различитих облика незаконитих активности. Категорије „Jewels & Gold“ (Накит и злато), „Security & Hosting“, као и „Other“ (Остало) имале су мањи удео у укупној структури тржишта, али њихова апсолутна вредност није била занемарљива.

Географска анализа показала је да су Сједињене Државе убедљиво водеће по броју огласа, са више него двоструко већим бројем у односу на Уједињено Краљевство. Већина водећих земаља припада економски развијеним државама, што указује на повезаност дигиталне инфраструктуре, куповне моћи и учешћа у Dark Web економији. САД показују високу диверзификацију понуде, при чему 74% огласа чине наркотичке супстанце, а значајан удео имају и накит, фалсификати, услуге и оружје. Унутар категорије наркотика, канабис и хашиш чине око 29%, након чега следе психоделичне супстанце.

Уједињено Краљевство и Немачка показују сличан образац, са доминацијом канабиса и значајним уделом стимуланса и психоделичних супстанци. Насупрот томе, Авганистан представља специфичан случај, јер већина огласа не обухвата наркотике, већ фалсификована документа и дигиталне производе. Индија је идентификована као главни продавац кетамина, који унутар индијског тржишта чини чак 96% понуде, што указује на

.

снажан производни капацитет. Јапан се издваја као тржиште фокусирано на дигиталне производе и онлајн услуге, са минималним уделом наркотика.

Свеукупно посматрано, анализа структуре понуде на платформи AlphaBay показује да је тржиште функционисало превасходно као глобална платформа за трговину наркотицима, док су остале категорије – нарочито оне које се односе на финансијске преваре и сајбер-криминал – представљале секундарне, али структурно важне сегменте. Овај налаз указује да AlphaBay није био искључиво тржиште илегалних физичких производа, већ комплексни дигитални екосистем који је омогућавао трансакцију како материјалних добара, тако и услуга и дигиталних алата, чиме је проширивао домен криминалне економије у виртуелном простору.

### 3.2.4. AlphaBay 2.0 (2021-2023)

Након затварања оригиналног AlphaBay-а 2017. године, сајт се поново појавио у августу 2021. године под контролом једног од оригиналних администратора (*DeSnake*). AlphaBay 2.0 је био познат не само по повратку, већ и по строжим правилима тржишта. DeSnake је увео експлицитна ограничења на продају посебно ризичних производа, укључујући: Covid-19 вакцине**,** фентанил и оружје.

Иако је ново тржиште функционисало по истом принципу као и оригинално, користећи Tor и I2P мреже за анонимност, а као искључиво средство плаћања уведена је криптовалута Monero. Додатно је имплементиран систем за самоодбрану „AlphaGuard“ који је био дизајниран да спречи инфилтрацију полицијских органа и заштити средства корисника. Кључни аспекти AlphaGuarda укључивали су: Механизам самоуништења који је подразумевао да су сервери и средства могли су аутоматски бити уништени ако се детектују неочекиване промене у инфраструктури и административни Прекид је подрезумевао да су само корисници са административним приступом, попут DeSnake-а, могли онемогућити AlphaGuard уношењем сигурносног кључа у року од 72 сата од активирања догађаја.

Ипак, платформа је била нестабилна, корисници су пријављивали техничке проблеме и сумњали у легитимност поновног покретања. До почетка 2023. године сајт је

.

практично угашен, чиме је окончан сваки значајнији покушај његовог поновног функционисања. Упркос напредним заштитама, AlphaBay 2.0 је имао ограничен животни век. Према више извора, 2023. године AlphaGuard је активиран, покрећући гашење платформе. Из непознатих разлога, DeSnake није успео да унесе административни кључ у року од 72 сата, што је довело до неповратног затварања тржишта.[88]

### 3.2.5. Hansa Market (2015-2017)

Hansa Market представља једно од најзначајнијих даркнет тржишта у периоду након гашења платформе Silk Road и пре затварања AlphaBay-a. Његов развој, организациона структура и начин гашења пружају значајан увид у еволуцију дигиталног криминала, али и у промену стратегија органа за спровођење закона у борби против транснационалног сајбер криминала.

Hansa Market покренут је средином 2015. године, у периоду реорганизације даркнет тржишта након затварања Silk Road-a. Платформа је у релативно кратком временском периоду стекла репутацију стабилног и релативно безбедног тржишта, са нагласком на професионализацију администрације и техничку сигурност. За разлику од ранијих тржишта која су се ослањала на појединачне администраторе са ограниченим техничким знањем, Hansa Market је показивао знаке сложеније организационе структуре. Њиме су управљала најмање два администратора, држављани Немачке, са напредним знањем из области информационих технологија и безбедоносних система. Они су имплементирали: escrow систем, симстем репутације продаваца, двофакторску аутентификацију, PGP енкрицију комуникације, редовно ажурирање безбедосносних протокола, мере заштите од DDoS напада. Платформа је функционисала преко Tor мреже, чиме је омогућена анонимност корисника и скривање локације сервера. Инфраструктура је била дизајнирана тако да минимизује ризик од откривања, укључујући одвојене сервере за различите функције система.

Финснијски модел био је заснован на провизији по трансакцији, која се кретала у процентуалном распону од 3% до 10%, у зависности од статуса продавца и обима продаје.

[88] *CybelAngel — Dark Web Marketplace Takedowns: AlphaBay and Hansa* (преузето 19.02.2026) https://cybelangel.com/blog/alphabay-hansa-two-major-dark-web-marketplaces-shut/)

.

Трансакције су обављане путем криптовалута, првенствено Bitcoin-a, а касније су подржане и друге валуте ради повећања нивоа анонимности. Escrow систем представљао је кључни механизам изградње поверења. Средства су задржавана на платформи све док купац не потврди пријем робе. У случају спора, модератори су деловали као арбитри. Овај механизам имитирао је легитимне e-commerce моделе, чиме је повећана перцепција сигурности међу корисницима.

Понуда на Hansa Marketu је била разноврсна и типична за даркнет тржишта друге генерације. Најзаступљенија категорија, са више од 90% укупне трговине, била је продаја илегалних наркотика укључујући: канабис и његове деривате, кокаин, МДМА и друге синтетичке дроге, амфетамине, опиоиде (укључујући хероин и друге синтетичке опиоиде) и психоделике. На свом врхунцу, око 3.600 Хансиних продаваца нудило је више од 24.000 производа повезаних са дрогама. Поред наркотика, тржиште је нудило и малвера и exploit алата, приступ компромитованим базама, базама података са украденим информацијама, phishing пакете и DDoS услуге, фалсификована документа (пасоши, возачке дозволе, личне карате, дипломе и сертификате), украдене кредитне картице и финансијске податке и услуге прања новца путем криптовалута. Оружје се појављивало ређе него на другм тржиштима, али је било повремено присутно. Пре затварања тржиште је имало хиљаде активих огласа, а значајан број продаваца долазио је из Европе и Северне Америке, што указује на висок степен интернационализације тржишта.

Кључни моменат у историји Hansa Marketa догодио се јула 2017.године, када је FBI затворио AlphaBay. Након тога велики број корисника ове платформе мигрирао је на Hansa Market, који је у том тренутку већ био под тајном контролом холандске полиције. Холандаска полиција је у јуну 2017. године индентификовала сервере Hansa Marketa и ухапсила администраторе, Уместо тренутног гашења, донета је стратегијска одлука да се тржиште привремено задржи у функцији како би се прикупили подаци о корисницима. Ова операција спроведена је у оквиру шире акције познате под називом Operation Bayonet у координацији са sa Europolom и FBI-јем[89]. Током периода тајног управљања платформом бележене су IP адресе корисника, прикупљани су подаци о комуникацији,

[89] Wired. (n.d.). *Hansa: Dutch police sting operation*. *Wired*. (преузето 23.03.2026.) https://www.wired.com/story/hansa-dutch-police-sting-operation

.

евидентиране сутрансакције анализирани су обрасци понашања и прикупљани су подаци о крипто-новчаницима. Дана 20.07.2017. године Hansa Market је званично угашен, а на сајту је постављена порука о заплени. Операција је омогућила идентификацију хиљада корисника широм света и покретање бројних кривичних поступака[90].

Hansa Market предсатвља пример трансформације дигиталног криминала у високо организовану, транснационалну и технолошки софистицирану активност. Његова стуктура, обим трговине и начин гашења указују на професионализацију криминалних онлајн мрежа, примену корпоративних модела управљања у нелегалном окружењу, значај криптовалута у савременим облицима организованог криминала, адаптивност илегалних тржишта након репресивних мера. Истовремено, случај Hansa Market-а показује развој нових стратегија органа за спровођење закона, укључујући дигиталну инфилтрацију, анализу великих количина података и координисану међународну сарадњу.

### 3.2.6. Dream Market (2013-2019)

Dream Market представљао је једно од најдуговечнијих и најзначајнијих Dark Web тржишта након гашења Silk Road и великих међународних операција против AlphaBay и Hansa Market. Његов значај у еволуцији дигиталног црног тржишта огледа се у чињеници да је платформа опстала више од пет година (крај 2013 – 30. април 2019), што је изузетно дуг период за Dark Web тржишта, која су често кратког века због полицијских акција, интерних превара или техничких проблема.

Dream Market је основан крајем 2013. године, недуго након пада Silk Road-а, а отприлике годину дана пре појаве AlphaBay-а. Оснивач је користио псеудоним SpeedStepper. Тржиште је функционисало на Tor мрежи и временом је постало једна од кључних платформи за илегалну онлајн трговину.

Након координисаних међународних операција 2017. године које су довеле до гашења AlphaBay-а и Hansa Market-а, Dream Market је постао једно од главних уточишта за продавце и купце који су изгубили своје налоге и инфраструктуру. Масовна миграција

[90] Bitcoin Insider. (n.d.). *Hansa controlled by law enforcement prior to shutdown*. *Bitcoin Insider*. (преузето 25.02.2026) https://bitcoininsider.org/article/208093/hansa-controlled-law-enforcement-prior-shutdown

.

корисника са ових платформи значајно је повећала обим понуде и трансакција, учврстивши Dream Market као једно од највећих даркнет тржишта тог периода[91].

Према доступним подацима, тржиште је имало више од 100.000 активних огласа. Око 75% садржаја односило се на продају наркотика, што га сврстава у групу тржишта са доминантно „нарко-фокусом“, слично као што је то био случај са Silk Road-ом и AlphaBay-ом. Као и већина великих даркнет платформи, Dream Market је нудио широк спектар илегалних производа и услуга:

- Илегалне дроге, које су чиније највећи део понуде и трансакција.

Најчешће продаване дроге биле су: Марихуана (најзаступљенија категорија по броју огласа и трансакција. Обухватала је различите сорте (strain-ове) и облике продаје, кокаин (једна од водећих категорија по вредности и обиму продаје) и Бензодиазепини (лекови као што су диазепам и алпразолам, који су чинили значајан део понуде. Ове три групе заједно чиниле су нешто мање од половине свих трансакција на тржишту). Поред њих, у понуди су се често појављивали: метамфетамин, хероин, лекови на рецепти супстанце за побољшање перформанси. Иако су опиоиди били присутни (укључујући оксикодон и фентанил), њихов удео у укупном броју трансакција био је релативно мањи у поређењу са марихуаном, кокаином и бензодиазепинима.

- Фалсификована документа
- Украдене финансијске податке (кредитне картице, банковне налоге)
- Хаковане налоге и базе података
- Malware и хакерске алате
- Дигиталне услуге повезане са сајбер криминалом
- Оружје (ређе у односу на дрогу)[92]

Поред биткоина, значајну улогу је имала употреба криптовалуте Monero, која пружа виши ниво анонимности захваљујући прикривању података о пошиљаоцу,

[91] Hack The Box. (2021, September 14). *The life and death of dark web markets*. Hack The Box Blog. (преузето 26.02.2026) https://www.hackthebox.com/blog/dark-web-markets
[92] Farrier, T. (2020). *Into the reverie: Exploration of the Dream Market*. ResearchGate. (преузето 26.02.2026.) https://www.researchgate.net/publication/339479988_Into_the_Reverie_Exploration_of_the_Dream_Market

.

примаоцу и износу трансакције. То је представљало одговор на све већу способност органа реда да прате Bitcoin трансакције путем блокчејн анализе.

Dream Market је функционисао искључиво преко Tor мреже, користећи „onion routing“ технологију ради прикривања IP адреса корисника. За комуникацију између купаца и продаваца коришћена је PGP енкрипција (Pretty Good Privacy), која је омогућавала сигурну размену порука путем система јавног и приватног кључа. Безбедносни механизми укључивали су двофакторску аутентификацију (лозинка + PGP кључ), PIN код за повлачење средстава, Escrow систем плаћања и систем оцена и рецензија.

Једна од најзначајнијих карактеристика била је escrow услуга. Средства купца су се задржавала на платформи док не потврди пријем робе. Ово је смањивало ризик од преваре. Такозвано прерано финализовање *(„finalize early“),* где продавац добија средства пре испоруке, сматрало се ризичним и препоручивало се само код високо поузданих продаваца, док је систем оцена од једне до пет звездица и могућност остављања коментара омогућавао изградњу репутације и стварао механизам саморегулације унутар тржишта.

Dream Market није био само трговачка платформа већ и заједница. Интерактивни форуми омогућавали су размену искустава, објављивање рецензија, дискусије о безбедносним праксама и савете о избегавању превара. Овај аспект је допринео осећају заједништва и стабилности платформе, што је био један од фактора њене дуговечности[93].

Значајан ударац платформи представљало је хапшење француског држављанина Gal Vallerius 2017. године, познатог под псеудонимом OxyMonster. Иако није званично потврђено да је био главни администратор, сматран је високо позицонираним чланом екосистема. Његово хапшење показало је да органи реда интензивно прате активности на даркнету.[94] 30. априла 2019. године Dream Market је изненада објавио гашење и најавио

[93] FroggyAds. (2023, November 19). *Dream Market deep web: Unveiling the shadowy eCommerce underworld*. FroggyAds. (преузето 27.02.2026.) https://froggyads.com/blog/dream-market-).
[94] Cyber Defense Magazine. (2017, October 4). *Dream Market dark web drug dealer OxyMonster arrested on way to beard contest*. Cyber Defense Magazine. (преузето 27.02.2026.) https://www.cyberdefensemagazine.com/dream-market-dark-web-drug-dealer-oxymonster-arrested-on-way-to-beard-contest/

.

прелазак на нову onion адресу. Као разлог су наведени учестали DDoS напади и захтев за откупнину од 400.000 долара. DDoS (distributed denial-of-service) напади подразумевају преоптерећивање сервера великим бројем захтева ради онемогућавања приступа. Иако су кружиле спекулације да су органи реда преузели платформу, званична потврда о заплени није објављена као у случају AlphaBay-а или Hansa-е. Ипак, затварање Dream Market-а изазвало је хаос у заједници и довело до новог таласа миграције корисника на алтернативне платформе.[95]

Dream Market представља кључну фазу у развоју даркнет тржишта. Његова дуговечност, релативна стабилност и способност да апсорбује кориснике након гашења конкуренције показују адаптивност криминалних онлајн екосистема. Истовремено, случај Dream Market-а показује сталну еволуцију безбедносних механизама, пораст употребе анонимнијих криптовалута, јачање међународне сарадње органа реда, нестабилну и ризичну природу даркнет инфраструктуре. Његово гашење 2019. године означило је крај једне од најстабилнијих фаза Dark Web тржишта и почетак новог циклуса појављивања и нестајања илегалних платформи.

### 3.2.7. Hydra Market (2015-2022)

Hydra Market био је највеће и најдуговечније Dark Web тржиште икада документовано, које је доминирало илегалном онлајн трговином, нарочито у руској језичкој регији. Платформа је основана 2015. године и брзо је постала кључни центар за дистрибуцију наркотика, фалсификованих докумената, украдених финансијских података, малвера и услуга прања новца преко криптовалута. Током активности, Hydra је имала око 17 милиона регистрованих корисника и 19 хиљада продаваца, што је чини значајно већом од свих претходних или истовремених даркнет маркета. Приступ платформи омогућавао се искључиво преко Tor мреже, а комуникација између купаца и продаваца била је потпуно анонимна[96].

[95] CyberScoop. (2019, March 27). *Dark web marketplace Dream Market to close after U.S. police nab suspected vendors*. CyberScoop. (преузето 27.02.2026.) https://cyberscoop.com/dream-market-shut-down/
[96] SOCRadar. (2023, May 10). *Hydra aftermath and the future of dark web marketplaces*. SOCRadar Cyber Intelligence Blog. (преузето 27.02.2026.) https://socradar.io/blog/hydra-aftermath-and-the-future-of-dark-web-marketplaces/

.

Једна од кључних карактеристика пословања Hydre била је метода „мртвих тачака“ *(dead-drop),* у којој продавачи остављају наручену робу, најчешће дроге, на унапред договореним тајним локацијама, а купци је потом преузимају. Ова метода, иако је повећавала трошкове доставе, значајно је смањивала директан контакт између корисника и продаваца, смањујући шансу за откривање од стране органа гоњења. Курири које запошљавају продавци крију дроге широм града пре него што трансакције започну, а продавци на веб-сајту Hydre објављују врсту, количину, приближну локацију и цену наручене робе. Након уплате, купци добијају детаљне информације о локацији „мртве тачке“, укључујући фотографије и GPS координате.

Hydra је развила софистициране интерне механизме поверења, укључујући систем повратних оцена и репутације продаваца, escrow услуге за сигурно плаћање и систем за решавање спорова између корисника. Ови механизми омогућавали су поузданост трансакција у контексту илегалног тржишта и смањивали морални ризик који иначе прате такве активности.

Већи део промета на платформи долазио је од илегалних дрога, укључујући хероин, кокаин, метамфетамин и прекурсоре за производњу наркотика. Поред тога, Hydra је нудила и друге илегалне производе и услуге, као што су фалсификовани документи, украдене финансијске информације, малвер и ransomware алати, услуге прања новца и мењачнице криптовалута. Обим илегалног бизниса био је ограничен правилима платформе, која је изричито забрањивала продају оружја, отрова, убијања по уговору, експлозива, државних тајни и порнографије. Поред тога, дроге које се сматрају посебно опасним, као што је фентанил и његови деривати, такође су биле забрањене.

Плаћање се вршило искључиво путем биткоина, а купци су имали две опције за депоновање криптовалуте. Прва је била екстерно купити биткоин и пребацити га на адресу коју је обезбедила платформа. Друга опција била је коришћење QIWI новчаника, платне услуге коју пружа руска финансијска компанија QIWI. Пошто QIWI поседује терминале налик банкоматима широм Русије, купци су могли да уплате готовину и преко крипто-мењачница повезаних са Hydrom и да је замене за биткоин. Због тога што терминали нису захтевали идентификацију, овај начин уплате омогућавао је висок степен

.

анонимности и био је један од кључних фактора популарности Hydre. Кориснички водич на сајту Hydre садржао је више страница са детаљним упутствима за коришћење QIWI терминала[97].

Hydra је била изузетно дуговечна платформа; док већина даркнет тржишта обично не преживи више од неколико месеци због полицијских акција или унутрашњих сукоба, Hydra је успешно функционисала око седам година. Током тог периода, развила је сложену организацију и правила пословања која су је чинила стабилнијом и сигурнијом за кориснике у односу на конкуренцију. По неким проценама, покривала је око 69% руске популације, а годишњи промет платформи премашивао је милијарде евра. Влада САД проценила је да је Hydra олакшала више од 5 милијарди долара незаконитих трансакција од јануара 2016. до марта 2022, а приближно 80% свих криптовалутних трансакција на даркнет тржиштима у 2021. години обављено је преко Hydre (United States v. Pavlov, 2022). Према Chainalysis (2021)[98], удео Hydre у светским приходима са даркнет тржишта 2020. године био је око 75%.

У априлу 2022. године немачке власти, у сарадњи са америчким агенцијама, запленили су сервере Hydra и званично угасиле платформу. Том приликом заплењено је око 543 биткоина, што је у то време вредело приближно 25 милиона америчких долара. Оптужени оператори су се суочили са озбиљним правним последицама, укључујући дугорочне затворске казне[99]. Пре свог пада, Hydra market је освојио 93,3% целокупне економске вредности примљене у екосистему тржишта Hydra 2022. године[100]. Гашење Hydre имало је значајан утицај на даркнет тржиште, смањујући глобални промет и изазивајући појаву нових тржишта, која су настојала попунити празнину. Међу тржиштима која су се развила након затварања Hydre, највећа су „OMG!OMG!“, „Blacksprut“, „Mega Darknet market“ и „Solaris“. Још једно тржиште, „Kraken“, отворено је

[97] Goonetilleke, P., Knorre, A., & Kuriksha, A. (2023). Hydra: Lessons from the world's largest darknet market. *Criminology & Public Policy, 22*(4), 735–777. (преузето 28.02.2026.) https://doi.org/10.1111/1745-9133.12647
[98] Chainalysis. (2021). *Darknet market report 2021: Hydra dominates global illicit crypto transactions*. Chainalysis Research. (преузето 28.02.2026.) https://blog.chainalysis.com/reports/darknet-market-report-2021

[100] Chainalysis. (2022, August 3). *How darknet markets and fraud shops fought for users in the wake of Hydra's collapse*. Chainalysis Blog. (преузето 28.02.2026.) https://www.chainalysis.com/blog/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/

.

у децембру 2022. године и представља наследника Hydre, управљано од стране особа које су биле повезане са затвореним тржиштем[101].

Студија Hydre показује да велике платформе, иако олакшавају илегалну трговину, истовремено развијају организационе и технолошке стандарде који их чине отпорнијим и дуговечнијим од просечног даркнет тржишта. Ово истраживање указује и на потребу ефикасне међународне сарадње и регулације финансијских токова како би се ограничила експанзија и утицај оваквих илегалних економија, као и на комплексну динамику између доступности илегалних производа и потенцијалне саморегулације унутар оваквих тржишта

### 3.2.8. Савремена Dark Web тржишта

Након 2023. године, Dark Web тржишта су се значајно променила у односу на период доминације великих платформи као што је Hydra. Уместо једног доминантног тржишта, екосистем је постао фрагментисан, са бројним мањим и средњим платформама које функционишу паралелно. Ова тржишта и даље се ослањају на висок степен анонимности и приватности корисника, користећи Tor мрежу, PGP шифровање и криптовалуте попут биткоина и монера за плаћање, чиме се значајно отежава праћење трансакција и идентификација учесника.

Једна од кључних карактеристика савремених Dark Web тржишта јесте развијен систем безбедносних протокола и механизама репутације, попут оцена и рецензија које омогућавају купцима да процене поузданост понуђача, што подсећа на механизме поверења који постоје и на легалним онлајн тржиштима. Поред традиционалне продаје наркотика, модерна даркнет тржишта значајно су проширила своју понуду и на дигиталне податке, дигиталне подаци, акредитиве за приступ различитим налозима, малвере, алате за извођење сајбер напада, као и различите  друге специјализоване услуге. Маркетинг и корисничко искуство су такође у фокусу – понуда попуста, loyalty програма и брзе испоруке користе се за задржавање и привлачење корисника. Ова тржишта су такође

[101] TRM Labs. (2022, December 12). *Eight months after the Hydra shutdown, new Russian-language darknet markets fill the void*. TRM Labs Blog. (преузето 01.03.2026.) https://www.trmlabs.com/resources/blog/eight-months-after-the-hydra-shutdown-new-russian-language-darknet-markets-fill-the-void

.

показала способност брзе адаптације: у случају нестанка неке платформа или суочавањем са полицијским акцијама, корисници и продавци прелазе на друге mirror сајтове или нове платформе.

Ова тржишта показују и изузетну способност адаптације. Када нека платформа буде угашена или постане предмет полицијских истрага, корисници и продавци релативно брзо прелазе на друге платформе или користе такозване „mirror“ сајтове како би наставили активности. Поред тога, све већу улогу имају и маркетиншке стратегије усмерене ка привлачењу корисника, као што су попусти, програми лојалности и бржа испорука робе. Према извештајима компаније за блокчејн аналитику Chainalysis, Dark Web тржишта су у 2023. години показала финансијски опоравак, иако су органи за спровођење закона наставили активности усмерене на њихово откривање и затварање. Укупни приходи ових тржишта достигли су приближно 1,7 милијарди долара, што представља опоравак након пада забележеног 2022. године, када је затворено доминантно тржиште Hydra.

Иако ниједна појединачна платформа није достигла ниво доминације који је Hydra имала, неколико тржишта се истакло по обиму активности и прихода. Међу најзначајнијим тржиштима у 2023. години издвајају се Mega Darknet Market, са приливом већим од 500 милиона долара, затим Kraken Market, који је стекао значајну популарност међу руским тржиштима, као и Blacksprut и OMG!OMG!, који су се позиционирали као важни актери након гашења Hydre. Подаци указују да су приходи Dark Web тржишта у периоду од 2021. до 2023. године пролазили кроз одређене осцилације. У 2021. години укупни приходи премашили су 1,7 милијарди долара, да би 2022. године дошло до пада услед гашења Hydre. Током 2023. године приходи су се поново стабилизовали на приближно 1,7 милијарди долара, што указује на релативну отпорност овог екосистема.

Једна од најважнијих промена након гашења Hydre јесте управо фрагментација тржишта. Док је Hydra у једном тренутку контролисала више од 90% прихода Dark Web тржишта, данас више платформи дели различите ниже и улоге унутар овог екосистема. Овај процес специјализације омогућио је појаву већег броја тржишта која се фокусирају на специфичне производе или услуге.

.

Оперативни трендови на Dark Web тржиштима такође показују одређене иновације. Примећена је повећана употреба крипто процесора за плаћање који су интегрисани путем API система, што омогућава ефикаснију и сигурнију обраду трансакција. Биткоин и даље остаје доминантна криптовалута за плаћање на овим тржиштима, иако се у појединим сегментима користе и монеро или стабилне криптовалуте. Иако су приходи Dark Web тржишта показали опоравак, њихов удео у укупном криптовалутном криминалу и даље остаје релативно мали у поређењу са другим облицима незаконитих активности, као што су трансакције повезане са санкционисаним ентитетима или различити облици финансијских превара. Ипак, отпорност овог екосистема, чак и након великих полицијских операција и затварања значајних платформи, указује на то да ће даркнет тржишта вероватно наставити да постоје као релативно стабилан сегмент криминалних активности у криптовалутном окружењу.

На крају, можемо закључити да Dark Web тржишта након 2023. године карактеришу фрагментација, висок степен анонимности, проширена понуда илегалних производа и услуга, развијени системи репутације и безбедности, као и значајна способност прилагођавања и опстанка у условима сталног притиска органа за спровођење закона.

## 4. ТИПОЛОГИЈА КРИВИЧНИХ ДЕЛА НА DARK WEB- У

Типологија ових дела обухвата неколико основних категорија, које се разликују по природи деликта, методама извршења и мотивима починилаца. И то:

- Неовлашћена производња и стављање у промет опојиних дрога
- Секусална екпслоатација деце и дечија порнографија
- Трговина људима
- Трговина оружјем и експлозивним материјама
- Cyber crime as a service (CaaS)
- Прање новца путем криптовалута

.

### 4.1. Неовлашћена производња и стављање у промет опојиних дрога

Online тржишта дрога имају дугу историју која сеже чак до 1970-их, када су студенти са Масачусетског технолошког института (МИТ) и Универзитета Станфорд известили о првој познатој трансакцији дроге на интернету, у којој је размењиван канабис. У истом периоду, први рачунарски мрежни системи као што је ARPANET (1969) омогућавали су анонимну размену података, што је касније послужило као прототип за Dark Web. Крајем 1990-их, појавили су се дискусиони форуми и групе за производњу и употребу дрога, попут форума The Hive (1997), који је омогућавао учесницима – од самопроглашених хемичара до теоретичара и форензичких стручњака – размену информација о синтези лекова.

Прелазак са онлајн на дигитална тржишта дрога драстично је променио начин продаје и дистрибуције[102]. Darknet или Dark Web, представља мрежу у којој људи анонимно учествују у различитим активностима, легалним и илегалним, користећи шифровање и криптовалуте да би сакрили своје трансакције. Продавци дрога сада могу комуницирати са купцима и понудити илегалне супстанце без физичког сусрета, што значајно повећава безбедност и ефикасност. Администратори веб-сајтова користе системе који олакшавају поуздану размену робе, укључујући:

- Рангирање добављача на сајту
- Приказ броја успешних трансакција
- Оцена квалитета пошиљке
- Систем звездица (1–5).

Dark Web тржишта демонстрирају сложену природу мутативног организованог криминала. Крипто тржишта пружају веома безбедан начин за куповину и продају илегалних дрога, услуга и робе. Готово све врсте дрога, укључујући психоактивне супстанце, могу се купити релативно лако. Купце углавном чине повремени или искусни

[102] Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy, 35*, 7–15. (преузето 03.032026.) https://doi.org/10.1016/j.drugpo.2016.04.020

.

корисници дрога, привучени због повећане безбедности, квалитета, разноврсности и погодности, укључујући брзу доставу. Они доносе одлуке на основу:

- цене
- детаља о производу
- извештаја са „трипова“ (личних искустава)
- репутације добављача
- повратних информација других купаца. [103]

Историјски, појединачна тржишта дрога на Dark Web-у нису дуго постојала, али индустрија у целини је превазишла бројне препреке, укључујући полицијске упаде и преваре при затварању сајтова. Од затварања платформе Silk Road, број трансакција се утростручио, а приходи су повећани за 50%, иако је обим трговине и даље мањи него на офлајн тржиштима. Darknet омогућава предузетницима да развију нове пословне моделе и приступе широј бази корисника, али истовремено уводи нове ризике као што су пресретање поште и сајбер преваре.

Према студији коју су спровели Sudan, Tai, Kim и Krausz (2023), истражен је обим и природа трговине дрогом на Dark Web-у, са посебним фокусом на промене у дистрибуцији и доступности психоактивних супстанци у периоду од 2012. до 2023. године. Аутори су анализирали податке из постојеће литературе о дрогама доступним на криптотржиштима између 2012. и 2019. године, као и нове податке прикупљене са 13 различитих Dark Web тржишта у периоду од августа 2022. до јануара 2023. године, укључујући огласе за наркотике, типове дрога и географско порекло супстанци.

Анализа литературе о дистрибуцији дрога између 2012. и 2019. године показала је да су се најзаступљеније категорије дрога на Dark Web тржиштима током овог периода биле:

[103] RAND Europe (2016). *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands: Summary*. RAND Corporation, Santa Monica, CA & Cambridge, UK. (преузето 02.03.2026)https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1607/RAND_RR1607.summary-english.pdf

.

- **Канабис и хашиш**: око 22.7% свих огласа
- **Рецептурни лекови**: 20.4% свих огласа
- **Стимуланси** (као што су кокаин и метамфетамини): 14.3%
- **Остале супстанце** (укључујући бензодиазепине и дисоцијативне лекове): 13.5%
- **Екстази/MDMA**: 12.8%
- **Психоделици** (попут LSD-а и гљива): 10.8%
- **Опиоиди**: 5.5%

Током овог периода, канабис и хашиш били су најчешће доступне супстанце, док су опиоиди били на дну по учесталости. Ова дистрибуција остајала је релативно стабилна током већине ових година. Подаци прикупљени са 13 различитих тржишта у периоду између 2022. године показују значајне промене у дистрибуцији дрога:

- **Канабис и хашиш**: 29.5% свих огласа
- **Стимуланси**: 19.4%
- **Опиоиди**: 9.25% (дупло више него у 2012–2019)
- **Рецептурни лекови**: 4.3% (пад са више од 20%)
- **Психоделици и екстази/MDMA**: мање заступљени

Као највећа промена, види се нагли пад у доступности рецептурних лекова, који су некада били једна од најзаступљенијих категорија. Насупрот томе, број огласа за опиоиде значајно је порастао, што је у складу с глобалним трендом раста употребе синтетичких опиоида као што је фентанил[104].

Трговина дрогом на Dark Web-у 2024. години вредела је преко 1,7 милијарди долара, са растом од 20%. Главне дроге су: канабис, синтетичке дроге, кокаин и у мањој мери опиоиди. Синтетичке дроге имају највећи удео продаје на даркнету, док канабис и

[104] Sudan, H. K., Tai, A. M. Y., Kim, J., & Krausz, R. M. (2023). *Decrypting the cryptomarkets: Trends over a decade of the Dark Web drug trade*. *Drug Science, Policy and Law*. (преузето 05.03.2026.) https://www.drugpolicyfacts.org/node/4380?utm_source=chatgpt.com

.

кокаин користе друштвене медије због делимичне легалности. Географска средишта укључују САД, северну и западну Европу и Русију, са растућим учешћем тржишта у Азији и Латинској Америци.[105]

Према извештају Европола за 2025. годину, Dark Web тржишта генеришу 5–7,5 милиона долара дневно, а од 30.000 активних сајтова, 56–60% се бави криминалним активностима. Тржишта функционишу као легитимни веб-сајтови са описима производа, сликама и системом оцена, али користе шифровање и криптовалуте. На платформама се нуди дрога, оружје, фалсификовани производи, украдени подаци, хакерски алати и дивље животиње.[106]

Dark Web тржишта показују изузетну отпорност: када се сајтови затворе, продавци и купци се прелазе на друге платформе, осигуравајући континуитет трговине. Трансакције су веће у односу на онлајн, са растућом велепродајом: велика малопродаја ($100–499) чини 37,8%, потенцијалне велепродаје (преко $1.000) 31,9%, мала малопродаја 18,9% и друштвена понуда 11,4%.[107]

Прелазак на онлајн трговину убрзан је пандемијом COVID-19, јер су мере закључавања подстакле продавце и купце да користе дигиталне платформе. Online тржишта дрога се сматрају безбеднијом алтернативом уличној трговини, али носе нове ризике као што су сајбер преваре и здравствени проблеми од нерегулисаних супстанци. Поред тога, ова тржишта дубоко су повезана са сајбер криминалом и финансијским злочинима, што указује на потребу за међународном сарадњом, технолошким напредком и прикупљањем обавештајних података како би се успешно супротставила глобалној трговини дрогом.

[105] Ibid
[106] Global Initiative against Transnational Organized Crime. (2025). ***The digital drug revolution: How online markets are reshaping global illicit trade***. (преузето 06.03.2026.)https://globalinitiative.net/analysis/digital-drug-revolution-online-markets-global-illicit-trade-ocindex/
[107] Ibid

.

### 4.2. Секусална екпслоатација деце и дечија порнографија

Развој интернета, експанзија World Wide Web-а и мобилних технологија омогућили су лак и непосредан приступ порнографским садржајима, који се данас деле, продају и размењују на глобалном нивоу. Стога, преступниц више не морају да буду у непосредној физичкој близини да би починили кривично дело, већ им је потребан само online приступ (нпр. интернет собе за ћастање, e-mail, душтвене мреже) за комуникацју са малолетницима. У том смислу, интернет је уклонио многе препреке за приступ жртвама и производњу материјала који приказује сексуално злостављање деце, са којима су се преступници традиционално суочавали. Дигитално тржиште сексуалних садржаја бележи експоненцијалан раст, при чему је забрињавајући пораст материјала који приказују сексуалну експлоатацију деце, као и пораст насиља у кривичним делима која укључују сексуално злостављање малолетника. Трагично је што се временом смањује старосна граница жртава, што указује на погоршање овог проблема.

Матријал сексуалног злостављања деце (Child Sexual Abuse Material – CSAM), који се и у академским круговима назива и материјал сексуалне експлоатације деце (Child Sexual Exploitation Material - CSEM), а који представља ширу категорију материјала који укључује CSAM, али и виртуелне, симулиране или манипулисане приказе деце, као и материјале који су део сексуалне експлоатације, манипулације или принуде, представљају савремене термине који замењују израз „дечја порнографија“. Развој онлајн технологија омогућио је лакшу дистрибуцију и конзумацију овог материјала, али и његову све већу присутност на различитим сегментима интернета, укључујући и Dark Web[108] [109] [110].

Иако је тешко проценити стварне размере онлајн CSAM-а због скривене природе садржаја и изазова у детекцији, студије указују на његову сталну присутност. На пример, у анализи пет peer-to-peer (P2P) мрежа, процењено је да је око три од 10.000 интернет

[108] Brown R & Bricknell S 2018. *What is the profile of child exploitation material offenders? Trends & issues in crime and criminal justice* no. 564. Canberra: Australian Institute of Criminology. https:// www.aic.gov.au/publications/tandi/tandi564
[109] Holt TJ, Blevins KR & Burkert N 2010. *Considering the pedophile subculture online.* Sexual Abuse 22: 3–24
[110] Westlake BG 2020. *The past, present, and future of online child sexual exploitation: Summarizing the evolution of production, distribution, and detection*. In T Holt & A Bossler (eds), The Palgrave handbook of international cybercrime and cyberdeviance. New York: Palgrave Macmillan: 1225–1253

.

корисника широм света дистрибуирало CSAM током једног месеца[111]. Internet Watch Foundation је од 1996. до 2018. уклонила више од 400.000 веб-страница које приказују злостављање деце, при чему је само 2018. идентификовано и уклоњено 105.047 страница[112].

Dark Web пружа висок ниво анонимности и техничке заштите, што га чини погодним окружењем за реализацију различитих видова криминалитета, укључујући сексуалну експлоатацију деце. Платформе и сајтови као што су *Lolita City*, *Hard Candy*, *Jailbait*, *Love Zone*, *PedoEmpire*, *Kindergarten Porn* и *The Family Album* омогућавају педофилима да се повежу, деле фетише, размењују технике злостављања деце и, што је најозбиљније, да размењују детаљне инструкције о начинима проналажења, врбовања и завођења деце, као и извођења насилних сексуалних радњи[113]. Ови сајтови омогућавају произвођачима CSAM-а да дистрибуирају материјал који је настао злоупотребом деце ради задовољства педофила широм света [114].

Иако је дистрибуција CSAM-а глобални проблем, Сједињене Америчке Државе и даље представљају један од водећих произвођача садржаја о злостављању деце са великом базом корисника. Преко 150.000 деце годишње буде жртва сексуалног трговца у САД, а трговци људима могу зарадити и до 200.000 долара по детету. Извештаји Европола наводе да бројни сајтови на Dark Web-у преносе уживо силовања и злостављања деце, где педофили наређују злостављачима да изводе садистичке радње. Форуми на Dark Web-у посвећени CSAM активностима имају велики број чланова. Седам највећих форума имало је преко 2 милиона различитих корисничких ID-ова, а више од 300.000 корисника је активно учествовало, при чему су се неки регистровали на више форума. Ови системи нису случајно откривени и захтевају од потенцијалних чланова да прођу проверу и

[111] Bissias G, Levine B, Liberatore M, Lynn B, Moore J, Wallach H & Wolak J 2016. *Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks*. Child Abuse & Neglect 52: 185–199

[112] Internet Watch Foundation (IWF) 2018. Once upon a year. Cambridge, UK: IWF

[113] Nearchou, N. (2023). *Efforts to reduce child abuse on the Dark Web*. In *Combating Crime on the Dark Web* (Chap. 4). Packt Publishing. ( преузето 25.02.2026) https://subscription.packtpub.com/book/security/9781803234984/6/ch06lvl1sec21/efforts-to-reduce-child-abuse-on-the-dark-web

[114] Murali, V. (2019). *Online child sexual abuse material and its global proliferation: technological enablers and criminal networks*. Journal of Cyber Criminology, 13(2), 145–162.

.

доставе нови CSAM материјал приликом регистрације и обнове чланства, што указује на високи ниво мотивације код учесника[115] [116].

Студија коју је спровео Аустралијски институт за криминологију представља први криминалистички сценарио који појашњава како учиниоци кривичних дела секусалне злоупотребе деце делују на дарквебу. Према овој студији криминални сценарио чине 3 фазе[117]:

1. Фаза припреме кривичног дела

Пре приступа Dark Web-у, починиоци CSAM-а имају различите мотиве за своје деликвентно понашање као што је сексуално задовољство, истраживање сопствене сексуалности са децом и/или потврђивање сопствених сексуалних интереса. Многи починиоци настоје да ступе у интеракцију са особама које деле сличне интересе, што додатно подстиче њихову укљученост у сексуалне активности са децом, док неки од њих траже информације о техникама сексуалног злостављања и манипулације децом.

Предуслови за ову фазу укључују неколико корака:

- приступ интернету и способност навигације кроз clear web,
- тражење CSAM садржаја претраживањем порнографског садржаја за одрасле, претраживањем кључни речи преко Googla и стицање сазнања о CSAM садржају преко дискусионих форума или форума о сродним темама
- стицање информација о Tor мрежи и упутствима за приступ Dark Web-у.

2. Фаза извршења кривичног дела

Када починиоци идентификују сајтове и форуме са CSAM-ом, морају предузети кораке за приступ заштићеном садржају, укључујући креирање налога са корисничким именом и лозинком, заштиту идентитета, а затим ступање у интеракцију са другим члановима, као и на обичним друштвеним платформама, попут коментарања, „лајковања“,

[115] Europol (2014). *Internet Organised Crime Threat Assessment (IOCTA)* (преузето 27.02.2026.) https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta
[116]Europol (2021). *Serious and Organised Crime Threat Assessment (SOCTA)*. (преузето 27.02.2026.), https://www.europol.europa.eu/activities-services/main-reports/socta
[117] Benoit Leclerc, Jacqueline Drew, Thomas J Holt, Jesse Cale and Sara Singh 2021 „*Child sexual abuse material on the darknet: A script analysis of how offenders operate*“) *Trends & Issues in Crime and Criminal Justice No. 627* Australian Institute of Criminology

.

слања приватних порука и објављивање линкове, чиме граде мрежу која им омогућава конзумирање и дистрибуцију CSAM-а у складу са њиховим интересима.

3. Фаза наставка криминалне активности

Након извршења кривичног дела, појединци се крећу у једном од три смера. Први смер је конзумирање CSAM-а, затим напуштање Dark Web-а, због сложености навигације или недостатка интересовања за интеракцију. Други смер је вишеструко понављање фазе извршења и активније укључивање у конзумирање и дистрибуцију CSAM-а, за њих се фаза извршења кривичног дела циклично понавља током времења, јер проналазе платформу за изражавње и интеракцију са другим особама истих сексуалних интерса. Трећи смер представља повећање активности на Dark Web-у учешћем у специфичним заједницама у којима постепено стичу све виши статус, одржавањем или повећањем доприноса CSAM-у, као и тражењем приступа другим заједницама и форумима.

### 4.3.Трговина људима

Појава интернета, а посебно његовог анонимног сегмента познатог као Dark Web, значајно је изменила структуру и функционисање организованог криминала. Иако трговина људима постоји вековима, савремене технологије омогућиле су њену трансформацију, глобално ширење и повећање профитабилности. Дигиталне платформе, шифроване апликације, анонимне мреже и криптовалуте омогућавају криминалним групама да делују са мањим ризиком од откривања и уз већу ефикасност него икада раније.

Према подацима Међународне организације рада (ILO) и Уједињених нација, око 49,6 милиона људи живи у условима модерног ропства, укључујући 12 милиона деце. Илегална индустрија присилне комерцијалне сексуалне експлоатације годишње генерише 172,6 милијарди долара. Према проценама United Nations Office on Drugs and Crime (UNODC), у сваком тренутку у свету постоји око 2,5 милиона жртава трговине људима,

.

док је стопа кривичног гоњења и даље забрињавајуће ниска[118]. Деца чине скоро једну трећину свих жртава[119].

За трговце људима, Dark Web представља погодно окружење јер омогућава анонимну комуникацију са клијентима и сарадницима, могућност оглашавања илегалних услуга, продају приступа жртвама, координацију транспорта и логистике и финансијске трансакције путем криптовалута, нарочито Bitcoin-а и других дигиталних валута, отежава праћење новчаних токова и прикрива идентитет починилаца.

Према Crypto Crime Report из 2026. године истраживања фирме Chainalysis**,** плаћања криптовалутама повезана са мрежама трговине људима порасту за 85% у 2025. години, достигавши обим од стотина милиона долара у идентификованим трансакцијама. Извештај указује да су стабилкоини (stablecoins) посебно заступљени у овим трансакцијама, јер омогућавају лакшу конверзију и мању волатилност у односу на традиционалне криптовалуте. Истовремено, Bitcoin и одређене приватније валуте користе се у активностима повезаним са дистрибуцијом материјала сексуалног злостављања деце[120].

Према књизи Combating Crime on the Dark Web[121], Онлајн трговина људима обухвата више фаза. Прва фаза се односи на регрутовање жртава и обично почиње на легалним платформама: друштвени мрежама, апликацијама за упознавње или сајтовима за оглашавање послова. Трговци људима користе лажне понуде за посао, агенције за моделинг, романтичне преваре и технику „дотеривања“ (grooming), при чему постепено стичу поверење жртве, изолују је од породице и пријатеља и доводе у позицију зависности. У том контексту, рањиве групе – малолетници, мигранти, особе из сиромашних средина – представљају посебну мету.

---

[118] Scientific American. (2015, February 8). *Human traffickers caught on hidden internet*. Scientific American. (преузето 10.02.2026.) https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/

[119]UNICEF. (2018, July 27). *Children make up almost one-third of all human trafficking victims worldwide*. UNICEF. (преузето 10.02.2026.) https://www.unicef.org/stories/children-make-almost-one-third-all-human-trafficking-victims-worldwide/

[120] Chainalysis. (2026). *Crypto Crime Report 2026: Human Trafficking*. (преузето 10.02.2026.) https://www.chainalysis.com/blog/crypto-human-trafficking-2026/

[121] Nearchou, N. (2023). *Combating Crime on the Dark Web: Learn how to access the dark web safely and not fall victim to cybercrime*. Packt Publishing. ISBN 978-1803234984.

.

Друга фаза обухвата оглашавање и промоцију жртава. На различитим online платформама постављају се огласи који прикривено нуде сексуалне услуге, често уз употребу шифрованог језика и кодираних израза како би се избегло аутоматско откривање. Dark Web форуми и тржишта омогућавају продају приступа жртвама, размену контаката и координацију криминалних активности. Поред тога, развој стриминг технологија омогућио је уживо пренос сексуалне експлоатације, што додатно повећава профитабилност и проширује тржиште на глобални ниво.

Трећа фаза односи се на финансијске трансакције и логистику. Трговци људима користе комбинацију традиционалних финансијских инструмената (кредитне картице, трансфер новца) и дигиталних валута ради прикривања трагова. Интернет олакшава резервацију смештаја, транспорт жртава, изнајмљивање простора и координацију са другим криминалним актерима. Такође, услуге дељења вожње, online платформе за изнајмљивање станова и апликације за размену порука често се злоупотребљавају у циљу организације експлоатације.

За разлику од трговине дрогом или оружјем, где се роба продаје једнократно, жртва трговине људима може бити експлоатисана више пута дневно, што криминалним групама доноси континуирани приход. Управо та „поновљива експлоатација“ чини овај злочин изузетно профитабилним и окрутним. Посебно забрињава пораст криптовалутних плаћања повезаних са материјалом сексуалног злостављања деце. Платформе за размену датотека, шифроване поруке и затворене онлајн заједнице омогућиле су ширење материјала сексуалног злостављања деце, као и умрежавање починилаца на глобалном нивоу. Извештај Chainalysis указује да се велики број трансакција одвија у мањим износима (често испод 100 долара), што указује на претплатничке моделе приступа илегалном садржају. Ова фрагментација плаћања отежава детекцију, али истовремено ствара стабилан и континуиран извор прихода за криминалне групе.

Дигитализација је такође довела до појаве нових облика експлоатације, као што су виртуелна сексуална експлоатација, принудно учешће у порнографском садржају, „секс-трафикинг на даљину“ и уцене путем интимних фотографија (sextortion). Глобализација

.

омогућава да се жртве експлоатишу без физичког премештања, што додатно компликује правну квалификацију и надлежност органа гоњења

### 4.4. Трговина оружјем и експлозивним материјама

Током 2019. године, Аустралијски институт за криминологију спровео је истраживање продаје оружја на Dark Web-у, прикупљајући податке са 20 дарквеб тржишта. Од тога, 8 великих тржишта (Agartha, Apollon, Berlusconi, Dark Shades, Empire, Nightmare, Samsara и Tochka, представљала су omnibus тржишта**,** док су остала била нишна, специјализована за мало и лако оружје (SALW), као што су Luckp-47, Guns & Ganja и The Armory, која су обухватала више од половине нишних огласа (55,7%))[122].

Анализа је показала да је трговина илегалним оружјем релативно мала у односу на укупан број активности на овим платформама. Укупно је идентификовано 2.124 огласа за оружје од 1.099.257 листинга (0,193%). Велики део понуде (88,9%) био је на omnibus тржиштима, док је само 11,1% огласа било на нишним тржиштима. Најзаступљенија категорија били су пиштољи (70,5%), од којих је 88% било полуавтоматских. Следиле су пушке (10,3%), муниција (3,7%), подмашинске пушке (1,9%), експлозиви (1,7%), сачмарице (1,6%) и додаци (1,1%). Дигитални производи (5,3%), хемијско, биолошко, радиолошко и нуклеарно оружје (CBRN, 0,64%) и остало оружје (3,3%) били су присутни само на omnibus тржиштима. Најчешћи калибар полуавтоматских пиштоља био је 9 mm**,** а најзаступљенији произвођач Glock GmbH, који је правио више од половине свих пиштоља.[123]

Укупно је идентификовано 218 пушака, при чему је најчешћа select-fire или полуаутоматска пушка била Kalashnikov (AK-47, n=49, 23%)**,** а затим Colt AR-15 (5,5%)**.** Око половине пушака (49,6%) било је полуавтоматско и произведено у САД, Европи и другим земљама, а многе су имале потенцијал за конверзију у select-fire помоћу интернет ресурса и комплета за модификацију. Експлозиви су били углавном гранате (запаљиве,

[122] Broadhurst, R., Foye, J., Jiang, C., & Ball, M. (2021). *Illicit firearms and other weapons on darknet markets* (Trends & Issues in Crime and Criminal Justice No. 622). Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2021-03/ti622_illicit_firearms_and_other_weapons_on_darknet_markets.pdf
[123] Ibid

.

гасне или димне), а доступни су били и RPG, динамит, RDX и C-4 (укупно 6 листинга). Додатна опрема обухватала је нишане, пригушиваче, шипке/магазине, прибор за ношење, додаци за пушке и бацач граната. Категорија „остало“ обухватала је airsoft оружје, које се потенцијално може конвертовати у смртоносно и класификује се као SALW, као и ножеве, електрошокере, бибер спреј, боксере и палице. Дигитални производи укључивали су DIY приручнике, 3D моделе оружја, приручнике за прављење реплика RPG и „Anarchist Cookbook“ за израду оружја, електронике и експлозива[124].

Нишна тржишта нудила су ограничен број модела пушки, муниције, подмашинских пушки и пиштоља. Само два нишна тржишта нудила су експлозиве, а четири су нудила додатну опрему.

Цене оружја варирале су према категорији, уз Bitcoin као главни начин плаћања. Медијана цена пиштоља износила је A$964, при чему су полуаутоматске пиштоље биле скупље од револвера (A$1,002 naspram A$808). Пушке су имале медијану A$1,288, док су select-fire и bolt-action модели били скупљи. Подмашинске пушке биле су најскупље (медијана A$1,531, просек A$2,941). Експлозиви су коштали A$361–A$459, док су CBRN производи имали цене A$728–A$1,169. Муниција се продавала у кутијама од 50 метака по A$169, додатна опрема (нишани, пригушивачи, night vision) коштала је од A$864 до A$4,547, а дигитални производи су били најјефтинији (медијана A$3,10)[125].

Ови подаци указују да omnibus тржишта представљају главни канал продаје оружја на Dark Web -у, нудећи широку палету производа, док нишна тржишта задржавају фокус на специфичним категоријама. Иако је укупан обим трговине оружјем мали у односу на друге илегалне активности на Dark Web у, подаци наглашавају доминацију малог и лаког наоружања (handguns и rifles) и географску и произвођачку концентрацију која може бити релевантна за криминолошке анализе и стратегије контроле илегалне трговине. Omnibus тржишта често забрањују продају илегалног оружја, али продавачи могу заобићи правила користећи прикривене називе, описе или слике.

[124] Ibid
[125] Ibid

.

Укључивањем и нишних и omnibus тржишта, студија показује да нишна, специјализована тржишта избегавају нестабилност „великих“ тржишта и функционишу „под радаром“. У поређењу са претходним истраживањима, идентификовано је више врста оружја, што указује на еволутивну и нестабилну природу даркнет тржишта.

### 4.5. Сајбер криминал као услуга (Cyber crime as a service - CaaS)

Сајбер криминал као услуга (CaaS) представља савремени модел организованог дигиталног криминала који омогућава ширење сајбер претњи путем понуде илегалних алата и услуга „на захтев“. Уместо појединачних и технички високо обучених хакера, данашњу сцену карактеришу професионализоване криминалне групе које функционишу по принципима легалне ИТ индустрије — са јасном поделом улога, корисничком подршком, моделима претплате и системима провизије.

CaaS се односи на криминалну економију индустријских размера у којој се злонамерни софтвер, инфраструктура и приступ компромитованим системима продају или изнајмљују као комерцијалне услуге. Најраспрострањенији облици укључују RaaS (Ransomware-as-a-Service), односно изнајмљивање рансомвер платформи, PhaaS (Phishing-as-a-Service), услуге иницијалног приступа које нуде IAB групе (Initial Access Brokers), DDoS „booter“ сервисе, претплате на малвер, као и алате за преваре засноване на вештачкој интелигенцији.

Посебну улогу у развоју овог модела има Dark Web, који је допринео трансформацији сајбер криминала у организовано и високо профитабилно тржиште. На илегалним платформама напади се нуде „као услуга“, док се украдени подаци третирају као роба са унапред дефинисаним ценама, системима плаћања, па чак и рецензијама корисника. Оваква комерцијализација значајно подстиче различите облике криминала, укључујући крађу идентитета, финансијске преваре и корпоративну шпијунажу.

Најчешћи алати и услуге који се могу пронаћи на овим платформама су:

.

### 4.5.1. Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) представља модел организованог сајбер криминала у којем се злонамерни софтвер нуди се као услуга другим нападачима нападачима у замену за проценат од откупнине добијене нападом. Уместо да нападач сам развија сопствени ransomware, он може да „закупи“ већ готов алат од професионалних програмера који одржавају читаву инфраструктуру. Овај модел функционише по принципу легалних софтверских сервиса (SaaS), али у илегалне сврхе, чиме се значајно снижава праг уласка у сајбер криминал и омогућава чак и технички мање искусним појединцима да спроводе сложене и финансијски штетне нападе.

У оквиру RaaS екосистема постоје две кључне улоге. Прву чине оператери, односно креатори ransomware-a, који развијају злонамерни софтвер, обезбеђују сервере, системе за комуникацију са жртвама и платформе за наплату откупнине у криптовалутама. Другу групу чине афилијати — појединци или криминалне групе које користе тај софтвер за извођење напада. Зарада се најчешће дели тако што афилијат задржава већи проценат откупнине (често 60–80%), док остатак припада програмерима.

Сам напад обично почиње компромитацијом система путем фишинг порука, украдених лозинки или искоришћавањем безбедносних рањивости. Након уласка у мрежу, ransomware се активира и шифрује податке жртве, онемогућавајући приступ системима. Жртви се затим приказује порука са захтевом за плаћање откупнине, најчешће у криптовалути. Савремене RaaS групе често примењују тактику „двоструке изнуде“, што значи да поред шифровања података и краду осетљиве информације и прете њиховим јавним објављивањем уколико откупнина не буде плаћена.

RaaS је допринео експанзији глобалних ransomware кампања и појави бројних криминалних група као што су LockBit, REvil и DarkSide, које су нападале компаније, болнице, владине институције и критичну инфраструктуру широм света. Због своје профитабилности, анонимности коју омогућавају криптовалуте и глобалне доступности, Ransomware-as-a-Service данас представља један од најопаснијих и најбрже растућих облика сајбер криминала.

.

Извештај *Worldwide Ransomware, 2024* [126]пружа глобалну слику ransomware претње и показује да овај облик сајбер криминала наставља да се шири и напредује. У 2024. години, регистровано је 5.289 јавних ransomware напада, што представља пораст од 15% у односу на 2023. годину (4.591 инцидент). Иако је овај раст мањи у поређењу са претходном годином (2023. је имала 77% годишњи раст у односу на 2022. године, он и даље указује на континуирано ширење ове претње.

Према извештају, Сједињене Америчке Државе чине половину свих напада, због великог броја профитабилних мета и циљева у кључним секторима. Поред САД, значајна активност је примећена у Европи и Евроазији (око 48% глобалне активности), док су Северна Америка без САД**,** источна и јужна Азија и Јужна Америка такође биле погођене.

Екосистем ransomware група је фрагментиран, а најчешће коришћене верзије у 2024. години биле су: LockBit (13,06%), RansomHub (12,9%), Akira (4,75%), Hunters International (4,5%) и AKO (3,42%), док остатак активности чини више од 61% напада. Операције као што је Operation Cronos довеле су до хапшења чланова злонамерних група, заплене крипто-налога и више од 7.000 кључева за дешифровање, омогућавајући неким жртвама да поврате податке без плаћања откупнине. Међутим, ове интервенције нису значајно промениле структуру ransomware екосистема, јер су се нове и ре-брандиране групе попут Akira**,** BianLian и Play појавиле као активни актери у другој половини 2024[127].

Важно је напоменути да иако број пријављених инцидената даје релативно јасну слику трендова, реалан број напада може бити значајно већи јер многе жртве не објављују инциденте или детаље о плаћеним откупнинама како би избегле репутацијске и правне последице. Поред тога, други извори указују да је само у 2024. години више од 195 милиона записа (корисничких података) компромитовано у потврђеним ransomware нападима.

У 2025. години, ransomware напади настављају да представљају значајну претњу у области сајбер безбедности, са растућим уделом у укупним инцидентима који доводе до

[126] Office of the Director of National Intelligence (ODNI). (2024). *Worldwide ransomware, 2024: Increasing rate of attacks tempered by law enforcement disruptions*. Cyber Threat Intelligence Integration Center (CTIIC). (преузето 15.02.2026.), https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf
[127] Ibid

.

повреде података. Према подацима из Verizon-овог Data Breach Investigations Report (DBIR) за 2025. годину[128], ransomware је присутан у 44% свих анализираних безбедносних инцидената, што представља пораст од 12% у односу на претходну годину, када је овај проценат износио 32%. Овај тренд потврђује све већу учесталост ransomware напада као примарног покретача пробоја безбедности, насупрот секундарним методама напада.

Ransomware напади посебно погађају мала и средња предузећа (SMB), која чине 88% свих погођених организација. За разлику од већих организација, које, иако суочене са нападима, имају боље развијене безбедносне протоколе, SMB предузећа се суочавају са озбиљним изазовима у вези са слабијим ресурсима, споријим циклусима закрпа и недостатком одговарајућих заштитних механизама.

Један од кључних помака у 2025. години јесте промена у понашању организација у вези са исплатом откупнине. Према извештају IBM-а, 64% организација није платило откупнину, што представља значајан пораст у односу на 50% из 2023. године. Овај помак указује на широку промену у приступу према ransomware нападима, где се организације све више опредељују за стратегије опоравка, уместо да се повињују захтевима нападача. Медијана износа откупнине пала је на $115,000, што је смањење у односу на претходну годину, када је износила $150,000[129].

Иако одбијање плаћања представља позитиван помак у контексту отпорности организација, трошак ransomware напада и даље остаје значајан. Према подацима IBM-а, просечан трошак ransomware напада, укључујући трошкове истраге, правне последице, застоје у пословању и репутацијску штету, достигао је износ од $5.08 милиона. У Сједињеним Америчким Државама, просечне осигуравајуће накнаде у вези са ransomware нападима порасле су за 68%, достигавши износ од $353,000, што указује на растуће трошкове опоравка и санације након напада[130].

[128] Verizon. (2025). *Data Breach Investigations Report (DBIR) 2025*. Verizon Business. (преузето 17.02.2026) https://www.verizon.com/business/resources/reports/dbir/
[129] SOCRadar. (2025, 26. decembar). *Top 20 ransomware statistics you should know (2025)*. SocRadar. (преузето 17.02.2026) https://socradar.io/blog/top-20-ransomware-statistics-to-know-2025/
[130] ibid

.

Промене у методама напада такође су евидентне. Иако је шифровање података традиционално била најчешћа тактика ransomware напада, у 2025. години шифровање је примењено у 50% напада, што представља пад у односу на 70% из 2024. године. Нападачи све чешће користе методе попут крађе података, чиме се повећава притисак на жртве, које су суочене са дуплом уценом (data exfiltration). Према извештајима, у 28% напада где је шифровање примењено, нападачи су такође украли податке, што значи да ransomware напади све више укључују дуплу уцену, где је циљ не само шифровати податке већ и изложити их јавности[131].

Еволуција ransomware екосистема такође је евидентна. У трећем кварталу 2025. године, 85 extortion група било је активно, а број нових жртава месечно достигао је просек од 535. Најактивнији соj ransomware-а био је Akira, одговоран за 34% напада, док је Qilin имао удео од 10%. Индустрије попут производње и здравства остале су међу најпогођенијима, при чему је сектор производње забележио 61% пораст напада у односу на претходну годину[132].

### 4.5.2. Phishing as a servise

Комплети за фишинг представљају унапред припремљене пакете који обично садрже копије легитимних веб-страница (на пример страница за пријаву банке, друштвене мреже или корпоративне е-поште), скрипте које аутоматски бележе унето корисничко име и лозинку, као и административни панел за праћење украдених података. Често укључује и упутства за постављање лажне странице на компромитовани сервер или хостинг услугу, као и шаблоне е-порука које се шаљу жртвама. Напреднији комплети садрже алате за заобилажење безбедносних механизама, као што су CAPTCHA заштита или основни филтери за откривање нежељене поште.

Начин функционисања је релативно једноставан: нападач пошаље лажну поруку која изгледа као да долази од поуздане институције (банке, компаније, службе за доставу, техничке подршке). Порука обично садржи линк ка лажној страници која визуелно готово

[131] Sophos. (2025). *The State of Ransomware 2025*. (преузето 18.02.2026) https://www.sophos.com/en-us/blog/the-state-of-ransomware-2025
[132] SOCRadar. (2025, 26. decembar). *Top 20 ransomware statistics you should know (2025)*. SocRadar. (преузето 17.02.2026) https://socradar.io/blog/top-20-ransomware-statistics-to-know-2025/

.

у потпуности имитира оригиналну. Када жртва унесе своје податке, они се шаљу директно нападачу. У неким случајевима, жртва се након тога преусмерава на праву страницу како не би одмах посумњала на превару.

Посебно опасан облик је такозвани „*spear phishing“,* односно циљани фишинг напад, у којем се поруке персонализују на основу претходно прикупљених информација о жртви. Ове информације често потичу из претходних цурења података или са јавних профила на друштвеним мрежама. На пример, након великог цурења података са платформе LinkedIn 2021. године, нападачи су користили стварне контакт податке и радне позиције како би креирали уверљиве поруке које су имале већу стопу успеха.

Комплети за фишинг се често продају по моделу „Phishing-as-a-Service“, што значи да купац добија техничку подршку, ажурирања шаблона и чак инфраструктуру за масовно слање порука. Цена може варирати од неколико десетина до неколико стотина долара, у зависности од сложености и циљане институције. Неке верзије омогућавају и аутоматско заобилажење двофакторске аутентификације путем техника пресретања сесије.

Последице фишинг напада могу бити озбиљне: крађа новца са банковних рачуна, преузимање корпоративних налога, покретање ransomware напада или даља продаја украдених акредитива на илегалним тржиштима. За компаније, једна компромитована е-пошта може довести до Business Email Compromise (BEC) преваре и великих финансијских губитака. Због тога се заштита од фишинга заснива на комбинацији техничких и организационих мера — редовна едукација запослених, примена вишефакторске аутентификације, филтрирање е-поште, као и праћење потенцијалних злоупотреба података. Иако су фишинг комплети технички релативно једноставни, њихова доступност и лакоћа употребе чине их једним од најопаснијих и најраспрострањенијих алата савременог сајбер криминала.

Према најновијим подацима, на глобалном нивоу сваког дана буде послато 3,4 милијарде злонамерних емаилова, што чини око 1,2% укупног глобалног саобраћаја емаилова. У 2024. и 2025. години, број фишинг напада и даље је у порасту, а нове методе

.

као што су СМС (смс-инг), QR кодови и напади који користе вештачку интелигенцију значајно повећавају ризик од успешног напада[133].

Према извештају *Anti-Phishing Working Group - APWG* за трећи квартал 2024. године, укупно је забележено 932.923 фишинг напада, а у четвртом кварталу исте године број је износио 989.123. У првом кварталу 2025. године било је забележено 1.003.924 напада, док је у другом кварталу 2025. године овај број порастао на 1.130.393. Напади су у великој мери циклични, што значи да се интензивирају током одређених периода, али се обим и број напада одржавају на високом нивоу током целе године. У првих пет недеља 2025. године, број инцидената у Сједињеним Америчким Државама повећао се за 149% у поређењу са истим периодом у 2024. години. Фишинг и даље остаје највећи узрок финансијских губитака за предузећа, а најновији извештаји указују на огромне износе које нападачи могу да однесе, посебно када су мета високо позиционирани менаџери и извршни директори[134].

Иако је електронска пошта и даље најчешћи канал за фишинг нападе, нападачи су све чешће почели да користе нове канале као што су СМС и QR кодови како би заобишли стандардне безбедносне механизме који се користе за откривање фишинг напада. У трећем кварталу 2025. године, Mimecast је детектовао више од 716.000 јединствених злонамерних QR кодова, што је представљало повећање од 13% у односу на претходни квартал. Поред тога, мобилни фишинг наставља да расте, а СМС напади забележили су пораст од 35% у трећем кварталу 2025. године. Напади који користе вештачку интелигенцију постали су све чешћи, јер ова технологија омогућава нападачима да у врло кратком временском периоду креирају убедљиве фишинг кампање. Док је раније време потребно за израду фишинг кампање било око 16 сати, коришћењем великих језичких модела (LLM) време је смањено на само пет минута, што значајно повећава ефикасност напада[135].

[133] Control D Blog – Phishing Statistics & Industry Trends. (2025). (преузето 20.02.2026), https://controld.com/blog/phishing-statistics-industry-trends/
[134] Anti-Phishing Working Group. (2024). *Phishing attack trends report 2024–2025*. Anti-Phishing Working Group. (преузето 17.02.2026), https://apwg.org
[135] ibid

.

Циљеви фишинг напада остају углавном платформе које користе акредитиве, као што су CaaC (Software-as-a-Service) пријаве, друштвене мреже и платформе за плаћање. Нападачи траже начине да добију приступ једној групи акредитива који им омогућавају приступ већем броју система. У извештају APWG за трећи квартал 2025. године, највише напада било је усмерено на CaaC и вебмаил платформе (21,2%), следе друштвене мреже (14,6%) и финансијске институције (13,2%). Нападачи су све више заинтересовани за нападе на малопродају, инжењерске компаније и осигуравајуће компаније, где се такође бележи раст броја напада[136]. Према подацима из FBI IC3 извештаја за 2024. годину, откривање и садржај напада који почињу фишингом имају озбиљне последице по организацију, са просечним трошковима од 1,2 милиона долара више ако напад није препознат до 200. дана. Примећено је да предузећа која имају активне безбедносне програме и редовно обучене запослене пријављују фишинг нападе четири пута чешће него предузећа која не спроводе редовну обуку[137].

### 4.5.3. Zero-day експлоатације

Zero-day експлоатације представљају један од најопаснијих и најсофистицираних облика сајбер напада јер циљају безбедносне рањивости у софтверу које још увек нису познате произвођачу или за које не постоји доступна закрпа. Назив „zero-day“ означава да компанија има „нула дана“ да реагује, односно да није имала прилику да исправи пропуст пре него што је он злоупотребљен. Управо због те временске предности нападача, овакве експлоатације имају висок степен успешности и представљају изузетно вредан ресурс у сајбер криминалном и шпијунском окружењу.

Zero-day рањивост настаје услед програмске грешке или пропуста у дизајну софтвера. Када истраживач безбедности или злонамерни актер открије такав пропуст, могућа су два сценарија: рањивост се одговорно пријављује произвођачу ради израде закрпе, или се продаје и користи у тајним нападима. Уколико се одлучи за злоупотребу, нападач развија експлоатацију — посебан код који омогућава искоришћавање рањивости

[136] Anti-Phishing Working Group. (2024). *Phishing attack trends report 2024–2025*. Anti-Phishing Working Group. (преузето 21.02.2026) https://apwg.org
[137] FBI Internet Crime Complaint Center (IC3) – 2024 Annual Report**.** (преузето 21.02.2026) https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

.

за неовлашћен приступ систему, извршавање злонамерног кода, преузимање контроле над уређајем или крађу података.

Посебна опасност zero-day експлоатација лежи у чињеници да традиционални антивирусни и заштитни системи често не могу да их препознају, јер не постоји претходно дефинисана сигнатура или познати образац понашања. Напади могу остати непримећени дужи временски период, што омогућава нападачима да прикупљају осетљиве информације, поставе додатни злонамерни софтвер или припреме терен за касније нападе, као што је ransomware.

Zero-day експлоатације су посебно тражене на илегалним тржиштима јер омогућавају пробијање чак и добро заштићених система. Њихова цена може достићи десетине или стотине хиљада долара, у зависности од тога који софтвер или оперативни систем је погођен и колико је рањивост критична. Често су мета велики технолошки системи, корпоративне мреже, финансијске институције и владине агенције. Поред криминалних група, zero-day експлоатације користе и напредне упорне претње (APT), које су често повезане са државним актерима и сајбер шпијунажом.

Историја бележи бројне случајеве злоупотребе zero-day рањивости у широко коришћеном софтверу, укључујући оперативне системе, веб-прегледаче и серверске платформе. На пример, више пута су откривене критичне рањивости у производима компаније Microsoft које су омогућавале даљинско извршавање кода пре него што је објављена безбедносна исправка. Слични случајеви забележени су и код производа компаније Apple, где су zero-day пропусти коришћени за компромитацију мобилних уређаја.

Последице zero-day напада могу бити изузетно озбиљне: крађа поверљивих података, индустријска шпијунажа, саботажа инфраструктуре или масовне кампање дистрибуције малвера. Пошто не постоји одмах доступна закрпа, одбрана се заснива на примени напредних безбедносних механизама као што су системи за детекцију аномалија, сегментација мреже, принцип најмањих привилегија и континуирано праћење активности у систему.

.

Период од 2021. до 2024. године представља кључну фазу у еволуцији zero-day експлоатације, како у погледу обима, тако и у погледу брзине и стратешког усмерења нападача. Подаци које су објавиле водеће организације за обавештајне податке о претњама, пре свега Google Threat Intelligence Group[138] и Mandiant[139], показују да се глобални број активно искоришћених zero-day рањивости стабилизовао на значајно вишем нивоу него у претходној деценији. Током 2021. године забележено је 106 zero-day експлоатација у дивљини, што представља историјски максимум. Иако је 2022. године број пао на 62, већ 2023. године регистровано је 97 случајева, док је у 2024. години евидентирано 75 активно злоупотребљених zero-day рањивости. Ови подаци указују да скок из 2021. године није био статистичка аномалија, већ почетак „нове нормале“ у којој се између 60 и 100 zero-day експлоатација годишње може сматрати очекиваним нивоом активности. Просечна вредност за анализирани четворогодишњи период износи око 85 случајева годишње, што представља структурно повећање у односу на раније циклусе[140].

Посебно забрињавајући тренд представља драстично скраћивање времена између јавног откривања рањивости и њене злоупотребе. Према анализама компаније CyberMindr, просечно „време до експлоатације“ у 2024. години износило је приближно пет дана, док је у претходним годинама тај период износио више од 30 дана. Ова динамика указује на висок степен аутоматизације и оперативне зрелости нападача, који све чешће користе алате за брзу реверзну анализу закрпа и развој функционалних експлоата у року од неколико дана. Последица овог убрзања јесте да традиционални месечни циклуси управљања закрпама више не пружају довољан ниво заштите, јер нападачи могу започети масовну злоупотребу пре него што већина организација имплементира безбедносне исправке[141].

У анализи статистике неопходно је правити разлику између zero-day и N-day експлоатације. Zero-day подразумева злоупотребу рањивости која је непозната добављачу

[138] Google Threat Intelligence Group. (2025). *Hello 0-days, my old friend: A 2024 zero-day exploitation analysis*. Google Cloud Blog. (преузето 22.02.2026) https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends
[139] Mandiant. (2023). *M-Trends 2023 special report*. (преузето 22.02.2026) https://www.mandiant.com/resources/m-trends-2023
[140] Khalil, M. (2025, September 6). *Zero-Day Exploit Statistics: The 2025 threat report for defenders.* DeepStrike. (преузето 23.02.2026) https://deepstrike.io/blogs/zero-day-exploit-statistics-2025/
[141] ibid

.

у тренутку напада и за коју не постоји закрпа, док N-day означава експлоатацију већ познате рањивости за коју је исправка доступна, али није примењена. Иако zero-day напади представљају технички најсложенију категорију, значајан број компромитација и даље произилази из кашњења у имплементацији закрпа, што указује да проблем безбедности није искључиво технички, већ и организациони[142].

Још једна кључна карактеристика савременог периода јесте стратешки заокрет нападача ка enterprise инфраструктури. Према извештају *M-Trends 2025* компаније Mandiant, експлоати су пету годину заредом били најчешћи иницијални вектор компромитације, чинећи 33% истражених упада. Посебно су погођени уређаји на рубу мреже, као што су VPN системи и заштитни зидови, који су директно изложени интернету, поседују високе привилегије и омогућавају широк приступ унутрашњој мрежи након компромитације. Овај тренд представља одступање од ранијег фокуса на крајње корисничке уређаје, што се може објаснити чињеницом да су мобилне и десктоп платформе у међувремену значајно ојачале своје безбедносне механизме[143].

Подаци о најпогођенијим добављачима додатно илуструју овај заокрет. Према *Google Threat Intelligence Group*, у 2024. години највише zero-day случајева забележено је код Мајкрософта (26) и Гугла (11), али је посебно значајан податак да је чак 18 различитих enterprise добављача било мета, укључујући Ivanti. Анализа KEV каталога који одржава Cybersecurity and Infrastructure Security Agency показује да је током 2024. године додато 186 активно експлоатисаних рањивости, при чему је Мајкрософт имао 36 уноса, Иванти 11, Гугл 9, а компаније Adobe и Епл по 7. Ови подаци потврђују да нападачи све чешће усмеравају ресурсе ка инфраструктурним производима који омогућавају висок утицај уз релативно једну тачку компромитације[144].

Екосистем zero-day експлоатације обухвата различите актере, од националних држава до организованих криминалних група. Историјски пример комплексне zero-day операције представља Stuxnet, који је користио четири Windows zero-day рањивости у

[142] Ibid
[143] Ibid
[144] Khalil, M. (2025, September 6). *Zero-Day Exploit Statistics: The 2025 threat report for defenders.* (преузето 23.02.2026) DeepStrike. https://deepstrike.io/blogs/zero-day-exploit-statistics-2025/

.

геополитичком контексту. Савремени пример комерцијално мотивисане злоупотребе јесте кампања групе Clop, која је 2023. године искористила zero-day у MOVEit систему за масовну крађу података. Паралелно са тим, формирало се и глобално тржиште рањивости, где посредничке компаније попут Crowdfense откупљују експлоате по ценама које достижу више милиона долара, нарочито када је реч о мобилним платформама и zero-click нападима[145].

Сумирајући статистичке показатеље, могу се издвојити три фундаментална тренда: прво, обим zero-day експлоатације остаје стабилно висок; друго, време до оперативне злоупотребе се драматично скратило; треће, стратешки фокус нападача померен је ка enterprise инфраструктури и уређајима на рубу мреже. У таквом окружењу, концепт потпуне превенције постаје нереалан циљ, јер је рањивост по дефиницији непозната у тренутку злоупотребе. Стога се савремена стратегија мора заснивати на претпоставци компромиса, континуираној видљивости, сегментацији мреже, минимизацији привилегија и брзом обуздавању инцидената. Zero-day експлоатација више није изоловани феномен резервисан за државне операције, већ структурни елемент глобалног сајбер конфликта, што захтева системски приступ заснован на отпорности као централном безбедносном принципу.

У савременом дигиталном окружењу, zero-day експлоатације представљају врхунац техничке софистицираности у сајбер претњама. Њихова реткост, вредност и ефикасност чине их кључним инструментом у високоризичним нападима, због чега организације морају развијати проактивне стратегије безбедности и реаговања како би ублажиле потенцијалне последице оваквих напада.

### 4.5.4. Украдени акредитиви (корисничка имена и лозинке) - Credential Theft

Листе украдених акредитива, односно комбинације корисничких имена и лозинки, представљају једну од највреднијих и најчешће тргованих „роба“ на Dark Web платформама. За разлику од сложених техничких експлоатација, злоупотреба акредитива је релативно једноставна, али изузетно ефикасна, јер омогућава нападачу да се представи као легитиман корисник и заобиђе многе безбедносне механизме. До крађе акредитива се

[145] Ibid

.

најчешће долази путем phishing напада, Malware-а који бележи притиске тастера (keylogger) и услед пробоја база података компаније. Једном када дође до великог цурења података, милиони комбинација корисничких имена и лозинки могу се појавити на илегалним форумима или маркетима. Познат пример је цурење података са платформе LinkedIn 2021. године, када су стотине милиона корисничких записа постале доступне на илегалним тржиштима, што је омогућило циљане преваре и нападе

Једном када дођу до приступних података, нападачи могу на више начина злоупотребити добијене податке. Најчешћи је такозвани „credential stuffing“ — техника у којој нападачи аутоматски тестирају украдене комбинације на различитим сервисима, ослањајући се на чињеницу да многи корисници користе исту лозинку на више налога. Успешна пријава омогућава преузимање налога, приступ финансијским средствима, крађу података или даљу компромитацију система.

Украдени акредитиви имају и тржишну вредност. На Dark Web платформама цена појединачног налога може бити релативно ниска, али приступ корпоративној е-пошти, администраторским налозима или финансијским сервисима може достићи знатно већу цену. Посебно су вредни приступи који омогућавају улазак у интерне мреже компанија, јер могу послужити као почетна тачка за ransomware нападе или индустријску шпијунажу.

За компаније, последице могу бити озбиљне. Једна компромитована лозинка може омогућити нападачу да приступи осетљивим документима, базама података клијената или финансијским системима. Уколико организација нема вишефакторску аутентификацију (MFA), посебно су рањиве јер једна украдена лозинка може омогућити потпуни приступ систему. Поред директних финансијских губитака, последице укључују и нарушавање репутације, губитак поверења клијената и потенцијалне правне санкције.

Заштита од злоупотребе украдених акредитива заснива се на више нивоа безбедности: коришћењу јединствених и сложених лозинки, примену вишефакторске аутентификације, редовно праћење сумњивих пријава, као и коришћење система за откривање аномалија. Такође, едукација корисника о опасностима фишинга и важности безбедног управљања лозинкама игра кључну улогу.

.

У савременом дигиталном окружењу, украдени акредитиви представљају један од најједноставнијих, али и најефикаснијих начина за покретање сложених сајбер напада. Њихова доступност на илегалним тржиштима и лакоћа злоупотребе чине их централним елементом многих облика сајбер криминала, од финансијских превара до масовних ransomware кампања.

Према извештају Flashpoint – Global Threat Intelligence Report 2025[146], више од 3,2 милијарде акредитива (корисничка имена и лозинке) је компромитовано током 2024. године, што представља раст од око 33% у односу на 2023. Украдени подаци доминирају илегалним тржиштима и користе се у различитим криминалним кампањама, укључујући ransomware и друге типове малвера. Током прва два месеца 2025. године већ је украдено преко 200 милиона акредитива. Од укупно 3,2 милијарде украдених акредитива у 2024. години, чак 75% (2,1 милијарда) потиче од деловања *infostealer* малвера — нових варијанти старих претњи које су заразиле више од 23 милиона уређаја широм света. Једноставност, ефикасност, широка доступност и ниски трошкови инфостилера довели су до тога да постану примарни вектор за ransomware нападе и велике пропусте у подацима које организације морају активно пратити у 2025. години.

Годишњи извештај лабораторије FortiGuard Labs – 2025 Global Threat Landscape Report[147] потврђује драматичан раст претње инфостилер малвера. Извештај, који анализира активности сајбер-криминала током 2024. године, наводи да је претња инфостилер малвера порасла за чак 500% у периоду од 12 месеци. Према подацима извештаја, 1,7 милијарди украдених лозинки доступно је на криминалним тржиштима на дарк вебу. Сајбер-криминалци укупно имају приступ више од 100 милијарди компромитованих налога на подземним форумима, што представља пораст од 42% у односу на претходну годину. Извештај упозорава да су групе као што су BestCombo, BloddyMery и ValidMail специјализоване за паковање украдених података у такозване

[146] Flashpoint. (2025). *Flashpoint 2025 global threat intelligence report: Stay ahead of emerging threats*. Flashpoint. (преузето 25.02.2026.) https://flashpoint.io/resources/report/flashpoint-2025-global-threat-intelligence-gtir/

[147] FortiGuard Labs. (2025). *2025 global threat landscape report*. Fortinet. (преузето 25.02.2026.) https://filestore.fortinet.com/fortiguard/2025_Global_Threat_Landscape_Report.pdf

.

„combo листе“, које се користе за аутоматизоване credential-stuffing нападе, што доводи до повећаног броја преузимања налога, финансијских превара и корпоративне шпијунаже.

Према анализи компаније Kaspersky, која је обухватила фишинг и scam кампање од јануара до септембра 2025. године, чак 88,5% напада било је усмерено на крађу акредитива за онлајн налоге. Додатних 9,5% напада циљало је личне податке (име, адреса, датум рођења), док је 2% напада било усмерено на податке банкарских картица. У региону Блиског истока забележено је више од 47 милиона кликнутих фишинг линкова у периоду од новембра 2024. до октобра 2025. године — сви су откривени и блокирани од стране Kaspersky решења. Ипак, како не користе сви корисници заштитна решења, фишинг и даље остаје једна од најраспрострањенијих сајбер претњи. Истраживање показује да већина фишинг страница шаље украдене податке путем е-поште, Telegram ботова или панела под контролом нападача, пре него што подаци доспеју на подземна тржишта. Украдени акредитиви се ретко користе само једном — често се консолидују у „data dump“ скупове и продају по ценама од већ 50 долара. Према *Kaspersky Digital Footprint Intelligence* подацима, просечне цене украдених података у 2025. години износиле су:

- 0,90 USD – налози за глобалне интернет портале
- 105 USD – крипто платформе
- 350 USD – приступ онлајн банкама
- око 15 USD – лични документи (пасоши, личне карте) [148]

Цена зависи од старости налога, стања на рачуну, повезаних начина плаћања и безбедносних подешавања. Како се скупови података комбинују и обогаћују, нападачи могу креирати детаљне дигиталне профиле жртава, што омогућава циљане нападе на руководиоце, финансијско особље, ИТ администраторе или појединце са вредном имовином. Како је изјавила Олга Алтухова, старији аналитичар веб садржаја у Kaspersky-ју: прикупљени логини, лозинке, бројеви телефона и лични подаци се агрегирају, проверавају и препродају, понекад годинама након првобитне крађе. У комбинацији са

[148] Kaspersky. (2025). *Kaspersky reports nearly 900 million phishing attempts in 2024 as cyber threats increase*. (преузето 26.02.2026.) https://www2.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase

.

новим информацијама, чак и стари акредитиви могу омогућити преузимање налога и циљане нападе[149].

### 4.5.5. Ботнети и DDoS услуге за изнајмљивање

Ботнети и DDoS услуге за изнајмљивање представљају један од најраспрострањенијих облика „сајбер напада као услуге“ који се нуди на Dark Web тржиштима. Ови алати омогућавају нападачима да релативно лако изазову прекид рада веб-сајтова, онлајн сервиса или читавих мрежа, без потребе за напредним техничким знањем.

Ботнет је мрежа заражених уређаја — рачунара, сервера, паметних телефона или IoT уређаја (нпр. паметне камере, рутери) — који су компромитовани злонамерним софтвером и којима нападач управља на даљину. Власници тих уређаја најчешће нису ни свесни да је њихов систем део ботнета. Централни сервер или командно-контролна инфраструктура омогућава нападачу да истовремено управља хиљадама или милионима заражених уређаја. Када се ботнет активира ради DDoS (Distributed Denial of Service) напада, сви заражени уређаји истовремено шаљу огромну количину захтева ка одређеном серверу или веб-сајту. Циљ је да се систем преоптерети саобраћајем и постане недоступан легитимним корисницима. Последице могу укључивати привремени или потпуни прекид пословања, финансијске губитке и нарушавање репутације компаније.

На Dark Web-у се ове услуге често нуде под називима као што су „DDoS-for-hire“ или „booter/stresser“ сервиси. Купац може изабрати трајање напада (нпр. један сат, један дан), интензитет саобраћаја и тип напада (HTTP flood, UDP flood, SYN flood и сл.). Цена варира, али основни напади могу коштати релативно мало, што додатно повећава њихову доступност. Оваква комерцијализација омогућава чак и појединцима без техничке стручности да изведу напад на конкурента, компанију или институцију.

Историјски гледано, један од најпознатијих ботнета био је Mirai, који је 2016. године искористио рањивости IoT уређаја и извео масовне DDoS нападе који су привремено онемогућили приступ бројним популарним интернет сервисима. Овај случај

[149] Ibid

.

је показао колико ботнети могу бити деструктивни када обухвате велики број повезаних уређаја.

Поред финансијске изнуде (где нападачи траже новац да би зауставили напад), DDoS напади се користе и као средство саботаже, политичког притиска или скретања пажње док се паралелно спроводи неки други тип напада, као што је крађа података. У неким случајевима, DDoS служи као „димна завеса“ за сложеније операције упада у систем. Заштита од ботнета и DDoS напада подразумева примену напредних система за филтрирање саобраћаја, коришћење услуга за ублажавање DDoS напада (DDoS mitigation services), редовно ажурирање уређаја и примену безбедносних конфигурација, посебно код IoT опреме. Такође је важно пратити необичне обрасце саобраћаја и имати план реаговања у случају инцидента. Ботнети и DDoS услуге за изнајмљивање представљају пример како је сајбер криминал постао индустријализован — напади су доступни „на клик“, по релативно ниској цени, а њихов утицај може бити изузетно штетан по пословање и стабилност дигиталне инфраструктуре.

У 2024. години, глобално је регистровано око 6,6 милиона DDoS напада, што је пораст од 108% у односу на претходну годину[150]. Средња величина ботнета у овом периоду износила је око 38.000 уређаја по ботнету, док су неки од највећих ботнета обухватали десетине милиона заражених уређаја. Напади су били усмерени на различите индустрије, са највећим ударом на технолошке провајдере, телекомуникације, финансијски сектор, као и на интернетску инфраструктуру. Типови напада укључивали су обичне волуметријске нападе, сложене HTTP и DNS нападе, SYN flood, UDP и ICMP нападе, као и комбинације више вектора који су чинили нападе тешко детектованим и блокираним[151].

Наредне године, 2025, забележен је драматичан раст DDoS активности. У првом кварталу, Cloudflare је детектовао 20,5 милиона напада, што је повећање од 358% у односу на исти период 2024. године[152]. Највећи напад у јуну 2025. достигао је 7,3 Tbps, покренут

[150] StormWall. (2024). *Annual DDoS Report 2024*. (преузето 26.02.2026.) https://stormwall.com
[151] DeepStrike. (2024). *DDoS Attack Statistics*. (преузето 25.02.2026.)https://deepstrike.io/blog/ddos-attack-statistics
[152] Cloudflare. (2025). *Cloudflare DDoS Threat Report 2025*. (преузето 25.02.2026.) https://cloudflare.com

.

од великог ботнета са више од 120.000 инфицираних уређаја[153]. Током трећег квартала 2025, ботнет Аисуру са 1–4 милиона заражених уређаја спровео је хиперволуметријске нападе који су прелазили 1 Tbps и 1 Bpps, са просечних 14 хиперволуметријских напада дневно и врхунцима од 29,7 Tbps и 14,1 Bpps[154].

Ботнети су током овог периода све више користили IoT уређаје (рутере, камере, телевизоре) као примарне мете за компромитацију. Велики ботнети омогућавали су извођење напада који су паралисали мрежну инфраструктуру великих компанија и чак изазивали колатералне поремећаје интернета у целом региону[155]. Напади су били комбиновани, са више вектора (SYN flood, DNS amplification, HTTP flood, UDP flood), а AI-powered DDoS напади омогућавали су аутоматизовано прилагођавање интензитета и трајања напада у реалном времену.

Географски, Сједињене Америчке Државе су биле најчешћа мета у 2024. години (14,3% свих напада), праћене Кином (12,8%) и Индијом (10,2%)[156]. У 2025, повећан је удео Азијских земаља као извора напада, са Индонезијом на првом месту, а други велики извори били су Бангладеш, Еквадор и Аргентина[157].

Највише нападнуте индустрије у 2024. били су финансијски сектор (22%), влада (19%), телекомуникације (16%), забавни сектор (14%) и малопродаја (12%)[158]. У 2025, осим телекомуникација и финансија, компаније које се баве генеративном вештачком интелигенцијом, аутомобилска индустрија, рударска и минерална индустрија бележиле су пораст DDoS активности за више стотина процената у односу на претходну годину[159].

---

[153] Tom's Hardware. (2025). *Report on Record-Breaking DDoS Attacks 2025*. (преузето 07.03.2026.) https://tomshardware.com
[154] Cloudflare. (2025). *Aisuru Botnet Attack Analysis 2025*. (преузето 08.03.2026.) https://blog.cloudflare.com
[155] Krebs on Security. (2025). *Collateral Internet Disruptions by Botnets*. (преузето 08.03.2026.) https://krebsonsecurity.com
[156] StormWall. (2024). *Annual DDoS Report 2024*. (преузето 09.03.2026.) https://stormwall.com
[157] DeepStrike. (2025). *Geography of DDoS Attacks 2025*. (преузето 09.03.2026.) https://deepstrike.io/blog/ddos-attack-statistics
[158] StormWall. (2024). *Annual DDoS Report 2024*. (преузето 10.03.2026.) https://stormwall.com
[159] Cloudflare. (2025). *Cloudflare DDoS Threat Report 2025*. (преузето 10.03.2026.) https://cloudflare.com

.

### 4.5.6. Алати засновани на Dark AI ( Мрачна вештачка интелигенција)

Мрачна вештачка интелигенција (Dark AI) представља примену AI технологије у злонамерне или незаконите сврхе. За разлику од легитимних система, ови алати немају безбедносне механизме који спречавају генерисање фишинг порука, злонамерног кода, дипфејкова, ransomware-а или аутоматизованог социјалног инжењеринга[160].

Од масовног усвајања генеративне AI технологије 2023. године, глобални сајбер напади порасли су за око 30%. Dark AI омогућава: повећање броја хакера без техничког знања, масовну аутоматизацију фишинга, персонализоване ransomware нападе, генерисање еволутивног малвера, креирање дипфејкова и клонирање гласа као и заобилажење безбедносних система[161]. Током последње деценије, Dark Web се трансформисао од нишних форума до сложених тржишта која омогућавају широк спектар илегалних активности, а ова промена је сада појачана алатима вођеним вештачком интелигенцијом, дизајнираним са злонамерним намерама, као што су WormGPT**,** FraudGPT и DarkBERT, на које су медији недавно указали[162].

Алати мрачне AI имају исти принцип рада као и легитипни системи вештачке инталигенције попу ChatGPT, Google Gemini, али без безбедносних ограничења и етичких механизама контроле. Рад  Dark AI се може објаснити кроз неколико логички повезаних фаза:

**1. Прикупљање података** - Модели тамне вештачке интелигенције захтевају велике скупове података  украдени из база података,  преузети са дарк веб форума, прикупљени са друштвених мрежа и добијени из претходних сајбер напада. Циљ је изградња скупа података који омогућава: креирање уверљивих фишинг порука, писање злонамерног кода, анализу рањивости иперсонализацију напада.

[160] Srėbaliūtė, A. (2025, December 19). *What is dark AI and how it changes cyber-attacks*. NordLayer. (преузето 15.03.2026.) https://nordlayer.com/blog/what-is-dark-ai/
[161] Ibid
[162] Savard, J. (2025, February 6). *AI without ethics: A crash course on the dark web and its new tools*. IRONSCALES. (преузето 15.03.2026.) https://ironscales.com/blog/ai-without-ethics-a-crash-course-on-the-dark-web-and-its-tools

.

**2.Обука или фино подешавање модела -** Нападачи користе open-source LLM моделе (нпр. GPT-J), модификоване верзије постојећих система или врше „jailbreaking“ легитимних алата. Модел се поново обучава (retraining) или фино подешава (fine-tuning), како би генерисао садржај без ограничења (малвер, ransomware код, фишинг текстове, социјални инжењеринг сценарије).

**3.Аутоматизација извршења напада** - Када је модел спреман, он омогућава: масовно генерисање фишинг имејлова, креирање злонамерног софтвера, генерисање лажних веб страница, израду deepfake садржаја, аутоматизовану комуникацију са жртвама (чат-ботови за социјални инжењеринг). Ово драматично повећава брзину и обим напада.

**4. Адаптација и избегавање детекције -**Напредни Dark AI системи могу: анализирати реакције жртава, тестирати безбедносне системе, мењати шаблоне порука како би избегли филтере идинамички прилагођавати злонамерни код. Ова способност адаптације чини их тежим за откривање у односу на традиционалне претње.

**5. Континуирано унапређење-** Успешни напади се користе као повратна информација (feedback loop): успешни шаблони се поново уносе у модел, стратегије са већом стопом успеха се оптимизују, а неуспешне методе се елиминишу. Тако свака наредна кампања постаје ефикаснија од претходне[163].

Средином 2023. године појављује се WormGPT, заснован на моделу GPT-J који је развила организација EleutherAI 2021. године. GPT-J је open-source модел са шест милијарди параметара, сличан GPT-3 архитектури. WormGPT је био доступан путем претплате на дарк вебу и омогућавао је заобилажење безбедносних механизама (тзв. „LLM jailbreaking“). Према анализи компаније SlashNext из јула 2023, алат је коришћен пре свега за BEC (Business Email Compromise) нападе, односно компромитовање пословне комуникације. Наводно је обучен на подацима повезаним са злонамерним софтвером[164].

[163] Srėbaliūtė, A. (2025, December 19). *What is dark AI and how it changes cyber-attacks*. NordLayer. (преузето 16.03.2026.) https://nordlayer.com/blog/what-is-dark-ai/

[164] Poireault, K. (2023, August 10). *The dark side of generative AI: Five malicious LLMs found on the dark web*. Infosecurity Europe. (преузето 15.03.2026.) https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/generative-ai-dark-web-bots.html

.

Након повлачења WormGPT-а, 22. јула 2023. године појављује се FraudGPT (познат и као FraudBot). Рекламиран је на дарк вебу и Телеграм каналима као „бот без ограничења“. Безбедносне компаније Cybersixgill и Netenrich анализирале су његове активности. Претплата се кретала од 200 долара месечно до 1700 долара годишње, уз тврдње о више од 3000 продаја. Док је WormGPT био фокусиран на масовни фишинг, FraudGPT је наводно омогућавао сложеније и дугорочне нападе, укључујући ransomware кампање[165]. Паралелно се рекламира и DarkBard, варијанта заснована на Google Bard технологији. С друге стране, DarkBERT развила је компанија S2W Security. За разлику од претходних алата, DarkBERT је иницијално креиран у истраживачке и одбрамбене сврхе, али постоје докази о његовој злоупотреби у криминалним активностима[166].

Крајем јула 2023. промовисан је WolfGPT као алтернатива ChatGPT-у са злонамерном наменом, наводно развијен у Python-у, са могућностима креирања криптографског малвера и напредног фишинга. Дана 31. јула 2023, компанија FalconFeeds пријавила је појаву алата XXXGPT, намењеног за ботнете, RAT-ове, банкарске малвер комплете и крађу података[167]. Француски стартап Mithril Security је у јулу 2023. креирао PoisonGPT како би демонстрирао могућност „тровања“ open-source LLM модела. Користили су ROME (Rank-One Model Editing) технику представљену на конференцији NeurIPS 2022. У модел су уметнуте лажне тврдње (нпр. да се Ајфелова кула налази у Риму или да је Јурај Гагарин ходао по Месецу), а разлика у перформансама у односу на оригинални GPT-J била је свега 0,1% на ToxiGen бенчмарку. Модел је постављен на Hugging Face под називом сличним EleutherAI-у, како би се показала опасност од замене легитимних модела[168]. Ова врста тамног AI алата не напада људе — она напада друге AI алате убризгавањем злонамерних или обмањујућих података у AI материјал за обуку како би се овековечиле дезинформације, што резултира тиме да наизглед нормални AI модели пружају обмањујуће информације када се питају о одређеним темама[169].

[165] Ibid
[166] Ibid
[167] Ibid
[168] Ibid
[169] Gorman, B. (2025, September 16). *What is dark AI and how can you protect yourself?* Norton. (преузето 16.03.2026.) https://us.norton.com/blog/ai/dark-ai

.

Поред специјализованих алата као што су FraudGPT и DarkBERT, сајбер криминалци користе и легитимне open-source алате попут Nmap, Shodan, Metasploit и SQLMap за извиђање и искоришћавање рањивости. За само годину дана, помињања и продаја алата заснованих на вештачкој интелигенцији на Dark Web-у порасли су за преко 200%, преваре са преваром идентитета учетворостручиле су се, а 73% компанија широм света доживело је неки облик кршења података повезаног са вештачком интелигенцијом. Дистрибуција „злонамерних“ алата на Dark Web-у постаје све софистицираниja и инспирисана традиционалним моделима електронске трговине. На подземним форумима, описаним као „универзитет за сајбер криминалце“, откривено је преко 3.000 објава у којима се дискутује о томе како модификовати језичке моделе (LLM) за злонамерну употребу, уз дељење AI скрипти, примера и корак-по-корак водича. На тржиштима заснованим на претплати, алати попут FraudGPT-а изнајмљују се за 170 евра месечно или 1.500 евра годишње, док све-у-једном комплети прелазе 4.000 евра и укључују техничку подршку и ажурирања. Премијум приступ AI платформама као што је ChatGPT продаје се за 8 до 500 евра, а аутоматизоване услуге могу генерисати до 1.000 лажних налога дневно користећи украдене личне податке. Поред тога, ботови на платформама као што су Telegram и Discord промовишу ове алате кроз тест поруке, чинећи их лако доступним свима[170].

### 4.6. Прање новца путем криптовалута

Прање новца на дарк вебу представља сложен и вишеслојан процес прикривања незаконито стечених средстава како би она изгледала легитимно и могла да се несметано користе у легалним или даљим илегалним токовима. Сајбер криминалци користе комбинацију анонимних мрежа, криптовалута и специјализованих услуга како би онемогућили идентификацију стварног власника средстава.

Процес обично почиње стицањем незаконите добити. Најчешћи извори укључују ransomware нападе, где жртве плаћају откуп у криптовалути, финансијске преваре уз употребу украдених банковних података и кредитних картица, као и продају дроге, оружја или хакерских алата на Dark Web маркетима. Ова средства се најчешће примају у

[170] Tejedor, J. (2025, June 5). *A dangerous alliance: How AI is reshaping the dark web economy*. Telefonica Tech. (преузето 16.03.2026.) https://telefonicatech.com/en/blog/a-dangerous-alliance-how-ai-is-reshaping-the-dark-web-economy/

.

криптовалутама јер омогућавају висок степен псеудоанонимности. Следећа фаза је депоновање средстава у дигиталне новчанике. Криминалци пребацују незаконито стечену криптовалуту на нове адресе, често унутар приватних или офшор платформи које не спроводе строге провере идентитета. Блокчејн технологија јесте транспарентна, али трансакције су повезане са криптографским адресама, а не са именима и презименима, што значајно отежава идентификацију појединаца[171].

Након депоновања, долази фаза „слојевања“ (*layering*), чији је циљ замагљивање трага новца. У овој фази се користе такозвани миксери или тумблери – услуге које мешају криптовалуту једног корисника са средствима других корисника, а затим враћају „очишћене“ новчиће на нове адресе. На тај начин се прекида директна веза између оригиналне и коначне адресе. Средства се често деле на више мањих износа, шаљу на различите новчанике и више пута конвертују из једне криптовалуте у другу како би се додатно отежало праћење[172].

Системи за мешање криптовалута, као што су SmartMixer или Dark Wallet, дуго су били популарни међу актерима са дарк веба који траже анонимност. Dark Wallet су 2014. године креирали Амир Такаи и Коди Вилсон као алат отвореног кода за анонимизацију биткоин трансакција. Једна од његових кључних функција било је мешање новчића – комбиновање трансакција више корисника у једну сложену трансакцију. Корисник је могао да подели плаћање на више мањих делова или да одложи трансакцију, што је додатно компликовало анализу блокчејна. Због оваквог начина функционисања, спољним посматрачима је изузетно тешко да утврде ко је заиста извршио одређену трансакцију[173].

Последња фаза је интеграција средстава у легални систем. Након што се замагли траг порекла, средства се конвертују у фиат валуту преко централизованих или P2P крипто-берзи, често уз коришћење лажних идентитета или посредника. У неким случајевима, новац се користи за куповину робе и услуга које се касније препродају, чиме се ствара привид легалног прихода. Понекад се користе и такозвани „money mules“ –

[171] Sanctions.io. (2024, October 25). *How illicit actors launder money through crypto exchanges*. (преузето 17.03.2026.) https://www.sanctions.io/blog/how-illicit-actors-launder-money-through-crypto-exchanges
[172] Ibid
[173] Pideeco. (n.d.). *How do criminals launder their money using the Dark Web?* (преузето 17.03.2026.) https://pideeco.be/articles/dark-web-and-money-laundering/

.

појединци који, свесно или несвесно, пребацују средства преко својих рачуна како би прикрили стварне налогодавце[174].

Значајан проблем у борби против оваквих активности јесте чињеница да, иако су све блокчејн трансакције јавно забележене, идентификација особе иза одређене крипто-адресе захтева додатне истражне радње и међународну сарадњу. Комбинација анонимних мрежа, миксера, више новчаника и различитих криптовалута ствара комплексну структуру која отежава праћење токова новца. Прање новца на Dark Web- у тиме постаје кључни механизам одржавања сајбер криминалних активности. Оно омогућава криминалцима да профит од незаконитих радњи претворе у употребљива средства, истовремено повећавајући ризике за глобални финансијски систем и представљајући велики изазов за регулаторне и правосудне институције.

## 5. ОРГАНИЗАЦИЈА И СТРУКТУРА КРИМИНАЛНИХ МРЕЖА НА DARK WEB-У

### 5.1. Мрежа ћелија као модел организације криминалних активности на Dark Web-у

Мрежа ћелија (cell-based network / cellular structure) представља организациони модел у којем је криминална мрежа подељена на више малих, релативно аутономних јединица – ћелија. Свака ћелија функционише независно једна од друге и има строго дефинисан задатак, уз минималну размену информација, тако да њени чланови немају увид у целокупну структуру мреже. Овакав модел је првобитно развијен у контексту терористичких и обавештајних организација, где је служио као средство за заштиту целокупне структуре од инфилтрације и разбијања[175]. Са развојем дигиталних технологија и анонимизационих мрежа, овај модел је прилагођен и широко примењен у окружењу Dark Web-а, где се показао као изузетно ефикасан за организовање различитих облика криминала, укључујући трговину дрогом, сајбер криминал и финансијске преваре[176].

[174] Group-IB. (n.d.). *What are money mules? How cybercriminals launder funds*. (преузето 15.01.2026.) https://www.group-ib.com/blog/money-mules/
[175] Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, University of Pennsylvania Press, 2008.
[176] David Décary-Hétu & Judith Aldridge, "Cryptomarkets and the Future of Illicit Drug Markets", *International Journal of Drug Policy*, 2015.

.

Основна сврха овакве организације јесте смањење ризика од откривања и онемогућавање потпуне реконструкције криминалне мреже у случају компромитације појединих ћелија[177].

На Dark Web-у, ћелије су најчешће организоване према функционалном принципу, а не хијерархијски. То значи да свака ћелија обавља строго одређен задатак, као што су техничка подршка и одржавање инфраструктуре, набавка и производња нелегалне робе, дистрибуција и логистика, финансијске трансакције и прање новца или посредовање и комуникација са купцима. Чланови једне ћелије углавном немају директан контакт са другим ћелијама, већ комуницирају преко ограниченог броја посредника или „контактних тачака“, што додатно смањује могућност откривања целокупне мреже[178].

Једна од кључних карактеристика мреже ћелија јесте принцип ограниченог знања, према коме сваки учесник има приступ само оним информацијама које су неопходне за извршење његовог задатка. Овај принцип значајно отежава рад органа гоњења, јер чак и у случају хапшења појединих учесника није могуће лако идентификовати остале чланове или организаторе криминалне активности[179]. Поред тога, мрежа ћелија омогућава висок степен заменљивости учесника, што значи да уклањање једног члана или чак читаве ћелије не доводи до прекида криминалних активности. Нови учесници могу релативно брзо да преузму исту улогу, чиме се обезбеђује континуитет деловања криминалне мреже. Управо ова флексибилност и отпорност чине ћелијски модел посебно погодним за деловање у дигиталном окружењу дарквеба. Одсуство јасне централне хијерархије додатно отежава идентификацију вођа и организатора, јер се улоге често мењају, а координација се врши кроз привремене и анонимне комуникационе канале. Европске и међународне безбедносне институције указују да управо овакав облик организације представља један од главних изазова у сузбијању криминала на Dark Web-у, јер традиционалне методе разбијања криминалних група постају мање ефикасне[7].

У том смислу, мрежа ћелија представља кључни структурни елемент криминалних активности на Dark Web-у, који омогућава висок степен анонимности, оперативне

[177] United Nations Office on Drugs and Crime (UNODC), *Drug Trafficking on Dark Markets: How Cryptomarkets Are Changing the Global Drug Trade*, Vienna, 2020.
[178] Europol, *Dark Web Markets and the Threat to Europe*, The Hague, 2019.
[179] CounterCraft, *Profiling Adversaries: The Dark Web Threat Landscape*, 2021. (преузето 16.02.2026.) https://www.countercraft.eu/blog/dark-web-threat-landscape/

.

сигурности и дуготрајности криминалног деловања. Разумевање овог модела од суштинског је значаја за развој ефикасних стратегија превенције и репресије усмерених на савремене облике организованог криминала у дигиталном окружењу.

### 5.2. Организација криминалних мрежа на Dark Web –у

Криминалне мреже које делују на Dark Web-у представљају специфичан и савремен облик организованог криминала, чија се структура и начин функционисања значајно разликују од традиционалних криминалних организација. Њихова организација је превасходно условљена технолошким окружењем у ком делују, као и потребом за очувањем анонимности, флексибилности и отпорности на откривање од стране органа гоњења. Уместо класичних, строго хијерархијских модела, риминалне мреже на Dark Web-у најчешће функционишу као мрежне, децентрализоване структуре, које се састоје од више аутономних чворова (појединаца или мањих група) који су међусобно повезани заједничком интересима и циљевима, али без централне командне тачке[180].

Овакав вид децентрализоване структуре омогућава криминалним мрежама на Dark Web-у да смање ризик од потпуног разоткривања, јер хапшење или компромитација једног члана не доводи нужно до откривања целокупне мреже. Чланови ових структура најчешће поседују ограничено знање о другим учесницима и њиховим улогама, без увида у обим или коначну сврху предузетих активности, што додатно отежава реконструкцију криминалне активности у истражним поступцима[181]. Оваква организација одражава савремене теорије организованог криминала које указују на прелазак са вертикалних ка хоризонталним, флексибилним мрежама, прилагођеним глобализованом и дигитализованом окружењу[182].

Кључну карактеристику ових мрежа представља изразита подела улога и висок степен специјализације. Учесници криминалних активности обављају строго дефинисане функције, које могу укључивати управљање дигиталним платформама, техничку подршку,

[180] United Nations Office on Drugs and Crime (UNODC), *World Drug Report*, 2020. United Nations. (преузето 01.03.2026.) https://www.unodc.org/unodc/en/data-and-analysis/wdr2020.html
[181] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2023 Europol. (преузето 01.03.2026.) https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta
[182] Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.

.

посредовање између различитих актера, као и непосредно извршење кривичних дела. Ова подела рада доприноси већој ефикасности, али и смањењу индивидуалне кривичне одговорности, јер је тешко повезати једног појединца са целокупним криминалним подухватом[183]. У том контексту се све чешће јавља модел такозваног „криминалитета као услуге“, у оквиру којег појединци нуде специјализоване услуге другим криминалним актерима, без директног учешћа у самом кривичном делу[184].

Идентификација и позиционирање чланова унутар криминалних мрежа на Dark Web-у заснива се на псеудонимним дигиталним идентитетима, који су у потпуности одвојени од стварног идентитета појединца. Поверење се не гради на личним односима, већ на репутацији стеченој кроз историју активности, оцене и коментаре других корисника и доследност понашања унутар заједнице[185]. Репутација има кључну улогу у одржавању стабилности мреже, јер губитак поверења често резултира искључењем из заједнице и губитком приступа ресурсима.

Иако делују у нелегалном простору, криминалне мреже на Dark Web-у развијају сопствене механизме интерне регулације и контроле. Они укључују системе оцењивања, арбитражу у случају спорова и различите облике санкција за кршење утврђених правила. Ови механизми служе као замена за формалне правне институције и имају за циљ смањење ризика од преваре и унутрашњих конфликата[186]. Поред тога, значајан део криминалних активности одвија се у затвореним и селективним заједницама, доступним искључиво на основу позива или препоруке, што представља додатни слој заштите од инфилтрације органа гоњења.

Транснационални карактер ових мрежа представља још једну њихову значајну особину. Чланови криминалних заједница на Dark Web-у често потичу из различитих држава и делују у више јурисдикција истовремено, што значајно компликује кривично

[183] Leukfeldt, R., *Cybercrime and Social Ties*, Routledge, 2018.
[184] Europol, *Crime-as-a-Service: From Concept to Reality*, 2021.
[185] Holt, T. J., *Darknet Markets and the Economics of Online Crime*, Palgrave Macmillan, 2019.
[186] Décary-Hétu, D., & Quessy-Doré, O., „*Digital Reputation in a Criminal Context*“,Crime Science 6(1), Article 6, 2017. https://doi.org/10.1186/s40163-017-0068-z

.

гоњење и захтева висок ниво међународне сарадње[187]. Уз то, ове мреже показују изузетну способност адаптације, брзо мењајући инфраструктуру, платформе и начине комуникације у случају репресивних мера.

### 5.3. Процес извршења кривичних дела – фазе, улоге и дистрибуција задатака

Савремени облици организованог криминала све више се премештају у дигитално окружење, а посебно на Dark Web -у. Кључне карактеристике овог система су анонимност, специјализација улога и децентрализована мрежна организација. Сходно томе, процес извршења кривичних дела на дарквебу представља структуриран, фазно организован модел који укључује планирање, техничку припрему, инфраструктурну подршку, оперативну реализацију и прикривање трагова. Ове фазе су међусобно повезане и чине јединствену целину.

1. Фаза планирања и организације

У почетној фази дефинише се врста криминалне активности (трговина наркотицима, продаја украдених података, малвер услуге, фалсификована документа и сл.). Организатори процењују ризике, односно могућност инфилтрације, праћење трансакција, оперативна безбедности – OPSEC, као и правне ризике у различитим јурисдикцијама. Бира се одговарајућа платформа сходно постављеним циљевима и то може бити даркнет тржиште, форуми, приватни канали, прикупљају се и анализирају информације о конкурнцији, потенцијалним купцима и постојећим каналима комуникације и успостављају нови комуникациони канали. Криминалне групе често функционишу по принципу ћелијске структуре, где сваки члан има ограничен увид у целокупну активност, чиме се умањује ризик од откривања мреже. Ова фаза је кључна јер од квалитета припреме зависи успешност свих следећих корака. Недовољна припрема може довести до откривања мреже или неуспеха трансакција.

2. Фаза техничке припреме

Ова фаза подразумева обезбеђивање анонимности и сигурности комуникације:

[187] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), & Europol. (2019). *Drugs and the darknet: Perspectives for enforcement, research and policy*. Publications Office of the European Union.

.

- коришћење Tor мреже за приступ Dark web-u;
- употреба енкриптованих комуникационих сервиса (PGP енкрипција);
- отварање криптовалутних новчаника ( најчешће Bitcoin или Monero);
- постављање лажних идентитета (креирање псеудонима и „vendor“ налога).

Оперативна безбедност (OPSEC) представља кључни елемент – грешке у овој фази често доводе до идентификације починилаца. Најчешћи узрок разоткривања представља људски фактор и непридржавање безбедносних протокола

3. Фаза успостављања инфраструктуре

У зависности од врсте криминала, криминална група формира одговарајућу дигиталну или логистичку инфраструктуру. Инфраструктура може обухватати:

- креирање сопствене продавнице на даркнет маркету
- коришћење посредничких escrow система за задржавање уплата;
- изнајмљивање „bulletproof“ хостинг;
- постављаење сервера за контролу (C2 сервери);
- успостављање логистичких канала за физичку испоруку робе.

У случају сајбер криминала (нпр. ransomware), инфраструктура укључује сервере за комуникацију са жртвама, системе за аутоматизовано генерисање кључева за дешифровање и механизме за пријем криптовалутних уплата.

4. Фаза извршења

Ово је централна оперативна фаза у којој се реализује само кривично дело и чији садржај варира у зависноти од природе криминалне активности. Код трговине наркотицима то подразумева оглашавање производа, комуникација са купцима, примање уплата у криптовалутама, паковање и слање пошиљки. Код сајбер криминала, попут продаје података или хакерских услуга то може бити објављивање узорака („samples“), аукцијска продаја или директна понуда, извршење DDoS напада, инсталација малвера ransomware напади и изнуда. Све трансакције се углавном одвијају у криптовалутама ради

.

избегавања директне финансијске идентификације, а често се користе и escrow системи ради смањења ризика од преваре.

5. Фаза прикривања трагова и прања новца

Након извршења дела следи прикривање трагова:

- коришћење крипто-миксера;
- пребацивање средстава преко више новчаника;
- конверзија у фиат валуту путем нерегулисаних берзи или посредника;
- брисање комуникација и уништавање дигиталних трагова
- коришћење посредника („money mules“) за подизање новца.

Иако ове мере имају за циљ онемогућавање форензичког праћења, развој блокчејн анализе и међународна сарадња органа гоњења значајно повећавају шансе за идентификацију починилаца.

Криминалне активности на Dark Web-у показују висок степен специјализације. Најчешће улоге су:

1. **Администратори (Admin)** – управљају платформом, постављају правила и контролишу финансијске токове.
2. **Модератори** – надгледају комуникацију и решавају спорове.
3. **Продавци (Vendors)** – нуде незаконите производе или услуге.
4. **Добављачи** – обезбеђују физичку или дигиталну „робу“.
5. **Курири/логистика** – врше физичку или дигиталу испоруку .
6. **Перачи новца (Money mules)** – задужени за трансфер и конверзију средстава.
7. **Техничка подршка/програмери** – развијају малвер, одржавају инфраструктуру.
8. **Купци/клијенти** – крајњи корисници незаконитих услуга или производа[188].

[188] Пример хијејархијски постављене криминалне организације представља међународна криминална сајбер група „Infraud Ogranisation“, која је деловала од октобра 2010. године до фебруара 2018. године. За више информација видети: Infraud Organization. (n.d.). In *Wikipedia*. (преузето 01 16.02.2026.) https://en.wikipedia.org/wiki/Infraud_Organization.

.

Ова структура омогућава високу ефикасност и отпорност на интервенције органа гоњења. Dark Web криминал често функционише по принципу:

- **Децентрализације** – нема јасне хијерархије у многим групама.
- **Ћелијске структуре** – свака „ћелија“ извршава одређени сегмент активности.
- **Брза адаптација** након гашења платформи;
- **Међународне повезаности** – различити делови ланца (набавка, продаја, прање новца) могу се одвијати у различитим државама.

Ова структура омогућава лаку заменљивост учесника, ефикасну координацију комплексних криминалних активности и смањење ризика за појединце у систему. Управо комбинација анонимности, специјализације и глобалне повезаности чини Dark Web привлачним окружењем за савремене облике организованог криминала.

## 6. КРИМИНОЛОШКИ АСПЕКТИ ОТКРИВАЊА И ПРЕВЕНЦИЈЕ DARK WEB КРИМИНАЛА

### 6.1. Дигитална виктимологија и специфичности жртава на Dark Web-у

У савременом свету, који карактерише глобализација и дигитализација, већина наших личних, професионалних и друштвених интеракција одвија путем интернета. Иако дигиталне платформе нуде бројне предности, оне такође отварају врата новим облицима насиља, превара и злостављања. Дигитална виктимологија постала је значајна тема и представља нову грану виктимологије која се бави разумевањем постанка жртве криминалних активности на Dark Web-у, проучавањем начина доласка до виктимизације, последица  по жртву, начин на који надлежне институције могу пружити заштиту, као и пружањем подршке жртвама дигиталних злочина.

Дигитална виктимизација односи се на ситуације у којима особа постаје жртва кривичних или штетних радњи путем интернета и дигиталних платформи. Жртве може бити појединци, компаније и државне институције. Dark web је специфичан простор на интернету који омогућава анонимност и обезбеђује сигурно окружење за илегалне активности. Овде се често дешавају различите врсте дигиталне виктимизације, које укључују:

.

1. **Продају украдених података** – Лични подаци, бројеви кредитних картица, лозинке и други осетљиви подаци могу се куповати и продавати на dark web форумима, што ставља жртве у опасност од крађе идентитета и превара.
2. **Трговину илегалним садржајем** – Сексуални материјали, компромитујући снимци и други облици експлоатације могу се дистрибуирати путем dark web-a, што ствара ризик од уцењивања и сексуалног злостављања.
3. **Финансијске преваре и манипулацију криптовалутама** – Преваренти користе dark web за крађу финансијских средстава и манипулацију корисницима у вези с инвестицијама у криптовалуте.
4. **Ransomware напади** – Софтвери који закључавају податке жртве, тражећи откупнину за њихово враћање, често се дистрибуирају на dark web-у.
5. **Doxing** – Објављивање приватних информација жртве на интернету, с циљем срамоћења и додатног насиља, посебно ако је везано за друштвени статус жртве[189].

Иако се штета дешава у виртуелном простору, последице за жртве су стварне и могу бити дубоко емоционалне и психолошке:

- **Анксиозност и депресија** – Жртве дигиталне виктимизације често пате од менталних поремећаја, који могу бити последица сталне изложености насиљу на мрежи.
- **Страх од даљих злоупотреба** – Многи људи који су постали жртве на интернету живе у сталном страху од поновног напада или злоупотребе.
- **Друштвено повлачење** – Многе жртве се повуку из друштвеног живота, из страха да ће поново постати мета.
- **Губитак посла или личних односа** – Репутацијска штета која настаје услед јавног излагања или компромитујућих информација може озбиљно угрозити каријеру и личне односе.
- **Осећање стида и кривице** – Жртве често осећају да је њихова виктимизација изазвана њиховим понашањем, што доводи до осећања стида и кривице.

[189] "Victimology in Digital Age." *International Journal of Research in Social Sciences and Humanities*, RSI International. (преузето 12.03.2026.) https://rsisinternational.org/journals/ijriss/articles/victimology-in-digital-age/

.

- **Финансијски губици** – Жртве онлајн превара и крађе идентитета често доживљавају значајне финансијске проблеме, као што су губитак новца, крађа банковних података или чак дугови који могу резултирати озбиљним финансијским губицима и бити тешко надокнадиви.
- **Губитак поверења у технологију** – Многи људи који постану жртве сајбер криминала почињу се повлачити из дигиталног света, губећи поверење у технологију и њене могућности заштите[190].

Дигитална виктимологија указује на неколико кључних карактеристика које чине жртве у дигиталном окружењу посебно рањивим. Анонимност починиоца представља велики изазов, јер отежава идентификацију и процесуирање нападача. Поред тога, глобалност простора значи да нападач и жртва могу бити у различитим државама, што додатно компликује правну одговорност и међународну сарадњу. Брзина ширења штете је још један фактор, јер садржај на интернету може вирално да се прошири у неколико минута, чиме штета постаје експоненцијално већа. Такође, трајност дигиталног садржаја значи да је једном објављен садржај тешко потпуно уклонити са интернета, чиме жртва постаје трајно изложена, што води ка секундарној виктимизацији која се јавља када жртве доживе додатну трауму кроз реакције околине или институција које често не препознају озбиљност и дубину проблема.

Када говоримо о дигиталној виктимизацији на Dark Web-у, специфичности жртава постају још сложеније. Жртве често нису ни свесне да су њихови подаци компромитовани, што значи да могу бити изложене озбиљним претњама без да су тога свесне. Виктимизација може бити масовна, као у случајевима цурења података хиљада корисника, чиме се значајно повећава број погођених и интензитет штете. Додатно, на Dark Web-у постоји висок ниво секундарне виктимизације, јер информације могу бити јавно објављене и дистрибуиране, чиме се жртве додатно излажу срамоћењу и манипулацијама. Уз све то, идентитет починиоца је готово потпуно анониман, што значи да је изузетно тешко пратити починиоце и спровести одговарајуће санкције. Ове специфичности чине

[190] "Victimology in Cyberspace: A Reality We Can't Ignore." *AIU Blog*, American International University. (Преузето 16.03.2026.) https://www.aiu.edu/blog/victimology-in-cyberspace-a-reality-we-cant-ignore/

.

жртве у сајбер простору и на Dark Web-у посебно рањивим и тешко заштићеним, што захтева озбиљну пажњу и јачу заштиту на глобалном нивоу.

### 6.2. Дигитални отисак (Digital footprint) и његов значај

Дигитални отисак *(Digital footprint)* представља скуп свих података и информација који настају свесним или несвесним активностима на интернету или приликом употребе дигиталних уређаја. Њега чине различити сегменти online активности, као што су историја претраживања, записи о посећеним веб-страницама, IP адреса и подаци о локацији, објаве и интеракције на друштвеним мрежама, онлајн банкарство (пријаве за кредитне картице, трговина криптовалутама, куповина акција), online куповина и подаци о плаћању, претплате на билтене и услуге, подаци са паметних уређаја (нпр. фитнес тракери), електронска пошта и текстуалне поруке, као и друге интеракције у дигиталном окружењу. Сваки од ових сегмената чини дигитални идентитет особе, а њиховом анализом могу се открити информације о навикама, интересовањима, финансијском стању и другим личним подацима, који се потенцијално могу повезати са одређеном особом. За разлику од физичког отиска који временом нестаје, дигитални отисак може бити дуготрајан, умножив и тешко избрисив.

Дигитални отисак се у теорији и пракси дели на више категорија и може бити активни или пасивни, јавни, приватни или комерцијални. Активни дигитални отисак настаје свесним деловањем корисника, као што је објављивање садржаја, коментара, фотографија и видео-записа на друштвеним мрежама попут Facebook, Instagram и TikTok, али и попуњавањем образаца, слањем електронске поште и другим облицима намерног дељења информација. Насупрот томе, пасивни дигитални отисак настаје без директне намере или чак знања корисника, аутоматским прикупљањем података путем информационих система, што укључује податке о локацији, времену приступа, типу уређаја, IP адреси, обрасцима понашања корисника и другим техничким подацима, које прикупљају пружаоци дигиталних услуга као што су Google и Meta, у сврху анализе понашања, унапређења услуга и персонализације садржаја и оглашавања. Јавни дигитални отисак обухвата информације доступне широј јавности, док приватни дигитални отисак укључује податке видљиве ограниченом кругу људи (нпр. приватне поруке или затворене

.

групе). Комерцијални дигитални отисак односи се на податке које компаније користе у маркетиншке и аналитичке сврхе.

Једна од кључних карактеристика дигиталног отиска јесте његова релативна трајност. Чак и када се одређени садржај избрише са платформе, он може остати сачуван на серверима, у архивама, кеш меморији или путем снимака екрана које су направили други корисници. Због тога се често наглашава да интернет „памти све“.

Велики и неконтролисани дигитални отисак може представљати ризик по безбедност корисника, будући да лични подаци корисника могу постати доступни на Даркнет маркетима на више начина, а један од главних извора је компромитовање дигиталног отиска, путем хаковања phishing, spear-phishing и других врста напада, којим злонамерни актери прикупљају информације као што су корисничка имена, лозинке, адресе електронске поште, бројеве кредитних картица, податке о банкарским трансакцијама о интернет навикама и интересовањима. Ови подаци се јављају као „ роба“ Dark Web-у или користити за нове phishing и spear-phishing нападе, крађу идентитета, финансијске преваре, уцене, doxxing (објављивање приватних информација) и социјални инжењеринг.

С друге стране, дигитални трагови које остављају криминалци приликом приступа Даркнету могу бити кључни за њихово откривање. Истражни органи и безбедносне агенције могу анализирати IP адресе, временске ознаке активности, коришћене софтверске алате, обрасце комуникације и друге дигиталне отиске како би идентификовали појединце који учествују у илегалним трансакцијама. Пратећи ове трагове, стручњаци могу реконструисати мрежне активности, утврдити обрасце понашања и повезати их са стварним идентитетима, што омогућава расветљавање трговине подацима, продаје илегалних роба и услуга, као и спречавање сложених облика сајбер криминала.

Овакво коришћење дигиталног отиска и трагова има значајну улогу у модерним истражним и превентивним стратегијама безбедности на интернету. Поред истражних циљева, дигитални трагови имају и доказни значај у судским и управним поступцима. Електронска комуникација, аудио-визуелни снимци, записи о приступу систему и други

.

дигитални подаци могу послужити као доказ у поступку, под условом да су прибављени и чувани у складу са законом.

### 6.3. Методе праћења криминалаца на Dark Web-у

У целини посматрано, борба против криминала на Dark Web-у представља синхронизовану комбинацију рударења података, анализе блокчејна, специјализованих претраживача, дигиталне форензике, заплене инфраструктуре и HUMINT операција. Иако Dark Web нуди висок ниво анонимности, он није апсолутно сигуран простор за криминалце. Свако дигитално деловање оставља траг, у блокчејну, логовима, меморији уређаја или мрежном саобраћају, а управо праћење и повезивање тих трагова омогућава идентификацију, процесуирање и санкционисање починилаца у глобалном дигиталном окружењу.

Праћење криминалаца на Dark Web-у представља један од најсложенијих задатака савремених органа за спровођење закона, јер је то окружење конципирано тако да обезбеди висок степен анонимности, енкрипције и децентрализације. Мреже као што је Tor омогућавају прикривање IP адреса и локације корисника, што традиционалне истражне методе чини мање ефикасним. Ипак, иако Dark Web делује као дигитално подземље изван домашаја институција, он није потпуно непробојан. Свака активност – било да је реч о комуникацији, финансијској трансакцији, постављању садржаја или администрирању сервера – оставља одређене дигиталне трагове који се могу анализирати и повезати у јединствен доказни ланац.

Један од најважнијих приступа је „рударење података“, које подразумева прикупљање и анализу великих количина информација са форума, тржишта и скривених сервиса. Претрага кључних речи омогућава идентификацију појмова повезаних са трговином дрогом, оружјем, људима или украденим подацима. Препознавање слика омогућава анализу фотографија оружја, наркотика или других илегалних предмета, док анализа мреже односа помаже у откривању веза између појединаца и група. Анализа сентимента омогућава праћење тона и намера у дискусијама, што може указати на припрему кривичних дела. Посебно место има претраживање Deep web-а, односно неиндексираних делова интернета, укључујући сегменте Dark Web-а који нису доступни

.

путем класичних претраживача. Комбиновањем ових техника могуће је уочити обрасце понашања, трендове и структуру криминалних мрежа.

Кључну улогу има и анализа блокчејна, јер су криптовалуте основно средство плаћања на Dark Web тржиштима. Биткоин, иако се често сматра анонимним, функционише на јавно доступној децентрализованој књизи трансакција. То омогућава кластеризацију адреса, односно повезивање више новчаника са једним корисником на основу образаца потписивања и коришћења. Праћење трансакција (transaction tracing) омогућава праћење кретања средстава од извора до крајње дестинације, чак и када се она пребацују преко више адреса. Taint анализа служи за идентификацију „заражених“ средстава повезаних са криминалним активностима, док препознавање образаца открива понављајуће моделе у времену, износима и учесталости уплата. Blockchain data-maining обухвата анализу метаподатака као што су време трансакције, тип новчаника и веза са берзама. Компаније као што су Chainalysis, Elliptic и TRM Labs развиле су алате за визуелизацију токова новца и процену ризика. Значај ових техника потврђен је приликом гашења тржишта AlphaBay 2017. године, али и у случају Welcome to Video, где је праћење крипто уплата довело до стотина хапшења широм света. Иако су неке платформе користиле валуте за приватност попут Монера, анализа Биткоин трансакција одиграла је значајну улогу у истрагама.

Поред финансијске анализе, развијени су и специјализовани претраживачи и платформе за надзор Dark Web-a. Компаније као што су DarkOwl, Flashpoint, Recorded Future и Searchlight Cyber аутоматски индексирају форуме и тржишта. Ови алати омогућавају претрагу корисничких имена, PGP кључева и крипто адреса, постављање аутоматских упозорења о новим претњама, архивирање садржаја ради очувања доказа, идентификацију нових тржишта и трендова, као и мапирање криминалних мрежа. На тај начин се значајно убрзава истрага и обезбеђују докази прихватљиви на суду.

Када дође до заплене уређаја или сервера, примењује се дигитална форензика уз употребу алата као што су EnCase, Forensic Toolkit (FTK) и Magnet AXIOM. Анализа обухвата дешифровање дискова и комуникација, проналажење wallet.dat датотека и seed фраза, форензику меморије (RAM) ради откривања активних сесија, дешифровање PGP

.

порука и опоравак обрисаних података. У случају тржишта Silk Road, управо су заплењени сервери и приватни кључеви омогућили читање интерне комуникације и повезивање администратора са платформом.

Истражни органи често циљају и инфраструктуру која омогућава рад ових сервиса. Током међународне операције Operation Onymous угашено је више десетина Tor сервиса. Методе укључују заплену физичких сервера, сарадњу са хостинг провајдерима, контролу или надзор Tor чворова, корелацију мрежног саобраћаја и „sinkholing“, односно приказивање банера о заплени. Након гашења платформи као што су Hansa Market и AlphaBay, корисници су видели званична обавештења о заплени, што је имало снажан психолошки и превентивни ефекат.

Техничке методе нису довољне без људског фактора. HUMINT, односно људска обавештајна делатност, обухвата инфилтрацију тајних агената, рад са доушницима, ангажовање заједнице и међународну сарадњу кроз заједничке истражне тимове.

Социјални инжењеринг, укључујући phishing, spear-phishing, имперсонацију, вишинг и реверзни социјални инжењеринг, може се као оперативна техника користити у законским оквирима користити ради прикупљања додатних информација или откривања идентитета осумњичених. Често управо комбинација техничких доказа и људских извора омогућава изградњу комплетног доказног ланца.

Сарадња органа за спровођење закона представља један од кључних фактора у борби против криминала на Dark Web-у. Због анонимности и међународног карактера ових активности, појединачне институције често немају довољно ресурса или надлежности да самостално воде истрагу. Размена информација и обавештајних података омогућава изградњу шире слике о криминалним мрежама, начинима деловања и повезаним актерима. Заједничке истраге омогућавају удруживање техничких ресурса и стручности, чиме се повећава ефикасност откривања и хапшења осумњичених. Међународна сарадња је посебно важна јер сервери, осумњичени и жртве често припадају различитим државама. Кроз заједничке истражне тимове и споразуме о екстрадицији могуће је успешно процесуирати осумњичене без обзира на географску удаљеност. Поред

.

тога, међуинституционалне обуке и формирање специјализованих радних група омогућавају континуирано унапређење знања и техника у области сајбер криминалистике.

### 6.4. Праћење Dark Web-a (Dark Web monitoring )

У ери дигитализације, лични и корпоративни подаци постали су један од највреднијих "роба" на Dark Web маркетима . Иако већина корисника интернета никада не посећује Dark Web, њихове информације могу завршити у његовим скривеним деловима као последица сајбер напада, кршења безбедности или злонамерног дељења. Лични подаци доспевају на Dark Web кроз фишинг, малвер, ботнете, несигурне мреже, експлоите, логовања тастера (keylogging) или снимања екрана (screen scraping). Прикупљени подаци се често пакују као „fullz" и продају за финансијске преваре или крађу идентитета[191].

Скенирање тамног веба је процес у коме дигитални алати претражују Dark Web са циљем утврђивања да ли су лични или корпоративни подаци постали доступни на тим платформама. Ови алати континуирано претражују милионе сајтова, форума и затворених мрежа у готово реалном времену, анализирају такозване „дампове података" базе података настале кроз позната кршења безбедности, односо базе украдених информација насталих током различитих сајбер напада и упоређују их са информацијама корисника, као што су имена и презимена, адресе е-поште, лозинке, IP адресе, подаци о кредитним картицама и банковним рачунима, налози на друштвеним мрежама, подаци о идентитету (пасош, лична карта) и нешифровани транскрипти комуникације[192].

Када се идентификују потенцијално компромитовани подаци, корисник добија детаљне информације о врсти података и њиховој локацији на дарк вебу, што омогућава благовремено предузимање мера заштите као што су промена лозинки или заштита финансијских налога и додатну проверу безбедности система. Напредни алати користе алгоритме за аутоматизовано препознавање и, у неким случајевима, људске аналитичаре

[191] Deepstrike. (2025, February 15). *Best dark web monitoring tools*. Deepstrike. (преузето 16.03.2026.) https://deepstrike.io/blog/best-dark-web-monitoring-tools

[192] Kaspersky. (n.d.). *What is a dark web scan?* Kaspersky. (преузето 16.03.2026.) https://www.kaspersky.com/resource-center/threats/what-is-a-dark-web-scan

.

који могу интерпретирати вишејезичне разговоре и активности на затвореним форумима. Неке платформе чак могу идентификовати трговину украденим подацима пре њихове злоупотребе, пружајући корисницима додатно време за превентивне мере.

Скенирање Dark Web-а омогућава рано откривање компромитованих података и превенцију злоупотребе, што значајно смањује ризик од финансијских превара и крађе идентитета. Редовно праћење омогућава организацијама да благовремено уоче потенцијална цурења података, идентификују слабости у системима и унапреде безбедносне мере, чиме се штите и подаци клијената и очувава углед компаније. Такође, скенирање Dark Web-а има значајну улогу и у откривању различитих облика сајбер криминала. Безбедносне организације и институције за спровођење закона користе ове алате како би идентификовале нелегалне активности, укључујући трговину илегалним супстанцама, оружјем или фалсификованим производима.

Алати за скенирање Dark Web-а и праћење компромитованих података могу се класификовати према нивоу услуга и дубини заштите коју пружају. Постоје три категорије ових алата. Прва категорија су бесплатни алати за појединце, сервисни пакети као што су: „ Have I Been Pwned“, „Firefox Monitor“ и „ BreachAlarm“, који омогућавају једнократне провере електронске поште и лозинки како би се утврдило да ли су постали предмет кршења безбедности. Поред тога, неки од ових сервиса нуде обавештења о новим кршењима, пружајући основни ниво надзора без финансијских трошкова. Следећа категорија обухвата бесплатне безбедносне апликације које пружају континуирано праћење акредитива и проверу у базама података о кршењу података у реалном времену. Примери оваквих решења укључују „Keeper BreachWatch“, „NordPass“ и „LastPass монитор“. Основне функције скенирања могу бити доступне без накнаде, док потпуно праћење и напредне функције обично захтевају премијум планове. Трећа категорија обухвата сервисе плаћене заштите идентитета, као што су „Experian Dark Web Scan”, “LifeLock” и “ Identity Guard”. Ови алати нуде континуирани надзор на Dark Web-а, праћење личних података, матичних бројева, банковних рачуна и других осетљивих информација. Поред тога, услуге овог типа често укључују и осигурање од крађе идентитета, пружајући додатни слој заштите. Корисници ових услуга плаћају месечну

.

претплату, што их чини приступачним углавном организацијама и појединцима који захтевају потпуни мониторинг и већу сигурност[193].

Ипак, скенирање Dark Web-а има одређена ограничења. Велики део даркнета функционише у затвореним или приватним мрежама којима алати за скенирање немају приступ, што значи да не могу обухватити све потенцијалне претње и активности. Резултати скенирања одражавају само стање у тренутку анализе, те нови инциденти или цурења података могу настати након што је скенирање обављено. Затим алати могу идентификовати компромитоване податке и њихову локацију, али не могу их директно уклонити са даркнета, што корисницима оставља потребу да предузму додатне мере заштите. Поред тога, напредне платформе за континуирано праћење могу бити финансијски и технички захтевне, што може представљати изазов за појединце и мала предузећа. На крају, тумачење података са Dark Web-а захтева пажљиву анализу, јер могући сложени или вишејезични садржаји могу довести до лажних упозорења или пропуштања критичних информација.

Због ових ограничења, скенирање Dark Web-а најбоље функционише као део ширег система безбедносних мера. Комбинација скенирања са коришћењем VPN сервиса, антивирусних програма, менаџмента лозинки, редовног ажурирања софтвера и одговорног управљања личним и корпоративним подацима обезбеђује свеобухватнију заштиту. Таква интегрисана стратегија омогућава рано откривање претњи, смањење ризика од сајбер криминала и ефикаснију превенцију потенцијалних злоупотреба дигиталних информација.

### 6.5. Криминолошки приступи превенцији криминала на Dark Web-у

Превенција криминала представља скуп мера и стратегија чији је циљ спречавање настанка криминалних активности, смањење њиховог обима и ублажавање последица које оне имају по друштво[194]. У контексту савременог дигиталног окружења, посебан значај има превенција криминала на Dark Web-у, делу интернета који функционише на принципу

[193] Deepstrike. (2025, February 15). *Best dark web monitoring tools*. Deepstrike. (преузето 17.03.2026) https://deepstrike.io/blog/best-dark-web-monitoring-tools

[194]Димитријевић, М. (2018). Превентивне активности у циљу спречавања и сузбијања криминалитета са освртом на стратегијски оквир Републике Србије. Право – теорија и пракса 35(7-9), 54-63. Доступно на : https://scindeks-clanci.ceon.rs/data/pdf/0352-3713/2018/0352-37131809054D.pdf

.

анонимности, што у значајној мери отежава идентификацију извршилаца кривичних дела, омогућава развој различитих облика илегалних активности и тржишта, укључујући трговину наркотицима, продају украдених података, оружја, фалсификованих докумената, и различитих видова злонамерних софтвера, као и до појаве сложених криминалних структура које функционишу на принципима подземне економије.

Криминолошка теорија превенцију криминала традиционално дели на три основна нивоа: примарну, секундарну и терцијарну превенцију. Ова подела омогућава систематски приступ сузбијању криминалних активности, јер обухвата мере које се примењују пре настанка криминала, током његовог развоја и након извршења кривичног дела[195].

### 6.5.1 Примарна, секундарна и терцијалана превенција

Примарна превенција усмерена је на спречавање криминалног понашања пре него што до њега дође. У контексту Dark Web-a, овај облик превенције подразумева стварање безбеднијег дигиталног окружења и смањење прилика за извршење кривичних дела. Примарна превенција обухвата развој и примену технолошких мера заштите, као што су напредни системи сајбер безбедности, заштита информационих система, енкрипција података и системи за рано откривање сајбер напада. Поред технолошких мера, значајну улогу има и подизање свести корисника о опасностима које постоје на интернету, као и развој дигиталне писмености[196]. Када корисници имају довољно знања о начинима злоупотребе података и о механизмима заштите, смањује се вероватноћа да постану жртве различитих облика криминала који се организују на Dark Web-у.

Секундарна превенција усмерена је на рано откривање и спречавање криминалних активности у фазама када се оне тек развијају. У случају Dark Web-a, секундарна превенција подразумева праћење активности на илегалним форумима и тржиштима, анализу комуникације између чланова криминалних мрежа и идентификацију потенцијалних претњи. Државне институције и безбедносне агенције користе различите методе дигиталне форензике, анализе криптовалутних трансакција и обавештајног рада

[195] Brandon Welsh, David Farrington, *The Oxford Handbook of Crime Prevention,* Oxford University Press, 2012.
[196] Y. Jewkes, M. Yar, *Handbook of Internet Crime*, Routledge, 2010

.

како би открише структуру криминалних група и спречиле реализацију планираних кривичних дела[197].

Терцијарна превенција односи се на мере које се примењују након извршења кривичног дела и усмерена је на спречавање поновног извршења криминалних активности. Овај облик превенције укључује деловање система кривичног правосуђа, односно полиције, тужилаштва и судова, који имају задатак да идентификују и процесуирају починиоце кривичних дела из области сајбер криминала. Терцијарна превенција подразумева и гашење илегалних платформи и тржишта на Dark Web-у, хапшење организатора криминалних мрежа и заплену незаконито стечених средстава. Један од најпознатијих примера успешне интервенције органа за спровођење закона је затварање тржишта Silk Road, које је годинама представљало једно од највећих Dark Web тржишта за продају наркотика и других илегалних производа.

### 6.5.2. Улога образовања и дигиталне писмености у као фактори превенције кривичних дела на Dark Web-у

Дигитална писменост представља значајан предуслов за остваривање безбедности у савременом дигиталном окружењу. У условима интензивне употребе интернета, мобилних уређаја и различитих дигиталних платформи, способност разумевања функционисања информационо-комуникационих технологија и безбедног руковања подацима постаје од суштинског значаја. Посебан значај дигитална писменост добија у контексту Dark Web-а, дела интернета који није доступан путем стандардних претраживача и који карактерише висок степен анонимности, али и бројни безбедносни ризици.

Недовољна информисаност и непознавање начина функционисања дарк веба могу довести до ситуација у којима појединци несвесно излажу своје личне или финансијске податке опасности од злоупотребе. Посебну опасност представља могућност да се лични подаци, као што су корисничка имена, лозинке, бројеви банковних рачуна или подаци са кредитних картица, појаве на Dark Web тржиштима као последица претходних

[197]Thomas J. Holt, Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*, Routledge, 2016.

.

безбедносних инцидената или цурења података[198]. Развијање дигиталних компетенција омогућава корисницима да благовремено идентификују потенцијалне претње у дигиталном окружењу и предузму адекватне мере ради заштите личних и пословних података. На тај начин се значајно умањује ризик од крађе идентитета, финансијских превара, ширења злонамерног софтвера (malware), ransomware напада, фишинг (phishing) превара, као и неовлашћеног приступа или откривања поверљивих корпоративних информација[199].

Један од кључних аспеката дигиталне писмености односи се на разумевање механизама функционисања сајбер напада. Фишинг поруке, на пример, често се представљају као легитимна комуникација финансијских институција или пословних субјеката, са циљем довођења корисника у заблуду и прибављања њихових личних података или приступних информација. У том смислу, дигитална писменост има значајну превентивну функцију, јер доприноси подизању свести о значају заштите података и едукацији корисника о начинима очувања сопствене дигиталне безбедности.

Заштита личних података у дигиталном окружењу подразумева примену више техничких и организационих мера. То, пре свега, обухвата ограничено дељење личних информација на интернету, употребу јаких и јединствених лозинки за сваки кориснички налог, редовну промену приступних података, као и коришћење менаџера лозинки ради безбедног управљања сложеним лозинкама[200]. Поред тога, значајну улогу има примена двофакторске или вишефакторске аутентификације, као и коришћење техничких средстава за заштиту информационих система, као што су антивирусни програми, firewall системи и редовна ажурирања софтвера, уз континуирано праћење могућих цурења података на Dark Web-у. Наведене мере представљају основни механизам превенције од злонамерног софтвера и других облика сајбер претњи[201]. Посебна пажња мора се посветити и избегавању небезбедних јавних Wi-Fi мрежа, које могу представљати потенцијални канал за пресретање и злоупотребу података. У таквим ситуацијама

[198] HP. (2024, October 29). *What is the dark web? Safety guide & risks.* HP Tech Takes. (преузето 18.03.2026.) https://www.hp.com/us-en/shop/tech-takes/what-is-dark-web
[199] Ibid
[200] Acronis. (2024). *Dark web cybersecurity best practices.* Acronis Blog. преузето 18.03.2026.) https://www.acronis.com/en/blog/posts/dark-web-cybersecurity-best-practices/
[201] Ibid

.

препоручује се употреба VPN услуга, које обезбеђују додатни ниво енкрипције и доприносе заштити идентитета корисника[202].

Имајући у виду чињеницу да се сајбер претње континуирано развијају и постају све сложеније, стална едукација корисника представља неопходан елемент дигиталне безбедности. Праћење стручне литературе, похађање специјализованих курсева и информисање о актуелним трендовима у области сајбер безбедности омогућавају благовремено препознавање ризика и адекватну заштиту у дигиталном простору[203].

С обзиром на то да Dark Web може представљати окружење у коме се врши трговина незаконито прибављеним подацима и дигиталним ресурсима, развијање дигиталне писмености представља важан инструмент превенције и заштите како појединаца, тако и организација. Повећањем нивоа информисаности и дигиталних компетенција корисника могуће је значајно умањити ризик од злоупотребе података и других облика сајбер криминала.

### 6.5.3. Улога полиције, тужилаштва и међународних организација у борби против криминала на Dark Web-у

Криминалне активности на Dark Web-у представљају један од најсложенијих изазова савременог сајбер криминала. Dark Web омогућава анонимну трговину илегалним производима и услугама, укључујући наркотике, оружје, фалсификоване документе, малвер, ransomware и украдене личне податке. Ефикасна борба против криминала у овом дигиталном простору захтева координисано деловање националних и међународних органа за спровођење закона, укључујући полицију, тужилаштво и специјализоване међународне организације, као што су Европол и Интерпол.

Националне полицијске агенције имају кључну улогу у идентификацији, истрази и хапшењу лица која учествују у криминалним активностима на Dark Web-у. Оне примењују напредне методе дигиталне форензике, анализу криптовалутних трансакција и праћење активности на илегалним тржиштима. Полицијске службе организују акције усмерене на затварање дарк веб платформи и хапшење кључних актера, чиме директно

[202] Ibid
[203] Op cit HP. *What is the dark web? Safety guide & risks.* HP Tech Takes

.

смањују обим илегалне трговине и разарају криминалне мреже. Пример оваквог деловања јесте холандска национална полиција, која је у сарадњи са FBI-ем и Европолом учествовала у гашењу тржишта AlphaBay и Hansa 2017. године, чиме је прекинута трговина више од 350.000 илегалних производа, укључујући наркотике, оружје и алате за сајбер криминал.

Полицијске агенције такође прате и мања тржишта и "single-vendor" продавнице које су постале све популарније након затварања великих платформи, као што је Dream Market. Пример је операција RapTor, у оквиру које су полицијске снаге из десет земаља идентификовале и ухапсиле 270 продаваца и купаца дарк веба, запленивши преко 184 милиона евра у готовини и криптовалутама, више од две тоне наркотика, преко 180 ватреног оружја и 12.500 фалсификованих производа[204].

Након што полиција прикупи доказе, тужилаштво преузима процесуирање починилаца, врши правну квалификацију извршених кривичних дела, припрема оптужнице и иницира заплену имовине. Посебан изазов представља прикупљање и верификација дигиталних доказа, као и утврђивање надлежности у случајевима када се кривична дела врше преко више држава. Због тога тужилаштва све чешће сарађују са националним специјализованим јединицама за високотехнолошки криминал, као и са полицијским органима у националним и међународним истрагама, како би доказни материјал био правно ваљан у различитим јурисдикцијама, уз коришћење међународних механизама правне помоћи. Тужилаштва такође координишу мере заштите жртава и сарађују са банкарским и финансијским институцијама у праћењу и блокирању незаконитих трансакција. Пример оваквог деловања представља улога тужилаштва у Сједињеним Америчким Државама током операције RapTor, где је сарађивало са више федералних агенција (FBI, DEA, HSI) на идентификацији и оптуживању високорангираних продаваца на Dark Web-у.

[204] U.S. Department of Justice. (2025, May 22). *Law enforcement seize record amounts of illegal drugs, firearms, and drug trafficking proceeds in international operation against darknet trafficking of fentanyl and opioids; 270 arrested across four continents*. U.S. Department of Justice. (преузето 18.03.2026.) https://www.justice.gov/opa/pr/law-enforcement-seize-record-amounts-illegal-drugs-firearms-and-drug-trafficking-proceeds

.

С обзиром на транснационални карактер сајбер криминала, међународна сарадња представља кључни елемент ефикасне борбе против Dark Web криминала. Међународне организације, као што су Европол и Интерпол, имају централну улогу у координацији глобалних операција и размену обавештајних података.

Европол координише сарадњу полицијских служби држава чланица Европске уније у борби против организованог и сајбер криминала. У оквиру организације делује Европски центар за сајбер криминал (EC3), специјализовану јединицу која пружа оперативну, аналитичку и техничку подршку националним органима у истрагама везаним за дарк веб, укључујући припрему оперативних пакета обавештајних података[205]. Европол учествује у међународним операцијама усмереним на затварање илегалних интернет тржишта и идентификацију лица која учествују у незаконитим активностима.[206]

Интерпол, као глобална полицијска организација, омогућава размену информација и координацију истрага између полицијских органа из више од 190 држава. Интерпол развија специјализоване програме и алате за борбу против сајбер криминала, укључујући анализу дигиталних доказа, праћење криминалних мрежа и организовање заједничких међународних операција против група које делују на Dark Web-у. У оквиру Интерпола функционише и специјализована јединица за сајбер криминал, која се бави анализом глобалних трендова у области дигиталних претњи, укључујући активности на Dark Web-у.

Поред институционалне сарадње, значајан елемент међународног правног оквира представљају и заједнички истражни тимови (Joint Investigation Teams – JIT). Ови тимови омогућавају истражним органима из више држава да заједнички спроводе истраге, деле доказе и координишу активности у реалном времену. Овај механизам је посебно важан у истрагама које укључују Dark Web, јер се сервери, корисници и финансијске трансакције често налазе у различитим државама и правним системима.

---

[205] Europol. (2018, May 29). *Crime on the dark web: Law enforcement coordination is the only cure*. Europol Newsroom. (преузето 18.03. 2026) https://www.europol.europa.eu/media-press/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure

[206] INTERPOL. (2025). *Spotlight issue 2: Cybercrime focus*. INTERPOL Spotlight. (преузето 18.03. 2026) https://www.interpol.int/Resources/INTERPOL-Spotlight/Spotlight-Issue-2-Cybercrime/Spotlight-Cybercrime-Focus

.

Ефикасна борба против Dark Web криминала захтева мултидисциплинарни и координисан приступ. Само интегрисаним деловањем националне полиције, тужилаштва и међународних организација могуће је идентификовати и процесуирати продаваце и купце илегалних производа, смањити обим илегалне трговине и криминалне економије на дарк вебу, запленити криптовалуте, наркотике, оружје и фалсификоване производе, те смањити ризик од транснационалног криминала. Оваквим деловањем обезбеђује се дигитална безбедност, заштита грађана и спречава се злоупотреба Dark Web за криминалне активности.

## 7. НОРМАТИВНИ И ИНСТИТУЦИОНАЛНИ ОКВИР СУЗБИЈАЊА ДАРК WEБ КРИМИНАЛА

### 7.1. Међународни правни оквир (конвенције УН, Савет Европе – Будимпештанска конвенција)

Међународни правни оквир у борби против криминалних активности на интернету, укључујући и активности које се одвијају на Dark Web-у, заснива се на комбинацији глобалних и регионалних правних инструмената који имају за циљ сузбијање различитих облика сајбер криминала, јачање међународне сарадње, заштиту података и дигиталну безбедност. Иако до данас не постоји посебан међународни уговор који би искључиво регулисао криминалне активности на Dark Web-у, будући да он изворно није незаконит, постоје бројни правни механизми који се посредно примењују на незаконите активности које се на овим анонимним интернет мрежама одвијају.

У развоју и обликовању овог правног оквира значајну улогу имају међународне организације, пре свега Уједињене нације и Савет Европе, чије конвенције и правни инструменти представљају основу глобалне сарадње у борби против сајбер криминала. У оквиру система Уједињених нација посебан значај има Конвенција УН против транснационалног организованог криминала из 2000. године, позната као Палермска конвенција, затим Резолуције 74/247 из 2019. године и 75/282 из 2021. године, чији је резултат усвајање Конвенције Уједињених нација против сајбер криминала из 2024. године. Са друге стране, на регионалном нивоу, најзначајнији правни инструмент у области сајбер криминала представља Будимпештанска конвенција Савета Европе о сајбер криминалу из 2001. године.

.

Сагледани заједно, ови међународни механизми представљају темељ глобалног правног оквира који омогућава државама да ефикасније сарађују у откривању, истрази и процесуирању кривичних дела извршених путем савремених дигиталних технологија и анонимних интернет мрежа. Иако Dark Web као технолошки феномен није директно регулисан посебним међународним уговором, постојећи правни инструменти омогућавају примену кривичноправних норми и механизама међународне сарадње на широк спектар незаконитих активности које се на овим платформама одвијају.

### 7.1.1. Конвенција УН против транснационалног организованог криминала из 2000. године- Палермска конвенција

Конвенција УН против транснационалног организованог криминала из 2000. године – Палермска конвенција[207] представља један од најзначајнијих међународних правних инструмената у области борбе против организованог криминала. Усвојена је у оквиру Уједињених нација 15. новембра 2000. године у Палерму, а ступила је на снагу 29. септембра 2003. године. Основни циљ Конвенције јесте јачање међународне сарадње у спречавању и сузбијању транснационалног организованог криминала, као и унапређење националних законодавстава у овој области. Конвенција успоставља правни оквир за сарадњу држава у поступцима екстрадиције, међусобне правне помоћи, размене информација и спровођења заједничких истрага.

Доношење Палермске конвенције представља одговор међународне заједнице на све израженију глобализацију криминалних активности и јачање транснационалних криминалних мрежа. Савремене организоване криминалне групе делују преко граница више држава и користе технолошке иновације, глобалне финансијске системе и интернет платформе ради извршења различитих кривичних дела, као што су трговина људима, трговина наркотицима, прање новца и други облици организованог криминала. У том контексту, Конвенција успоставља универзалне правне стандарде који омогућавају ефикаснију међународну сарадњу и координисано деловање држава у сузбијању ових појава.

[207] *Конвенција Уједињених нација против транснационалног организованог криминала* (Палермска конвенција), усвојена Резолуцијом Генералне скупштине УН 55/25 од 15. новембра 2000. године, потврђена у Републици Србији („Службени лист СРЈ – Међународни уговори“, бр. 6/2001).Оригиналан текст конвенције видети на: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

.

Један од значајних доприноса Конвенције огледа се у дефинисању појма организоване криминалне групе, која се одређује као структурисана група од најмање три лица, која постоји одређени временски период и делује у циљу извршења једног или више тешких кривичних дела ради стицања материјалне користи. Поред тога, Конвенција обавезује државе потписнице да у своје националне правне системе инкриминишу одређене облике криминалног понашања, као што су учешће у организованој криминалној групи, прање новца, корупција и ометање правде.

Посебан значај Палермске конвенције огледа се у механизмима међународне сарадње које она успоставља, а који обухватају екстрадицију, међусобну правну помоћ, заједничке истраге и сарадњу органа за спровођење закона. Ови механизми омогућавају ефикасније откривање, истраживање и кривично гоњење транснационалних криминалних активности.

Поред основног текста конвенције, усвојена су и три додатна протокола који се баве специфичним облицима организованог криминала. То су Протокол о спречавању, сузбијању и кажњавању трговине људима, нарочито женама и децом, Протокол против кријумчарења миграната копном, морем и ваздухом као и Протокол против незаконите производње и трговине ватреним оружјем, његовим деловима и компонентама и муницијом.

Иако Палермска конвенција није усмерена искључиво на сајбер криминал нити на активности које се одвијају на Dark Web-у, имајући у виду да у време њеног доношења овај феномен није био у потпуности развијен, основни принципи и механизми које Конвенција успоставља могу се применити и на овај облик криминалитета. Многе криминалне активности које се реализују путем анонимних интернет мрежа, попут незаконите трговине наркотицима, оружјем, трговине људима и прања новца, представљају облике транснационалног организованог криминала који су обухваћени њеним одредбама. Криминалне групе које делују у оквиру анонимних интернет мрежа често функционишу као транснационалне структуре, чији чланови делују са територија различитих држава и користе сложене финансијске и комуникационе механизме ради прикривања свог идентитета и незаконитих активности. Стога Палермска конвенција

.

представља важан правни основ за развој међународне сарадње у откривању, истрази и кривичном гоњењу криминалних активности које се одвијају у дигиталном окружењу.

### 7.1.2. Резолуције генералне скупштине Уједињених нација бр. 74/247 из 2019. године и бр. 75/282 из 2021. године

Важан допринос развоју међународног правног оквира дају и активности Уједињених нација усмерене на креирање глобалних стандарда за борбу против злоупотребе информационо-комуникационих технологија у криминалне сврхе. У том контексту, Резолуција Генералне скупштине УН бр. 74/247, усвојена 27. децембра 2019. године покренула је процес израде нове међународне конвенције о борби против злоупотребе информационо-комуникационих технологија у криминалне сврхе. Резолуцијом је успостављен отворени међувладин ad hoc комитет експерата са задатком да изради нацрт универзални правни инструмент који би могао обухватити и специфичне изазове повезане са криминалним активностима на Dark Web-у и омогући ефикаснију сарадњу држава у спречавању, откривању и процесуирању различитих облика сајбер криминала. Резолуција такође наглашава потребу за јачањем међународне сарадње, размене информација и изградње институционалних капацитета држава у борби против криминала који се врши путем дигиталних технологија.

Наставак овог процеса представља Резолуција Генералне скупштине УН бр. 75/282, усвојена 26. маја 2021. године, којом се додатно прецизирају мандат и начин рада ad hoc комитета задуженог за израду будуће конвенције. Овом резолуцијом утврђен је временски оквир рада комитета, као и процедура одржавања низа међувладиних састанака на којима ће се разматрати нацрт текста конвенције. Посебан нагласак стављен је на инклузивност процеса, што подразумева учешће свих држава чланица, као и сарадњу са релевантним међународним организацијама, академском заједницом и другим заинтересованим актерима. На тај начин настоји се обезбедити да будући међународни правни инструмент одражава различите правне системе и интересе држава.

Обе резолуције су имале значајну улогу у развоју глобалног правног оквира за борбу против сајбер криминала. Иако не представљају правно обавезујуће међународне уговоре, оне су покренуле институционални процес који је довео до усвајања Конвенције

.

Уједињених нација против сајбер криминала 2024. године, која представља први универзални међународни уговор посвећен борби против сајбер криминала.

### 7.1.3. Конвенција Уједињених нација против сајбер криминала 2024. године

Конвенција Уједињених нација против сајбер криминала из 2024. године представља најновији и свеобухватан међународни правни инструмент чији је циљ успостављање заједничких стандарда и јачање глобалне сарадње у спречавању злоупотребе информационо-комуникационих технологија у криминалне сврхе. Усвојена је у оквиру Уједињених нација након вишегодишњег преговарачког процеса, покренутог резолуцијама Генералне скупштине УН 74/247 (2019) и 75/282 (2021), у којем су учествовале државе чланице, међународне организације и експерти из области сајбер безбедности и кривичног права. Конвенција има за циљ да одговори на изазове савременог дигиталног окружења у коме се различити облици криминалитета све чешће реализују путем интернета, дигиталних платформи и анонимних мрежа, а њен основни циљ јесте јачање међународне сарадње у спречавању, откривању и процесуирању кривичних дела извршених путем информационо-комуникационих технологија.

Један од кључних елемената Конвенције односи се на усклађивање националних законодавстава држава чланица у погледу инкриминације кривичних дела извршених путем информационо-комуникационих технологија. Конвенција предвиђа да државе у своје националне правне системе уведу кривична дела као што су: неовлашћени приступ рачунарским системима, незаконито пресретање електронских комуникација, незаконито ометање рада рачунарских система, злоупотреба рачунарских уређаја и програма, као и различити облици интернет превара. Поред тога, Конвенција обухвата и кривична дела која се врше уз помоћ дигиталних технологија, као што су крађа и злоупотреба личних података, online финансијске преваре, злоупотреба дигиталних платформи за ширење незаконитих садржаја и друге активности које угрожавају безбедност информационих система и корисника интернета. Циљ овог приступа јесте обезбеђивање усклађености националних законодавстава и ефикасно кривично гоњење транснационалних сајбер криминалних активности.

.

Посебан значај имају и одредбе које се односе на кривична дела повезана са организованим криминалом у дигиталном окружењу. Савремене криминалне групе све чешће користе интернет инфраструктуру и анонимне мреже за трговину незаконитим робама и услугама, укључујући наркотике, оружје, украдене податке и малвер. Конвенција успоставља правни основ за кривично гоњење активности које се реализују путем дигиталних платформи, укључујући и оне на Dark Web-у, где се криминалне активности често организују уз висок степен анонимности.

Поред материјалноправних одредби, Конвенција садржи и процесноправне механизме за ефикасније откривање и истраживање сајбер криминала. Ови механизми обухватају прикупљање и очување електронских доказа, приступ дигиталним подацима, праћење електронских комуникација у складу са националним законодавством и примену специјалних истражних техника. Посебна пажња посвећена је очувању дигиталних доказа, имајући у виду да се електронски подаци могу лако изменити, избрисати или преместити на сервере који се налазе у различитим државама.

Конвенција такође успоставља механизме међународне сарадње, који укључују екстрадицију, међусобну правну помоћ, размену информација, заједничке истраге и координацију органа за спровођење закона, као и успостављање контакт тачака доступних 24 часа дневно како би се омогућила брза комуникација између надлежних органа различитих држава. С обзиром на транснационални карактер сајбер криминала, овакви механизми омогућавају бржу и ефикаснију реакцију надлежних органа. Конвенција подстиче успостављање директних канала комуникације између држава, као и развој капацитета у области сајбер безбедности кроз техничку помоћ, обуку стручњака и размену експертских знања.

### 7.1.4. Конвенција Савета Европе о сајбер криминалу ( Будимпештанска конвенција, 2001)

На регионалном нивоу, најзначајнији правни инструмент у области сајбер криминала представља Конвенција о сајбер криминалу, позната као Будимпештанска конвенција, усвојена 23. новембра 2001. године у Будимпешти под окриљем Савета

.

Европе[208]. Она представља први и најзначајнији међународни правни инструмент који се непосредно бави кривичноправним аспектима злоупотребе рачунарских система и интернета. Конвенција дефинише основне облике сајбер криминала, укључујући: неовлашћени приступ рачунарским системима, незаконито пресретање података, злоупотребу уређаја и рачунарске преваре. Поред тога, конвенција посебно третира кривична дела у вези са дечијом порнографијом и кривична дела која се односе на злоупотребу интернета за извршење других облика транснационалног криминала.

Поред материјалноправних одредби, конвенција прописује и процесна овлашћења неопходна за ефикасну истрагу сајбер криминала. Она омогућава претрес рачунарских система, заплену дигиталних података, очување електронских доказа, пресретање комуникација у реалном времену, као и примену специјализованих истражних техника. Посебна вредност Будимпештанске конвенције огледа се у развоју механизама међународне сарадње, који омогућавају брзо и ефикасно прикупљање доказа у транснационалним истрагама. Државе потписнице сарађују кроз Комитет за Конвенцију о сајбер криминалу, који прати примену конвенције, размену искустава и информација, као и развој стандарда за кривично гоњење сајбер криминала. Успостављена је и мрежа националних контакт тачака, доступних 24 часа дневно, ради брзе размене информација у хитним случајевима.

Будимпештанска конвенција је временом проширена додатним протоколима. Први додатни протокол односи се на криминализацију ширења расистичког и ксенофобног материјала путем рачунарских система, са циљем заштите жртава говора мржње и дискриминације на интернету. Други додатни протокол усмерава се на јачање међународне сарадње, посебно у погледу прикупљања електронских доказа у кривичним поступцима. Он омогућава директне захтеве пружаоцима интернет услуга у другим државама ради добијања података о корисницима и интернет саобраћају, предвиђа формирање заједничких истражних тимова и убрзану сарадњу у хитним случајевима.

[208] Конвенција о високотехнолошком криминалу, усвојена у Будимпешти 23. новембра 2001. године, („Службени гласник РС” – Међународни уговори бр. 19/2009)

.

Ови механизми су посебно значајни у истрагама које укључују активности на Dark Web-у, где се сервери, корисници и дигитални трагови често налазе у више јурисдикција, а криминалне мреже користе анонимне и енкриптоване комуникације за трговину наркотицима, оружјем, украденим подацима или малвером. Захваљујући Будимпештанској конвенцији, државе потписнице могу координисано приступати овим истрагама, размењивати податке и успостављати правне мере за ефикасно процесуирање починилаца. На тај начин, Будимпештанска конвенција и њени протоколи представљају темељ правног оквира за регионалну и транснационалну борбу против сајбер криминала, омогућавајући усклађивање националних законодавстава, развој стандарда истрага и успостављање сталних механизама међународне сарадње у дигиталном окружењу.

Будимпештанска конвенција, Палермска конвенција и Конвенција УН против сајбер криминала из 2024. године представљају комплементарне правне инструменте у међународној борби против криминала, али се разликују по фокусу, обиму и механизмима примене. Укратко, Будимпештанска конвенција (2001) је усмерена је искључиво на кривично-правне аспекте сајбер криминала и високотехнолошког криминала, она представља регионални оквир (Савет Европе), али се примењује и глобално кроз приступ држава које нису чланице Савета Европе, Палермска конвенција (2000) има шири фокус и бави се транснационалним организованим криминалом уопште, укључујући и онлајн и онлајн активности, а Конвенција УН против сајбер криминала (2024) интегрише оба приступа, пружајући универзални глобални оквир за борбу против криминала у дигиталном окружењу и омогућавајући ефикасну међународну сарадњу у истрагама које укључују Dark Web и сложене транснационалне криминалне мреже.

### 7.2. Национални законодавни оквир Републике Србије

Национални правни оквир Републике Србије који се односи на кривична дела извршена на интернету, па самим тим и на Dark Web-у, заснива се на више домаћих законских аката који регулишу област високотехнолошког криминала. Иако Dark Web није посебно дефинисан у законодавству као засебна правна категорија, кривична дела која се врше путем ових анонимних мрежа санкционишу се применом постојећих кривичноправних норми које се односе на злоупотребу рачунарских система, рачунарских

.

мрежа и рачунарских података. Поред домаћег законодавства, одређени аспекти кривичноправне заштите усклађени су са међународним стандардима кроз примену ратификованих конвенција, као што су: Палермска конвенција, Будимпештанска конвенција и Додатни протокол уз Будимпештанску конвенцију о криминализацији аката расистичке и ксенофобичне природе путем рачунарских система.

У законодавству Републике Србије не користи се термин „сајбер криминал“, већ се за означавање овог облика криминала користи појам високотехнолошки криминал (ВТК). Овај термин је прихваћен након што је Србија ратификовала Конвенцију Савета Европе о високотехнолошком криминалу (Convention on Cybercrime), познату као Будимпештанска конвенција, чиме је домаће законодавство усклађено са међународним стандардима у области борбе против криминала у дигиталном окружењу.

Основни извор кривичноправне регулативе представља Кривични законик Републике Србије[209], који садржи посебну групу кривичних дела под називом Кривична дела против безбедности рачунарских података (глава 27). Кривични законик не користи ни термин сајбер криминал ни термин високотехнолошки криминал, али у члану 112. одређује значење појединих појмова као што су: рачунарски податак, рачунар, рачунарски систем, рачунарска мрежа, рачунарски програм и рачунарски вирус.

У ову групу спада осам кривичних дела против безбедности рачунарских података, и то:

- оштећење рачунарских података и програма (чл. 298),
- рачунарска саботажа (чл. 299),
- прављење и уношење рачунарских вируса (чл. 300),
- рачунарска превара (чл. 301),
- неовлашћени приступ заштићеном рачунару, рачунарској мрежи или обради података (чл. 302),
- спречавање или ограничавање приступа јавној рачунарској мрежи (чл. 303),
- неовлашћено коришћење рачунара или рачунарске мреже (чл. 304),

[209] 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, 35/2019, 94/2024

.

- прављење, набављање или давање другом средстава за извршење кривичних дела против безбедности рачунарских података (чл. 304а).

Поред ових кривичних дела, бројне незаконите активности које се јављају на Dark Web-у могу бити санкционисане и применом других одредаба Кривичног законика, односно кривичних дела код којих се као објекат или средство извршења могу јавити рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику. То се посебно односи на:

- кривична дела против полне слободе, као што су: Полно узнемиравање ( чл. 182а), Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију ( чл. 185) и Искоришћавање рачунарских мрежа и комуникацију других техничких средстава за вршење кривичних дела против полне слободе према малолетном лицу;
- кривична дела против интелектуалне својине, као што су: Повреда моралоног права аутора и интерпретатора ( чл.198), Неовлашћено искоришћавање ауторског дела или предмета сродног права ( чл.199), Неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима ( чл. 200), Повреда проналазачког права ( чл. 201) и Неовлашћено коришћење туђег дизајна (чл. 202);
- кривична дела против иновине, као што су: изнуда ( чл.214) и уцена ( чл. 215);
- кривична дела против правног саобраћаја као што је фалсификовање исправе ( чл.355);
- Кривична дела против слободе и права човека и грађанина, као што су: угрожавање сигурности (нпр. претње преко интернета, чл. 138), прогањање (cyberstalking, чл.138а), неовлашћено прислушкивање (чл.143), неовлашћено фотографисање (чл.144), неовлашћено објављивање туђих снимака (чл.145), неовлашћено прикупљање туђих података (чл.146),
- Кривична дела против уставног уређења и безбедности Рапублике Србије као што су: Позивање на насилну промену уставног уређења ( чл.309), Изазивање националне, расне и верске мржње (чл. 317)

.

- Кривична дела против јавног реда и мира, као што су: Изазивање панике и нереда (чл. 343), Неовлашћено организовање изара на срећу ( чл.352)
- Кривична дела против привреде, као што су: Одавање пословне тајне (чл. 240) и Фалсификовање и злоупотреба платних картица ( чл.243)
- Кривична дела против човечности и међународног права, као што је Трговина људима ( чл.388).[210]

Поред Кривичног законика, значајан нормативни акт представља Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[211], који уређује образовање, организацију, надлежност и овлашћења посебних организационих јединица државних органа органа ради откривања, кривичног гоњења и суђења ових кривичних дела.

Овај Закон у чл. 2 ст. 1 и 2 дефинише високотехнолошки криминал као вршење кривичних дела код којих се као објеакт или средство извршења јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци као и њихови производи у материјалном или електронском облику, под којима се подразумевају рачунарски програми и ауторска дела која се могу употребити у елекронском облику[212].

Овим законом се такође уређује и надлежност специјализованих државних органа који су задужени за поступање у овим случајевима, па се примењује се ради откривања, кривичног гоњења и суђења за:

1. кривична дела против безбедности рачунарских података одређена Кривичним закоником;
2. кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају

[210] Слијепчевић, Л. (2018). *Високотехнолошки криминал у домаћим и међународним прописима, с посебним освртом на одредбе Кривичног законика које су ступиле на снагу од 1. јуна 2017. и Конвенцију Савета Европе о високотехнолошком криминалу* [PDF]. Правосудна академија. (преузето 19.03.2026) https://www.pars.rs/public/Dokumenti/Publikacije/1458/Visokotehnoloski-kriminal-u-d%C0%BEm%C0%B0cim-i-m%C0%B5djun%C0%B0r%C0%8Dpisim%C0%B0-ljuba-slijepcevic_0.pdf?/

[211] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, („Сл. гласник РС“, бр. 61/2005, 104/2009, 10/2023, 10/2023 – др. закон и 9/2026).

[212] Ibid, чл. 1 ст.2 и 3

.

рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара;

3. кривична 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 криминала, у складу са чланом 2. став 1. овог закона[213].

Такође овим законом предвиђено је постојање специјализованих институција, као што су:

- Посебно одељење Вишег јавног тужилаштва у Београду за борбу против високотехнолошког криминала, надлежно за поступање у предметима високотехнолошког криминала на територији целе Републике Србије;
- Посебно одељење Вишег суда у Београду за високотехнолошки криминал, надлежно за суђење у овим предметима;
- Служба за борбу против високотехнолошког криминала Министарства унутрашњих послова, која представља специјализовану полицијску јединицу задужену за откривање и истрагу кривичних дела из ове области.[214]

Поред националних закона, Република Србија је ратификовала више међународних конвенција које имају значајну улогу у борби против сајбер криминала и кривичних дела која се врше на дарк вебу. Најзначајнији међународни инструмент у овој области је Конвенција Савета Европе о високотехнолошком криминалу (Будимпештанска конвенција) из 2001. године, коју је Србија ратификовала 2009. године. Поред основне конвенције, Србија је ратификовала и Додатни протокол уз Будимпештанску конвенцију о инкриминацији дела расистичке и ксенофобичне природе извршених путем рачунарских система из 2003. године, који проширује примену конвенције на кривична дела која укључују ширење расистичких и ксенофобичних материјала путем интернета. Такође, Република Србија је 2023. године ратификовала и Други додатни протокол уз

[213] Ibid, чл. 3
[214] Ibid, чл. 4, чл. 9, чл. 10 и 11

.

Будимпештанску конвенцију, који омогућава унапређену међународну сарадњу и ефикасније откривање електронских доказа. Поред ових инструмената, Србија је потписница и других међународних конвенција од значаја за борбу против криминала на интернету и Dark Web-у, као што је Конвенција Уједињених нација против транснационалног организованог криминала (Палермска конвенција) из 2000. године.

### 7.3. Проблеми и изазови у правној квалификацији дела извршених на Dark Web-у

Током последње деценије, експанзија дигиталних технологија и интернета учинила је да Dark Web постане један од најизазовнијих простора за извршење кривичних дела. Дела на Dark Web-у обухватају широк спектар активности – од трговине наркотицима и оружјем, преко крађе и продаје личних података, до ransomware напада и сајбер криминала као услуге (CaaS – Cybercrime as a Service). Специфичан карактер овог простора, укључујући анонимност, децентрализовану структуру и глобални карактер, ствара значајне изазове за правну квалификацију кривичних дела, односно одређивање која врста кривичног дела је почињена, ко је надлежан и које санкције се могу примењивати. Истраживање ових проблема омогућава разумевање ограничења националног и међународног законодавства, идентификацију потребе за усаглашавањем правних оквира и развој ефективних метода доказивања и процесуалног поступања у дигиталном окружењу

Један од највећих проблема представља идентификација починиоца. Dark Web користи технологије које прикривају IP адресу и географску локацију корисника, што отежава доказивање кривичне одговорности, утврђивање надлежности националних судова и примену националног и међународног кривичног права. Анонимност корисника значи да чак и када се идентификују налози или сервери, није могуће аутоматски утврдити стварног починиоца, што захтева сложене истражне мере као што су дигитална форензика, праћење криптовалутних трансакција и сарадња са интернет сервис провајдерима.

Докази у дигиталном облику често су фрагментарни, лако модификовани или смештени на серверима у различитим државама, што условљава потребу за међународном правном сарадњом, спровођење дигиталне форензике у складу са правилима о валидности

.

доказа, као и решавање питања везаних за аутентификацију и потврђивање оригиналности докумената.

Дела извршена на Dark Web-у често не спадају у традиционалне категорије кривичних дела. Један од изазова је преклапање кривичних дела, односно ситуације када једна активност може потпасти под више инкриминација, на пример трговина наркотицима која је истовремено може бити и организована криминална активност. Поред тога, многа дела немају физички контакт, као што су ransomware напади, крађа података и продаја CaaS услуга, и зато се не уклапају увек у класичне категорије као што су „крађа“ или „превара“. Додатно, територијална надлежност представља значајан проблем, јер сервери и жртве могу бити у различитим државама, што отежава примену националног кривичног закона и поставља питање да ли је надлежна држава жртве, починиоца или локација сервера

Национални закони често нису довољни за адекватну инкриминацију дела на Dark Web-у, будући да законодавство није увек прилагођено новим дигиталним облицима кривичних дела и споро реагује на развој технологија и нове методе извршења криминалних активности, што отежава санкционисање починилаца. Ефикасно санкционисање захтева унапређену међународну сарадњу кроз усаглашавање националних закона са међународним стандардима, ратификацију и примену конвенција као што је Будимпештанска конвенција о сајбер криминалу, као и учешће у међународним оперативним иницијативама, споразумима о екстрадицији и механизмима размене података.

.

## 8. ЗАКЉУЧАК

Интензиван развој информационо-комуникационих технологија у последњим деценијама довео је до дубоких трансформација у функционисању савременог друштва. Дигитализација комуникације, економије и друштвених односа омогућила је бржи проток информација, развој нових услуга и глобално повезивање појединаца и институција. Међутим, истовремено са овим позитивним процесима јавиле су се и нове могућности за вршење различитих облика криминалитета у дигиталном окружењу. Сајбер криминал се данас све више испољава као сложен, транснационалан и технолошки условљен облик криминалитета, који поставља значајне изазове пред савремене системе кривичноправне заштите.

У том контексту, Dark Web представља један од најспецифичнијихсегмената савременог дигиталног простора. Анализа његовог појма, структуре и техничких карактеристика показује да је реч о комплексном систему који функционише на принципима анонимности, енкрипције комуникације и децентрализоване мрежне архитектуре, које корисницима висок степен заштите идентитета и приватности, али истовремено стварају погодне услове за развој различитих незаконитих активности. Наведене техничке специфичности, у комбинацији са употребом криптовалута као средства плаћања, допринеле су формирању специфичног дигиталног екосистема у оквиру кога се одвијају бројне економске и друштвене интеракције.

Са криминолошког становишта, Dark Web представља посебно дигитално окружење у коме се формирају нови облици криминалног понашања, као и специфичне виртуелне криминалне заједнице. Унутар овог простора формиран је читав екосистем платформи, форума и илегалних тржишта који омогућавају размену информација, продају незаконитих производа и пружање криминалних услуга.

Посебно значајну улогу у том систему имају такозвани Dark Web маркети, који функционишу као илегална дигитална тржишта на којима се тргује опојним дрогама, оружјем, украденим подацима, малверима и другим незаконитим садржајима. Историјски развој ових тржишта, од појаве платформе Silk Road до савремених децентрализованих тржишта, указује на континуирану прилагодљивост криминалних структура технолошким

.

променама, али и њихову способност да се прилагођавају технолошким иновацијама и мерама које предузимају органи за спровођење закона.

Суочавање са криминалом на Dark Web-у представља један од значајних изазова савременог кривичног права и криминологије. Транснационална природа ових активности, употреба анонимних комуникационих мрежа, криптографских технологија и криптовалута, као и висока техничка сложеност дигиталних платформи, значајно отежавају идентификацију учинилаца, прикупљање дигиталних доказа и њихову процесну употребу. Због тога је неопходно континуирано унапређивати методе дигиталне форензике, развијати напредне аналитичке алате за праћење криминалних активности и јачати међународну сарадњу у области борбе против сајбер криминала.

Поред репресивних мера, значајну улогу у супротстављању криминалу на Dark Web-у имају и превентивни механизми. Криминолошки приступи превенцији, који обухватају примарну, секундарну и терцијарну превенцију, могу допринети смањењу ризика од злоупотребе дигиталних технологија и развоја криминалних активности у онлајн окружењу. Посебан значај имају активности усмерене на унапређење дигиталне писмености, подизање свести о ризицима који постоје у сајбер простору, као и јачање институционалних капацитета државних органа за откривање и сузбијање сајбер криминала.

Имајући у виду све наведено, може се закључити да Dark Web представља комплексно и динамично дигитално окружење које се континуирано развија и еволуира. Иако поседује потенцијал за легитимну употребу, истовремено носи и значајне ризике од злоупотребе у криминалне сврхе. Стога је неопходно континуирано унапређивати нормативни и институционални оквир за борбу против овог вида криминалитета, као и развијати нове криминолошке, правне и технолошке приступе његовом откривању и превенцији. Само кроз интегрисану сарадњу правних, безбедносних и научних институција, уз јачање међународне сарадње и примену савремених технолошких алата, могуће је ефикасно одговорити на изазове које Dark Web поставља пред савремено друштво и систем кривичноправне заштите.

.

## ЛИТЕРАТУРА

### Књиге и монографије


1. Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Northeastern University Press.
2. Akers, R. L. (2009). *Social learning and social structure* (Rev. ed.). Transaction Publishers.
3. Akers, R. L. (2011). Social learning theory. In F. T. Cullen, J. P. Wright, & K. R. Blevins
4. Akers, R. L. (2017). *Social learning and social structure* (2nd ed.). Routledge.
5. Bandura, A. (1977). *Social learning theory*. Prentice Hall.
6. Berners-Lee, T. (2000). *Weaving the web: The original design and ultimate destiny of the World Wide Web*. HarperCollins.
7. Castells, M. (2001). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press.
8. Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
9. Comer, D. (2013). *Internetworking with TCP/IP* (Vol. 1, 6th ed.). Pearson.
10. Durkheim, É. (1897). *Suicide: A study in sociology*. Routledge.
11. Ferrell, J., Hayward, K., & Young, J. (2015). *Cultural criminology: An invitation* (2nd ed.). Sage.
12. Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.
13. Guyau, J.-M. (1884). *Esquisse d'une morale sans obligation ni sanction*. Félix Alcan.
14. Holt, T. J. (2019). *Darknet markets*. Palgrave Macmillan.
15. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. (2018). *Cybercrime and digital forensics*. Routledge.
16. Jewkes, Y., & Yar, M. (2010). *Handbook of Internet crime*. Routledge.
17. Leukfeldt, R. (2018). *Cybercrime and social ties*. Routledge.
18. Matza, D. (1964). *Delinquency and drift*. Wiley.
19. Nearchou, N. (2023). *Combating crime on the dark web*. Packt Publishing.
20. Sageman, M. (2008). *Leaderless jihad*. University of Pennsylvania Press.
21. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson.
22. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

.

23. Wall, D. S. (2015). *Dark web: Exploring and mitigating criminal opportunities*. Routledge.

24. Yar, M. (2013). *Cybercrime and society* (2nd ed.). Sage.

**Научни радови**

25.Adel, A., & Norouzifard, M. (2024). Weaponization of cybercrime in the dark net. *Big Data and Cognitive Computing, 8*(8), 91. https://doi.org/10.3390/bdcc8080091

26. Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169–217.

27. Cerf, V., & Kahn, R. (1974). A protocol for packet network intercommunication. *IEEE Transactions on Communications, 22*(5), 637–648.

28. Clarke, R. V., & Cornish, D. B. (1985). Modelling offenders' decisions. *Crime and Justice, 6*, 147–185.

29. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

30. Décary-Hétu, D., & Quessy-Doré, O. (2017). Digital reputation in a criminal context. *Crime Science, 6*(1), 1–12.

31. Garcia, D. (2019). Personality traits of cybercriminals. *Psychological Reports, 122*(6), 1–15.

32. Gray, A. (2024). The thrill seekers of the digital underworld: Psychological motivations of dark web users and cybercriminals. *ResearchGate* (preprint).

33. Hay, C., & Meldrum, R. (2016). Low self-control and crime. *Criminal Justice and Behavior, 43*(4), 489–513.

34. Hinduja, S. (2007). Neutralization theory and online piracy. *Ethics and Information Technology, 9*(3), 187–204.

35. Johnson, M. (2022). Community dynamics in dark web forums. *Social Computing Journal*.

36. Kumar, A., & Somani, A. (2022). Dark web: A facilitator of crime? *ResearchGate* (preprint).

37. Lee, A., & Chen, Y. (2021). Cognitive autonomy and online information seeking. *Cyberpsychology Review*.

38. Martin, J. (2014). Lost on the Silk Road: Online drug distribution and cryptomarkets. *Criminology & Criminal Justice, 14*(3), 351–367.

39. Nightingale, S., et al. (2020). Understanding user behavior on the dark web. *Journal of Cybersecurity*.

40. Omer, T. (2019). Privacy activism and dark web utilization. *Information Security Journal*.

.

41. Smith, R., & Kumar, P. (2018). Illegal content consumption and internet behavior. *Deviant Behavior, 39*(12), 1–15.

42. Sykes, G. M., & Matza, D. (1957). Techniques of neutralization. *American Sociological Review, 22*(6), 664–670.

**Интернет и други извори**

43. ABC News. (2016, January 28). *Explainer: What is the dark net?* https://www.abc.net.au/news/2016-01-28/explainer-what-is-the-dark-net/7038878

44. Acronis. (2024). *Dark web cybersecurity best practices*. https://www.acronis.com

45. Adel, A., & Norouzifard, M. (2024). Weaponization of cybercrime in the dark net. *Big Data and Cognitive Computing, 8*(8), 91. https://www.mdpi.com/2504-2289/8/8/91

46. AIU. (n.d.). *Victimology in cyberspace*. https://www.aiu.edu

47. Anti-Phishing Working Group. (2024). *Phishing activity trends report*. https://apwg.org

48. Australian Institute of Criminology. (2021). *Illicit firearms and other weapons on darknet markets*. https://www.aic.gov.au

49. Brandefense. (n.d.). *Cybercrime-as-a-service*. https://brandefense.io

50. Brave. (n.d.). *Digital footprint*. https://brave.com

51. Chainalysis. (2024). *Crypto crime report*.

52. Chainalysis Team. (2023). *How darknet markets fought for users after Hydra*. https://www.chainalysis.com/blog/how-darknet-markets-fought-for-users-in-wake-of-hydra-collapse-2022/

53. Check Point. (n.d.). *Malware-as-a-service*. https://www.checkpoint.com

54. Control D. (2024). *Phishing statistics and industry trends*. https://controld.com/blog/phishing-statistics-industry-trends/

55. CRIF. (2024). *Cyber attacks data and dark web*. https://www.crif.com

56. CyberArrow. (2024). *Types of dark web*. https://www.cyberarrow.io

57. Cybercrime.rs. (n.d.). *Cybercrime in Serbia*. https://cybercrime.rs

58. Cybersecurity Coalition. (n.d.). *Cybercriminal profiles*. https://cybersecuritycoalition.be

59. Cybersecurity Dive. (2025). *Zero-day exploits rise*. https://www.cybersecuritydive.com

60. DeepStrike. (2025). *Zero-day exploit statistics*. https://deepstrike.io

.

61. DeepStrike. (n.d.). *How law enforcement tracks criminals on the dark web*. https://deepstrike.io/blog/how-law-enforcement-tracks-criminals-on-the-dark-web

62. eSecurity Planet. (2024). *Threat intelligence report*. https://www.esecurityplanet.com

63. Fakultet organizacije i informatike. (n.d.). *TOR i anonimizacijske mreže*. https://security.foi.hr

64. Federal Bureau of Investigation. (2024). *Internet Crime Report 2024*. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

65. Google Threat Intelligence Group, & Mandiant. (2024). *Year in review of zero-days exploited in-the-wild in 2023*.

66. Greenberg, A. (2017). How Dutch police took down Hansa. *Wired*. https://www.wired.com/story/hansa-dutch-police-sting-operation/

67. Group-IB. (n.d.). *Money mules*. https://www.group-ib.com

68. Handalage, U., & Prasanga, P. (2021). *Dark web review*. ResearchGate.

69. Haptic Networks. (2024). *Dark web threats*. https://haptic-networks.com

70. IBM. (n.d.). *What is the dark web?* https://www.ibm.com

71. International Labour Organization. (2022). *Global estimates of modern slavery*. https://www.ilo.org

72. INFosecurity Europe. (2024). *Generative AI and dark web*. https://www.infosecurityeurope.com

73. INTERPOL. (2023). *Global threat assessment on human trafficking and migrant smuggling*.

74. Kaspersky. (2026). *Phishing attacks statistics*. https://www.kaspersky.com

75. Microsoft. (n.d.). *What is cybercrime as a service (CaaS)?* https://www.microsoft.com

76. NordLayer. (n.d.). *What is dark AI?* https://nordlayer.com

77. NordStellar. (n.d.). *AlphaBay analysis*. https://nordstellar.com

78. Nisos. (n.d.). *Dark web cybercrime*. https://nisos.com

79. Norton. (n.d.). *Dark AI*. https://us.norton.com

80. Observer Research Foundation. (n.d.). *Dark web analysis*. https://www.orfonline.org

81. Office of the Director of National Intelligence. (2024). *Worldwide ransomware report*. https://www.dni.gov

82. Panda Security. (2024). *Dark web statistics*. https://www.pandasecurity.com

.

83.Petrosyan, A. (2025). *DDoS statistics*. Statista. https://www.statista.com/statistics/1557643/ddos-attacks-global-number/

84.Pideeco. (n.d.). *Dark web and money laundering*. https://pideeco.be

85. Sanctions.io. (n.d.). *Crypto money laundering*. https://www.sanctions.io

86. SozTheo. (n.d.). *Anomie theory*. https://soztheo.com

87. SozTheo. (n.d.). *Rational choice theory*. https://soztheo.com

88. Statista. (2025). *Distribution of cyberattacks worldwide*. https://www.statista.com

89. TechTarget. (n.d.). *Dark web definition*. https://www.techtarget.com

90. Tor Project. (n.d.). *Tor documentation*. https://www.torproject.org

91. TRM Labs. (2022). *Darknet markets*. https://www.trmlabs.com

92. United Nations Office on Drugs and Crime. (2020). *Drug trafficking report*. https://www.unodc.org

93. United Nations Office on Drugs and Crime. (2022/2024). *Global report on trafficking in persons*. https://digitallibrary.un.org/record/4069246/files/GLOTIP2024_BOOK.pdf?utm_source=chatgpt.com

94. United Nations Office on Drugs and Crime. (2025). *Cybercrime in 2025*. https://www.unodc.org

95. VIDA. (n.d.). *Digital literacy and security*. https://vida.id

96. XtendedView. (2024). *Cybersecurity statistics*. https://xtendedview.com

**Правни извори**

97. Конвенција Уједињених нација против транснационалног организованог криминала (Палермска конвенција). (2000). Уједињене нације. Потврђена у: „Службени лист СРЈ – Међународни уговори“, бр. 6/2001.

98. Генерална скупштина Уједињених нација. (2019). Резолуција 74/247: Борба против употребе информационо-комуникационих технологија у криминалне сврхе. Уједињене нације.

99. Генерална скупштина Уједињених нација. (2021). Резолуција 75/282: Борба против употребе информационо-комуникационих технологија у криминалне сврхе. Уједињене нације.

100. Конвенција Уједињених нација против сајбер криминала. (2024). Уједињене нације.

.

101. Савет Европе. (2001). Конвенција о сајбер криминалу (Будимпештанска конвенција). Потврђена у: „Службени гласник РС – Међународни уговори“, бр. 19/2009.

102. Савет Европе. (2003). Допунски протокол уз Конвенцију о сајбер криминалу, који се односи на инкриминацију дела расистичке и ксенофобне природе извршених путем рачунарских система. Потврђен у: „Службени гласник РС – Међународни уговори“, бр. 19/2009.

103. Савет Европе. (2021). Други допунски протокол уз Конвенцију о сајбер криминалу о појачаној сарадњи и откривању електронских доказа. Потврђен у: „Службени гласник РС – Међународни уговори“, бр. 14/2023.

104. 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, 35/2019, 94/2024).

105. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. („Службени гласник РС“, бр. 61/2005, 104/2009, 10/2023, 10/2023 – др. закон и 9/2026).

.

# САЖЕТАК

## Dark Web – дигитални простор извршења кривичних дела

Рад се бави свеобухватним криминолошким и правним сагледавањем Dark Web-а као специфичног сегмента интернет простора који, услед својих техничких карактеристика, омогућава висок степен анонимности и представља погодно окружење за вршење различитих облика криминалитета. Предмет истраживања обухвата карактеристике дигиталног окружења, облике криминалних активности и механизме функционисања криминалних мрежа на Dark Web-у.. Циљ рада је да се идентификују узроци, облици и механизми криминалитета на Dark Web-у, изазови са којима се суочавају органи кривичног гоњења у процесу његовог откривања и сузбијања као и да се процени ефикасност постојећег нормативног оквира на националном и међународном нивоу. У раду су примењени нормативно-правни, криминолошки, компаративни и дескриптивно-аналитички метод. Резултати истраживања указују да анонимност, енкрипција и децентрализованост значајно доприносе развоју савремених облика криминалитета, укључујући развој сложених облика организованог криминалитета, укључујући илегална дигитална тржишта и модел криминала као услуге („cybercrime-as-a-service“), те да постојећи правни и институционални механизми нису у потпуности прилагођени овим изазовима. Закључује се да је за ефикасну борбу против криминала на Dark Web-у неопходно унапређење правне регулативе, јачање техничких и институционалних капацитета надлежних органа, јачање међународне сарадње и примену превентивних мера.

**Кључне речи: Dark Web, сајбер криминал, анонимност, енкрипција, Tor мрежа, криптовалите, криминал као услуга, превенција криминалитета**

.


## SUMMARY

## Dark Web – A Digital Environment for the Commission of Criminal Offenses

The paper provides a comprehensive criminological and legal analysis of the Dark Web as a specific segment of the Internet, which, due to its technical characteristics, enables a high degree of anonymity and serves as a favorable environment for various forms of criminal activity. The research focuses on the features of the digital environment, types of criminal activities, and the mechanisms of criminal network operations on the Dark Web. The aim of the study is to identify the causes, forms, and mechanisms of crime on the Dark Web, the challenges faced by law enforcement authorities in detecting and combating these activities, and to assess the effectiveness of the existing legal framework at both national and international levels. The paper applies normative-legal, criminological, comparative, and descriptive-analytical methods. The results indicate that anonymity, encryption, and decentralization significantly contribute to the development of modern forms of criminality, including complex forms of organized crime, illicit digital marketplaces, and the "cybercrime-as-a-service" model. It is concluded that effective combat against Dark Web crime requires the improvement of legal regulations, strengthening of technical and institutional capacities of competent authorities, enhancement of international cooperation, and implementation of preventive measures.



**Keywords: Dark Web, cybercrime, anonymity, encryption, Tor network, cryptocurrencies, cybercrime-as-a-service, crime prevention**

.

## БИОГРАФИЈА СТУДЕНТА

Аутор мастер рада Ана Станојевић рођена је 10. јуна.2000. године у Нишу. Завршила је Основну школу „Радоје Домановић“ у Нишу, као носилац дипломе „Вук Караџић“. Природно-математички смер Гимназије „Светозар Марковић“ у Нишу завршила је такође као носилац дипломе „Вук Караџић“ и корисник државне стипендије. Уписала је Правни факултет Универзитета у Нишу школске 2018/2019 године и дипломирала 30. септембра. 2024. године са порсечном оценом 9,07, а исте године је уписала мастер студије на Правном факултету Универзитета у Нишу, смеру Право и информационе технологије.

Током школовања остварила је запажене резултате на такмичењима из роботике и интерфејс технологије, на којима је више пута освајала прва места на републичком нивоу. Учествовала је и на међународном такмичењу „Olympics Technical Creativity of Youth of Southeastern Europe“ (Зрењанин, 2014), где је освојила треће место. Такође је учествовала на више манифестација посвећених популаризацији науке, укључујући фестивал „Наук није баук“ у Нишу, „Ноћ истраживача“ у Нишу и Фестивал науке у Београду, на којем јој је 2018. године додељено признање „амбасадор науке“.

Током основних студија, у циљу стручног усавршавања, била је ангажована у адвокатској канцеларији на пословима администрације и комуникације са клијентима. Након завршетка студија, од новембра 2024. године обавља приправнички стаж у Вишем суду у Нишу, у својству приправника-волонтера. Говори енглески и немачки језик.