УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

ЗЛОУПОТРЕБА МРАЧНЕ СТРАНЕ ИНТЕРНЕТА

ДИПЛОМСКИ РАД

МЕНТОР:

др Ана Ковачевић

ванредни професор

КАНДИДАТ:

Мартина Трајковић

Београд, 2017. године

На самом почетку желим да се захвалим својој професорки и менторки Ани Ковачевић на саветима и сугестијама приликом писања овог рада.

Садржај

1. Увод

У данашње време број корисника интернета се све више повећава. Тешко је замислиити домаћинство које нема рачунар или приступ интернету. Интернет користе особе свих узраста- од деце, до стараца. Некима је он извор забаве, неки интернет користе како би ступили у контакт са пријатељима, а некима је неопходан у обављању послова. Без обзира на разлог због којег се користи, може се рећи да је у 21. веку интернет постао неминовност.

Прогрес интернета и његова све већа примена несумњиво утичу на животе људи. Од потребне информације дели нас само један клик, пријатељ из другог града или државе више не делује тако далеко, можемо радити из своје дневне собе. Међутим и поред многих погодности које нам је интернет донео, не смемо занемарити његову лошу страну и не смемо га узимати здраво за готово. У рукама злонамерних појединаца или група он представља једно од најмоћнијих средстава нарушавања безбедности како држава, тако и међународне заједнице. Посебан проблем на интернету представља такозвани Deep Web, а уоквиру њега Darknet који је због анонимности својих корисника постао упориште илегалних активности и велика претња међународној заједници. У даљем раду објаснићу начин коришћења Darknet-а, као и начин његове злоупотребе.

2. Површински интернет, Deep Web и Darknet

Интернет представља један од основних појмова модерне технологије. Честа заблуда је поистовећивање интернета са једном великом мрежом повезаних рачунара. Разлика је у томе што се под интернетом подразумева скуп који обједињује све ове мреже што значи да технички, интернет сам по себи не означава јединствену мрежу.

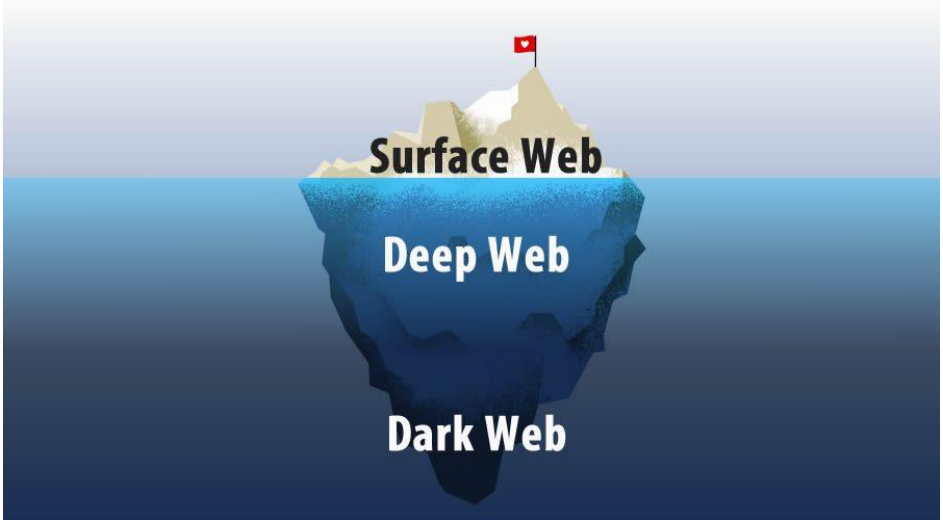
Класификација интернета се врши преко слојева. Сваки од ових слојева (или нивоа) представља сложеност коју је потребно достићи да би се постигла веза са одређеним рачунаром. Сваки рачунар повезан на ову глобалну мрежу свих мрежа поседује јединствени идентификациони код који се назива интернет адресом. Да би се олакшало проналажење тражене адресе уведен је систем интернет домена који замењује бројевну адресу (192.168.2.1 нпр.) неким прихватљивијим именом (www.google.com). Тако на пример, домен означава основни слој, који указује на регион државе у којој се рачунар налази. На сличан начин су универзитети у Београду повезани доменом ac.bg.rs. Интернет адресе односно рачунари повезани путем интернета којима је могуће приступити помоћу свог домена чине такозвани површински слој интернета. Треба обратити пажњу да површински интернет уједно чине они домени (сајтови) који су индексирани путем интернет претраживача. То значи да је њихов садржај, назив и сертификат поверења доступан сваком претраживачу који корисници интернета користе.

Дакле, уколико је некоме потребна информација о доласку аутобуса на релацији Лесковац – Београд, једноставним уносом параметара претраге, Google (или неки други претраживач) пролази кроз индексиране адресе и проверава да ли се на неком од њих налази потребна информација. Само индексирање страница се обавља путем регистровања интернет странице светској организацији за домене. Наравно, уколико је нека страница слабо рангирана својим индексом, односно уколико је саобраћај дате странице слаб, може се десити да се као резултат неке претраге уопште не појави у оквиру претраживача, али

то не мора значити да она не чини део површинског интернета. Странице овог слоја садрже стандардне нивое сертификата који нуде безбедност посетиоцу. Сама локација сервера (рачунара задуженог за одржавање сајта) у овом случају није скривена.

Други слој чине неиндексиране странице односно Deep Web. Да би се приступило овим страницама, потребно је знати прецизно навести адресу самог рачунара коме се приступа, и овакве странице се неће појавити као резултат интернет претраге. Први проблем на који се наилази приликом приступа оваквој страници је техничке природе а тиче се саме гаранције протекције корисника који јој приступа. Модерни интернет прегледачи без проблема успевају да разоткрију овакве странице и укажу на пропусте безбедности. У већини случаја, овакве странице јесу потпуно безопасне јер се многе пријатељски настројене странице налазе на овом нивоу из финансијских разлога у чију дубину нећу залазити.

Посебан слој Deep Web-а чини Darknet. Darknet се дефинише као део интернета чији је приступ омогућен само помоћу специјалних програма. Разлог због неопходности ових програма лежи у чињеници да је сам садржај ових сајтова шифрован на посебан начин. У оквиру ових посебних програма, постоји јако слаба разлика између њихових могућности. Њихова перформанса остаје иста и зависи искључиво од нивоа скривености странице која се у датом тренутку посећује. Неки од ових програма нуде одређен систем заштите и гаранције анонимности корисницима, али у пракси се показало да приступ овом делу интернета треба узети са великим ризиком.



Слика 1 - Однос величине површинског интернета, Deep Web-а и Darknet-а (Sabarinath, 2017).

Однос величине површинског интернета и Deep Web-а се може представити као санту леда, где површински интернет јесте оно изнад воде, оно што је видљиво, док све оно што се налази испод воде, што је невидљиво представља Deep Web, а у оквиру тог невидљивог дела налази се Darknet[1] (Слика 1). Наводи се податак да се на површинском интернету налази само 4% укупног интернет садржаја, док се остатак налази на мрачној страни интернета (A Complete Guide about the Deep Web, 2016).

3.1. Начин приступања Darknet-u

Сам Darknet је конципиран исто као и површински интернет. У оквиру њега такође постоје претраживачи, само су њихови индекси сада фокусирани само на странице Darknet-а. Опет, може се догодити да се неке странице Darknet-а не појављују као резултат претраге јер нису индексиране. Овај проблем се решава постојањем такозване скривене википедије**.** Ова страница је вероватно еквивалентна страници Google-а по својој посећиваности на Darknet-u. Сам приступ овој страници се врши преко посебног линка

[1] На слици можемо видети назив Dark Web који је, заправо, синоним појму Darknet.

који се састоји од карактера и симбола који се мења након неког временског периода и до кога се долази преко разних форума површинског интернета.

Скривена википедија нуди неке од најтраженијих страница Darknet-а који се, опет, рангирају на овој страници путем својих донација. За разлику од стандардног Google сајта, не постоји корпорација која се налази иза саме скривене википедије или уједињеног Darknet-а већ је сарадња између различитих сајтова заснована на узајамном поверењу. Међутим, одсуством сервиса који контролише саобраћај ове мреже, додатно се успорава брзина протока података кроз њу услед не синхронизације између протокла.

Сајтови који чине мрачан део Darknet-а се често ословљавају *Onion* сајтовима јер се већина њих завршава овим доменом. Наравно, домен .onion није регистрован у оквиру светске организације за давање домена па се његова екстензија може користити само у оквиру специјалних програма који су горе описани. Један од разлога коришћења овог домена је могућност давања смислених назива сајтовима што би без њега било практично немогуће.

Једном пронађена .onion адреса не може се отворити у, нама добро познатим, претраживачима. За приступ Darknet-u и отварању .onion адреса неопходан је посебан софтвер попут Tor-a, I2P or Freenet-a. У највећем броју случаја користи се Top, јер је најједноставнији за коришћење.

Tor је слободан софтвер за омогућавање анонимне комуникације. Он обезбеђује интернет саобраћај кроз слободну, светску волонтерску мрежу састављену од више од шест хиљада штафета како би прикрили корисникову локацију и употребу од стране било кога ко надгледа мрежу, или врши контролу саобраћаја. Основан је од стране америчке морнарице како би се омогућило анонимно комуницирање. Међутим коришћење Tora довело је и до великих безбедносних проблема међународне заједнице о чему ће бити речи у овом раду.

3.2. Bitcoin као валута на Darknet-u

Bitcoin представља скуп концепата и технологија који чине основу дигиталне валуте. Јединице ове валуте се зову bitcoin-i и користе се за складиштење и преноса своје вредности од једног корисника до другог путем интернета. Корисници који су у поседовању извесне количине bitcoin-a комуницирају путем низа установљених правила које се називају протоколи. Дакле, да би два интернет корисника била у стању да на било који начин врше размену bitcoin-a, неопходно је да се успоставе одређени кораци ауторизације.

За разлику од других валута, bitcoin је потпуно виртуелан. Не постоји физички новчић нити постоји електронски облик истог. Можда је најбољи начин замислити количину новца у bitcoin-има као низове наизглед насумично наређаних слова и бројева. Да би се тај низ приближио корисницима, свакој јединици bitcoin-a се додељује кључ којим корисник потврђује своје поседовање истог. Ови кључеви су најчешће чувани на рачунарима корисника. Поседовање овог кључа откључава трансакцију.

Bitcoin се преносе такозваним P2P (енг. Peer to Peer) системом (Марић, 2015). Peer to Peer систем би се најбоље могао превести као директна веза између два корисника. Под корисником се подразумева индивидуа која поседује количину bitcoin-a и која је притом "повезана" на интернет. Ова директна веза означава да не постоји централни сервер или тачка која има контролу над протоком података од једног корисника ка другом. На овај начин корисници остају анонимни, што поспешује куповину и пружање услуга на невидљивом интернету.

Кориснике често ословљавамо као "чвор везе" или "теме" (енг. node). Ово долази из терминологије рачунарских мрежа. Уколико бисмо представили P2P мрежу као граф где тачке ("чворови") представљају кориснике а линије које спајају два чвора интернет везу, онда се добија реална слика функционисања ове методе. Да би податак стигао од једног чвора до другог, потребно је пронаћи најкраћи пут од корисника који шаље до корисника који прима тај податак. Подаци који се шаљу се деле на мале пакете и сваки се шаље посебно, а склапају се тек када стигну до свог циља. На овај начин је оправдано

прослеђивање података који стижу до чвора коме нису намењени. Иако су сви чворови на мрежи једнаки у смислу могућности коју им мрежа пружа, постоји четири врсте чворова на P2P топологији мрежа у зависности од тога да ли су чворови сами корисници (физичка лица) или мрежни контролори или можда рудари.

Bitcoin-i се стварају у процесу који се назива рударење (енг. mining) који укључује решавање одређених математичких проблема док се процес трансакције одвија. Дакле, сваки корисник у подмрежи интернета коју називамо bitcoin мрежом може бити рудар користећи свој рачунар како би пратио и потврдио трансакцију. Када неки корисник потврди да је трансакција између нека друга два корисника мреже успешна, он је награђен делом валуте. У просеку, на сваких десет минута, неко је у стању да потврди макар једну трансакцију у том временском интервалу и на тај начин је награђен малом свотом потпуно нових bitcoin-a. Суштина је у томе да се на овај начин уклања нестабилност валуте (валута није повезана ни са каквом државом или главном банком), а и сама потреба за присуством посредника је отклоњена овом методом.

Први проблем који се може јавити приликом рударења јесте злоупотреба. Многи корисници који покушавају да на овај начин зараде неки део bitcoin-a се удружују у тимове и при том повећавају своје шансе за добитак малог процента. Ово се завршава тако што се сама провера аутентичности сведе на такозване DDoS нападе рачунара клијента у циљу провере што већег броја трансакције у минималном времену. Међутим, показује се да је ова врста напада прилично неуспешна узимајући у обзир да на самој bitcoin мрежи не постоји толики број трансакција у јединици времена да би се оваква делатност исплатила (Johnson Benjamin, 2014).

Протокол bitcoin-a укључује уграђене алгоритме који регулишу обављање посла рудара преко целе мреже. Цео систем је осмишљен динамички тако да без обзира на количину људи која прати актуелну трансакцију, на десет минута ће само један добити награду. Овај протокол такође удвостручује време потребно за стварање новог bitcoin-a сваке године, а такође и ограничава број тренутно активираних bitcoin-a. Укупан број bitcoin-a који може постојати је 21 милион новчића. Ова експоненцијална метода нам омогућава да видимо да ће се до 2140 године створити количина bitcoin-a једна својој граници, односно 21 милион новчића. Обзиром на успоравање времена потребног да се

створи нова јединица валуте, онемогућава се виртуелна инфлација, односно “штампање” већег броја новчаних јединица оједном.

Bitcoin мрежа је почела са радом 2009, основана је од стране лица, или групе људи под псеудонимом Сатоши Накамото (Bitcoin) и од тада је проверавана од стране многих других програмера. Дистрибуција рачуница који омогућавају безбедност bitcoin-a је од тада експоненцијално порасла. Укупно тржиште bitcoin-a тренутно вреди између 5 милијарди и 10 милијарди америчких долара, у зависности од тренутног односа те две валуте. Највећа трансакција испраћена у bitcoin мрежи је износила 150 милиона америчких долара која је безбедно стигла до свог анонимног корисника.

Сатоши Накамото се повукао из јавности у априлу 2011, остављајући одговорност развоја кода и мреже групи волонтера (Bitcoin). Идентитет особе или групе која је иза bitcoin-a је и даље непозната.

Вредност bitcoin-a се стално мења, али може се рећи да је од свог настанка па до данас вредност знатно порасла.

Слика 2 - График приказује вредност bitcoin-a од 2010. године до 12.10.2017 (Bitcoin (USD) Price) .

На основу графика (Слика 2) се може видети да је на самом почетку вредност ове дигиталне валуте била скоро па незнатна, 0.06 америчких долара, да би за седам година њена вредност знатно порасла, дванаестог октобра 2017. године вредност bitcoin-а износи 5, 184.30 америчких долара и предвиђа се даљи пораст.

Треба напоменути и то да ово није једини начин плаћања на Darknet-u. Неки маркети дозвољавају плаћање и кредитном картицом. Међутим, ако се узме у обзир могућност праћења приликом плаћања кредитном картицом, јасно је да купци избегавају овај начин и прибегавају плаћањем у bitcoin-има, пре свега због његове анонимности, .

4. Darknet маркети

Најочигледнију злоупотребу Darknet-а представљају сајтови који пружају најразличитије производе и услуге, познатији као Darknet маркети. Анонимни корисници на овим сајтовима могу да наруче све, од опојних дрога до убиства неког лица. Иако представљају велики изазов, ризик и претњу по безбедност не само државе, већ читаве међународне заједнице, још увек нису пронађена адекватна стретства и методе са супротстављање овом облику угрожавања. Један од разлога јесте начин плаћања. Као што сам већ објаснила, плаћање на Darknet-u се обавља пре свега крипто валутом званом bitcoin. На другом месту ту је такозвани PGP (pretty good privacy), који се преводи као прилично добра приватност (Dean, Dark Markets: How to Buy Things from the Deep Web's Black Markets). Користи се како би се шифровале поруке између продаваца и купаца, и онемогућава трећим лицима да стекну увид у њихову комуникацију. Најважнију ствар за шифровање представља адреса за испоруку, јер се то, очито, може користити за повезивање куповине и купца. Треба пазити на Darknet маркете која траже да се сачува адреса за испоруку на самом сајту или да се комуницира са продавцима без коришћења шифровања, јер би то могло да доведе до опасности од праћења

Упознати смо и са преварама приликом куповине на интернету. Многи сајтови и на површинском интернету се суочавају са овим проблемом. Након плаћања од стране купца, купљени предмет се може или не мора послати. Нпр. случај на ebay-u где је уместо купљеног телефона, купцу у кутији стигла цигла. Како би спречили овај вид злоупотребе Darknet маркети су увели новину, такозвану трећу странку, арбитара, који посредује између купца и продавца. Трећа странка преузима контролу над bitcoin-има којима се плаћа, све док купац не обавести да је успешно примио пакет. Уколико производ не стигне, о томе се обавештава трећа странка, и обезбеђује се повраћај новца (Dean, Dark Markets: How to Buy Things from the Deep Web's Black Markets, 2015). На овај начин се онемогућава сваки вид злоупотребе.

Задобијање поверења од стране купаца је веома важан и озбиљан посао. Иако на Darknet-u постоји мноштво сајтова који пружају свакојаке услуге, нису сви подједнако успешни. Darknet маркети са великим бројем купаца привлаче пажњу јавности, пре свега различитих агенција и међународних организација које се боре против њих. Иако су многи маркети стекли изузетну "популарност" и остварили невероватну корист, велики број њих је угашен операцијама у којима је учествовао већи број међународних организација и владиних агенција, о чему ће касније бити речи.

5. Облици угрожавања на Darknet-u

Најочигледнија злоупотреба Deep Web-а одвија се на Darknet-u. Већ сам напоменула да се на Darknet-u може наручити све, од опојних дрога до нечијег убиства. Иако делује нестварно и превише несхватљиво како да то да нас један клик дели од килограма кокаина, или било чега што смо наручили морам напоменути да се ове ствари дешавају и ван виртуелног света. Велики број "уличних криминалаца" је ухапшено, по најразличитијим основама. Управо због тог страха да буду ухваћени, људи се окрећу куповини на Darknet-u. Нема више сусрета са "дилером", или са било којом особом која пружа одређену услугу или продаје одређени производ. На овај начин анонимност је загарантована, а производе се добијају у поштанском сандучићу. Такође морам напоменути да пружање услуга и производа на Darknet-u није једини вид његове злоупотребе. Један од већих, ако не и највећи проблем представља деловање терористичких организација на Darknet-u.

У овом делу посебно ћу образложити неке видове злоупотребе Darknet-а, пре свега:

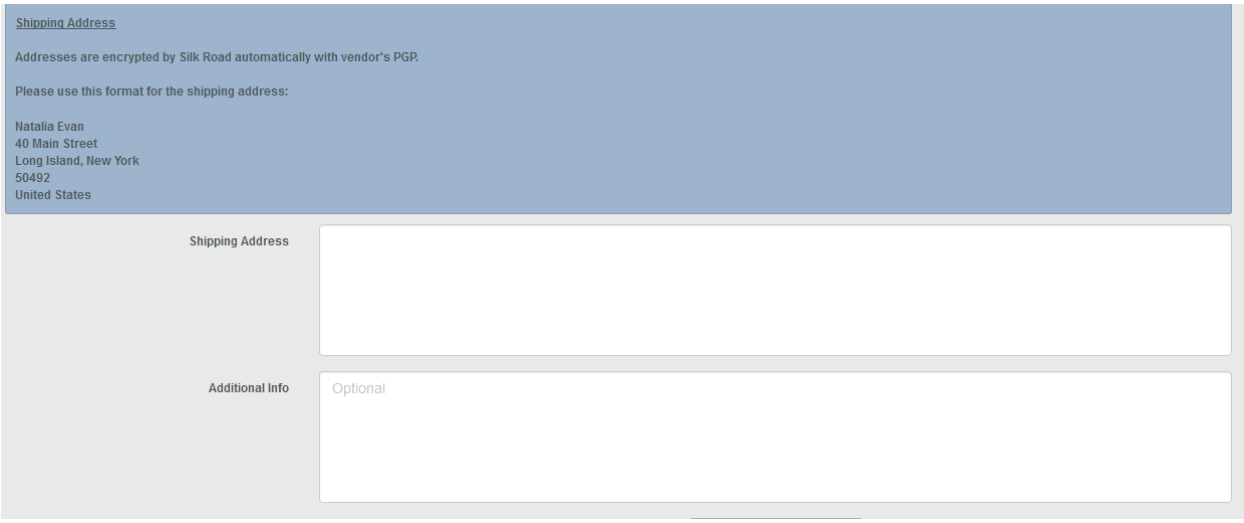
- Трговину наркотицима;
- Трговину оружјем;
- Трговину људима;
- Наручивање убиства;
- Пружање хакерских услуга;
- Фалсификовање докумената;
- Дечију порнографија;
- Тероризам.

5.1. Трговина наркотицима

Трговина наркотицима обухвата читаву делатност производње и дистрибуције наркотика. У Кривичном законику Републике Србије као кривично дело наводи се неовлашћена производња и стављање у промет опојних дрога (Службени гласник РС, 2005). Кривчни законик предвиђа низ инкриминисаних радњи које чине биће овог кривичног дела. Као инкриминисане радње наводе се:

- неовлашћена производња, прерада, продаја супстанци или препарата који су проглашени за опојне дроге;
- неовлашћено узгајање мака или психоактивног конопља, као и било које друге биљке из које се добија опојна дрога или које и сама садржи опојну дрогу;
- неовлашћена набавка, поседовање или давање на употребу опреме, материјала и супстанци које се користе у производњи опојних дрога.

Слика 3 - Регистрација на Darknet маркету Silkroad 3.0. (Silkroad 3.0.).



Слика 4 - Начин остављања адресе на Darknet маркету Silkroad 3.0. (Silkroad 3.0.).

Трговина наркотицима на Darknet-u, обавља се преко Darknet маркета. Процес куповине је једноставан, ништа другачији од куповине на било ком другом сајту са површинског интернета. Први корак јесте регистрација (Слика 3) на неком од Darknet маркета, након тога се тражи жељени производ, и на самом крају се оставља адреса (Слика 4) на којој тај производ треба да се испоручи. Након одређеног времена производ долази на кућну адресу.

Купљена дрога може стићи у јако необичним пакетима, попут фото албума, диска, или разгледнице. На овај начин обмањују се цариници и дрога несметано пролази границу.

На Darknet-u постоји већи број Darknet маркета који се баве продајом наркотика. Један од најпознатијих је, свакако, Silkroad 3.0.

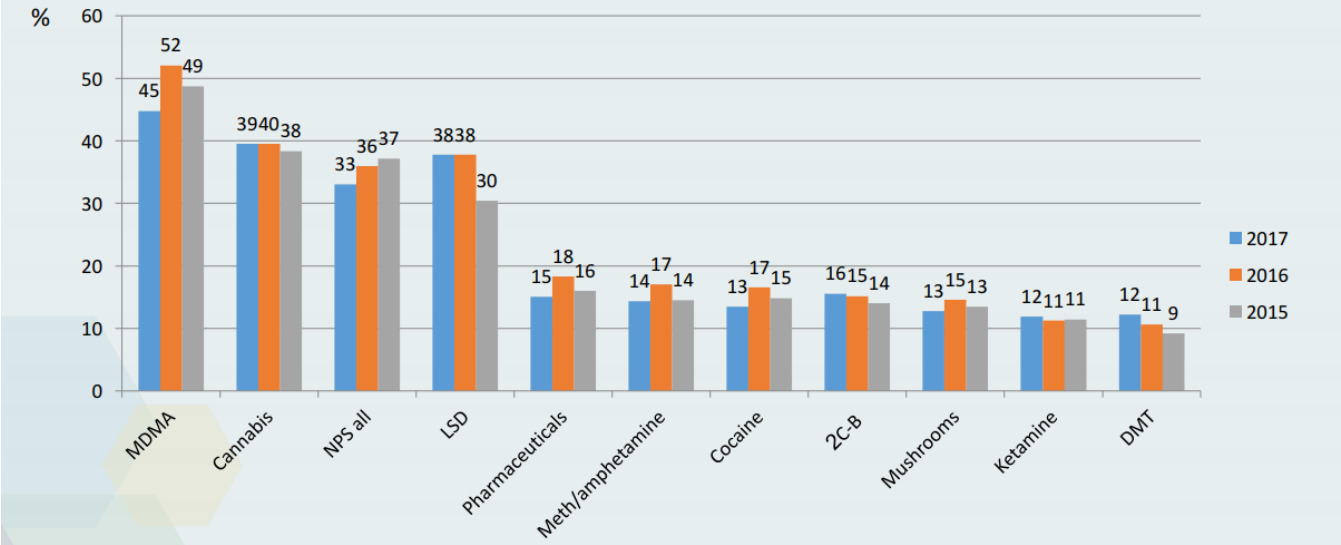
Silkroad 3.0 је наследник првобитног Silkroad-a, као и Silkroad-a 2.0. Претходнике Silkroad-a 3.0 су угасиле америчке власти у сарадњи са међународним организацијама.. Silkroad је био први Darknet маркет, познатији као платформа за продавање дроге. Основан је у фебруару 2011. године, а угашен у октобру 2013 (Silkroad). Silkroad 2.0 је основан у новембру 2013. године, а угашен је у новембру 2014. године (Silkroad). Након

тога је основан Silkroad 3.0 који и после свих падова његових претходника још увек функционише.

Оно што је интересантно управо код овог Darknet маркета јесте његова заступљеност у широј јавности, управо због велике фаме која се дигла приликом хапшења наводног главног администратора Silkroad-a. У својој првој акцији агенти ФБИ-ја су након дуге борбе и многобројних покушаја успели да уђу у траг наводном администратору овог сајта Росу Вилијаму Улбрихту. Рос Вилијам Улбрихт је на Silkroad-u био познат под својим псеудонимом Dread Pirate Roberts (Ross Ulbricht). Наводно је сам водио читав Darknet маркет и старао да сваки купац буде задовољан. Након његовог хапшења, и затварања сајта од стране ФБИ-ја, појавио се Silkroad 2.0. Администратор новог сајта је преузео Улбрихтов псеудоним. У навођењу чињеница повоодом акције ФБИ-ја и хапшењу Роса Вилијама Улбрихра користила сам реч "наводни администратор", "наводни оснивач", јер сам и свих чланака, вести и документараца стекла утисак да читав тај комплексан посао никако није могао да буде вођен од стране једне особе.

Оно што је веома важно да се напомене су управо производи који се могу наћи на овом Darknet маркету. Silkroad је маркет који се бави искључиво продајом наркотика. Продаја оружја, људи, фалсификованих докумената је забрањена.

Глобално истраживање о конзумирању наркотика из 2016. године наводи да је куповина наркотика на Darknet маркетима у порасту (Global Drug Survey 2016, 2016). Једна од десет особа је куповала наркотике на Darknet маркетима, док је пет посто испитаника навело да дрогу нису купили како би је конзумирали, већ су само желели да је наруче и виде како ће им стићи. (Global Drug Survey 2016, 2016).



Слика 5 - График приказује најчешће куповане наркотике на Darknet маркетима у 2015., 2016. и 2017. години (Winstock A, Barratt M, Ferris J, Maier L., 2017).

Глобално истраживање о конзумирању наркотика из 2017. године наводи да је најпродаванији наркотик на Darknet маркетима управо МДМА, након тога канабис, нове психоактивне супстанце, ЛСД, лекови, метамфетамин, кокаин, 2Ц-Б, печурке, кетамин, и ДМТ (Слика 5).

5.2. Трговина оружјем

Под појмом оружја у погледу Закона о оружју и муницији сматра се ручно преносива направа израђена или прилагођена да под притиском ваздуха, барутних и других гасова или дугог потисног средства може избацити зрно, куглу, сачму или неки други пројектил, односно распршити гас или течност и друга направа која је намењена за самоодбрану или напад, лов или спорт (Службени гласник РС, 1992). Оно представља средство опасно по живот, здравље и телесни интегритет људи.

Законом о оружју и муницији прописано је ко и под којим условима може легално набавити, држати и са собом носити оружје. Међутим поред легално набављеног оружја

можемо говорити и о оружју набављеном на црном тржишту. Оваква трговина оружјем, сматра се илегалном и представља велики изазов, ризик и претњу по безбедност сваке државе.

Сем Метјуз, новинар, урадио је интервју са једним од администратора Darknet маркета који се бави трговином оружја. На питање како шаљу оружје, речено му је да се најчешће користе електрични алати, тако што се алат се растави и празан део попуни деловима оружја и након тога поново састави, пре свега се користе бушилице, тестере, али и компјутере и намештај, а најважније је да се пронађе предмет са сличном густином метала као и само оружје како би се обманuo скенер, такође оружје долази без уља како га не би детектовали приликом тражења експлозивног материјала (Matthews, 2014).

Слика 6 - Насловна страна једног од Darknet маркета за продају оружја (Luckp 47 shop).

Процес наручивања оружја је исти као и код наручивања наркотика са Darknet маркета - регистрација, одабир жељеног производа и остављање адресе. Darknet маркети пружају велики избор најразличитијег оружја, пре свега пиштоља, митраљеза, пушака (Слика 6).

Илегално набављање оружја преко Darknet маркета представља велику опасност по међународни мир и безбедност, јер се на овај начин оружјем снабдевају и терористичке организације које свако представљају велики изазов, ризик и претњу.

Слика 7 - Sweguns - сајт на коме се врши откуп пиштоља (Sweguns).

Поред могућности куповине оружја на Darknet маркетима, могуће га је и продати. Darknet маркет Sweguns врши откуп пиштоља по цени од 120 америчких долара (Слика 7).

5.3. Трговина људима

Трговина људима представља једну од најуноснијих криминалних активности, поред трговине наркотицима и оружјем и као таква представља не само државни, већ и међународни проблем.

Појам трговине људима је први пут дефинисан Протоколом Уједињених нација за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминалитета из 2000. године. Овим протоколом под трговином људима се подразумева врбовање, превожење, пребацивање, скривање и примање лица, путем претње силом или употребом силе или других облика присиле, отмице, преваре, обмане, злоупотребе

овлашћења или тешког положаја или давања или примања новца или користи да би се добио пристанак лица које има контролу над другим лицем, с циљем експлоатације (Протокол Уједињених нација за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминалитета из 2000. године, 2000).

У Кривичном законику Републике Србије појам трговина људима обухвата употребу силе или претње како би се друго лице довело или одржало у заблуди, и то злоупотребом овлашћења, поверења, односа зависности, тешких прилика тог лица, као и врбовање, превожење, пребацивање, предавање, продавање, куповање, посредовање у продаји, сакривање или држање лица на било који други начин, све то у циљу експлоатације његовог рада, принудног рада, вршења кривичних дела, проституције или друге врсте сексуалне експлоатације, просјачења, употребе у порнографске сврхе, успостављања ропског или њему сличног односа, ради одузимања органа или дела тела или ради коришћења у оружаним сукобима (Службени гласник РС, 2005).

Трговина људима је присутна и на интернету, како на површинском, тако и на Deep Web-u, односно на једном његовом делу- Darknet-u. На Darknet-u се организују тајне аукције, на којима се тргује људима. У свом истраживању нисам наишла на такве сајтове,међутим, новинари су истраживали ову тему. У јулу 2015. године један новинар је успео да уђе у траг озлоглашеној криминалној Darknet групи Црна смрт која се бави трговином људима. У свом чланку је испричао то непријатно искуство и навео да је на њиховом сајту обављена аукција младе девојке отете у Паризу, а као доказ њеног постојања биле су приложене слике (Motherboard, 2015).

Алармиране овом ситуацијом, многе државе међународне заједнице су се укључиле у активном раду против трговине људима на интернету, али и Darknet-u. Један од најзначајних помака јесте активност DARPA-e (Defense Advanced Research Projects Agency) која ради на вишегодишњем пројекту под називом Memex program (Pellerin). Иако још увек није модификован за функционисање на Darknet-u, постоје изгледи да ће у будућем периоду моћи да помогне и у спречавању трговине људима на овој мрачној страни интернета.

5.4. Наручивање убиства

Наручивање убиства, најједноставније речено, преставља радњу у којој лице наручује и плаћа плаћеном убици убиство неке одређене особе. Наручивање убиства није нова појава, њу није изнедрио Darknet, али је постала знатно олакшана његовом употребом. Постоје бројни сајтови на Darknet-u који се баве пружањем ових услуга. На својим сајтовима се хвале својим "успесима". За одређену суму новца могуће је наручивање не само убиства, већ других радњи који доводе до уништења телесног интегритета неке особе.

Слика 8 - Ценовник услуга са Darknet маркета Slayers Hitman (Slayers assasination and life ruining services).

На једном од Darknet маркета који се бави пружањем ових услуга објављен је ценовник (Слика 8) и могуће је наручити убиство, уништавање нечијег живота, али и бројне друге услуге. Убиство се може извршити ватреним и хладним оружјем, отровоом, или мучењем, под уништавањем живота мисли се на напад киселином, остављање ожиљака на лицу, сакаћење, ослепљивање неког лица или пак кастрација, док се под осталим услугама мисли на мучење, али без убијања, силовање, физичко насиље, или само заплашивање (Слика 8).

Несумњиво је да ово представља велико угрожавање наше личне безбедности. За одређену количину новца, свако од нас може бити жртва плаћеног убице. И од тога нас

дели један клик наручиоца. Анонимност плаћених убица, а и наручиоца отежавају посао државних органа у борби против овог облика угрожавања.

5.5. Пружање хакерских услуга

Све већа популаризација интернета и умрежавање корисника на целој планети довело је до појаве особа које покушавају да из различитих разлога искористе сигурносне пропусте у системима. Те особе називамо хакерима. Хакер не мора нужно да наноси штету систему, стога се може направити поделу између њих на:

- Хакере са белим шеширом;
- Хакере са сивим шеширом;
- Хакере са црним шеширом.

Израз хакер с белим шеширом или етички хакер у области информационих технологија, јесте лице које је против злоупотребе рачунарких система. Овај термин се често користи да се опишу они који покушавају да продру у туђе системе и мреже како би помогли власницима тих система да постану свесни сигурносних пропуста, док хакери с белим шеширима покушавају да одбране рачунарске системе, хакери с црним шеширима тј. злонамерни хакери-„лоши момци“ – покушавају да упадну у туђе мреже и системе, украду поверљиве информације и/или нанесу неку штету (Плескоњић, 2010). Хакери са сивим шеширом упадају у туђе мреже и системе како би показали своје умеће и покушали да продају своје услуге.

Из овога се може закључити да се на Darknet-u могу наћи како хакери са сивим, тако и хакери са црним шеширом. За одређену суму новца ове особе могу да од рачунара направе играчку, која ће играти само по њиховим правилима. На Darknet-u се могу наћи бројни сајтови на којима се пружају хакерске ове услуге.

На једном од Darknet сајтова, Rent-A-Hacker, навооди се на шта је хакер спреман (Rent-A-Hacker):

- *DDoS напади;*
- *економска шпијунажа;*
- *набављање нечијих приватних информација;*
- *уништавање непријатеља нпр. финансијски;*
- *подметање дечије порнографије на рачунар неког лица.*

Product	Price	Quantity
Small Job like Email, Facebook etc hacking	200 EUR = 0.049 ฿	1 X Buy now
Medium-Large Job, ruining people, espionage, website hacking etc	500 EUR = 0.123 ฿	1 X Buy now
Large job which takes a few days or multiple jobs	800 EUR = 0.197 ฿	1 X Buy now

Слика 9 Ценовник услуга са Darknet маркета Rent-A-Hacker (Rent-A-Hacker).

Цене услуга варирају од тога шта купац жели. Хаковање e-mail адресе или Facebook налога кошта 200еура, уништавање неке особе, хаковање[2] интернет сајта или шпијунажа 500 еура, док неки већи посао, за који је потребно неколико дана кошта 800 еура (Слика 9).

5.6. Фалсификовање докумената

Могућност фалсификовања докумената алармирало је читаву међународну заједницу. Добро одрађени "фалсификати" омогућавају лицима да остваре одређена права

[2] . Под појмом хаковање подразумева се неауторизовани приступ одређеном компјутеру или систему.

која им иначе не припадају. То може бити приступ одређеном банковном рачуну, добијање лажних личних карата, или пасоша, као и добијање држављанства одређене државе. Поред наведених, присутни су и други облици злоупотребе.

У нашем кривичном законодавству као кривично дело јавља се фалсификовање исправа. Кривични законик прописује да ће бити кажњен свако ко направи лажну или преиначи праву исправу у намери да такву исправу употреби као праву као и онај ко лажну или преиначену исправу употреби као праву или је набави ради такве употребе (Службени гласник РС, 2005).

Многи Darknet маркети пружају ове услуге. За одређену суму новца може се добити други идентитет, постати држављанин ма које државе на свету. Међу најтраженијим услугама пре свега се наводе фалсификовање личник карата у Америци, добијање америчког држављанства, као и добијање пасоша Велике Британије.

На Darknet маркетима, администратори се хвале својим умећем да преваре државне органе својим фалсификатима.

Слика 10 - Darknet маркет на коме се може купити америчко држављанство (Become a citizen of the USA, real USA passport).

Као "држављанин" Сједињених Америчких Држава купац добија пасош, број социјалног осигурања, возачку дозволу, извод из матичне књиге рођених и остале

неопходне папире који би га учинили правим Американцем, а цена те у слуге је само 3500 америчких долара (Слика 10).

Један од највећих проблема управо код фалсификовања исправа је то што су оне доступне свима. Почетком ове године забележени су случајеви у којима припадници ИСИС-а користили пасоше купљене на Darknet-u (Ansa, 2017).

5.7. Дечија порнографија

Дечија порнографија представља било какав видео запис или фотографију који приказују малолетну особу у сексуалним активностима, или пак приказују интимне делове тела малолетних лица.

Од саме помисли на дечију порнографију људима се диже коса на глави. Несхватљиво је и апсолутно неразумљиво како неко може да учествује у тако гнусном злочину. Ако су деца наша будућност, и треба их штитити неприхватљиво је свако одступање од тога. Борба против дечије порнографије обухвата активност читаве међународне заједнице.

У оквиру Уједињених Нација донета је Конвенција о правима детета, као и факултативни протокол уз Конвенцију о правима детета о продаји деце, дечијој проституцији и порнографији (UNICEF).

У Кривичном законику Републике Србије као кривично дело наводи се приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију и наводи се да ће бити кажњен свако ко малолетнику учини доступним текстове, слике, аудио-визуелне или друге предмете порнографске садржине, ко искористи малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине, као и онај ко за себе или другог поседује, продаје,

приказује, јавно излаже или електронски или на други начин учини доступним слике, аудио-визуелне или друге предмете порнографске садржине (Службени гласник РС, 2005).

Сам интернет је уживаоцима малолетничке порнографије омогућио приступ разноврсном садржају. Претрага дечије порнографије преко површинског интернета није стран појам, али захваљујући напретком информационих технологија, откривање посетиоца тих интернет страница више не представља проблем владиним агенцијама и међународним организацијама. Управо због страха од казне која их може снаћи, ова лица се окрећу Darknet-u како би тамо задовољила своје сексуалне фантазије. Darknet представља рај за уживаоце малолетничке порнографије. Поред сајтова на којима се могу наћи фотографије и видео записи, уживаоци дечије порнографије су на Darknet-u основали своју комуну. На форумима деле савете једни другима, хвале се својим подвизима и размењују шкакљив материјал. И све то далеко од очију јавности, анонимно.

Слика 11- - Сајт на Darknet-u који је још увек у изради (PedoEmpire).

Док сам претраживала Darknet, наишла сам на један од њихових сајтова под називом PedoEmpire (Слика 11). Замисао овог сајта је да обухвати материјал са свих сајтова са Darknet-а како би посетиоци без имало муке могли да у сваком тренутку пронађу оно што им је потребно.

5.8. Тероризам

Са сигурношћу се може рећи да је 21. век, доба у којем терористичке организације представљају највећу опасност по читаво човечанство. Терористички напад у Америци 2001. године алармирао је читав свет, и од тада па све до данас, као један од основних циљева глобалних међународних организација наводи се и борба против тероризма. Донете су бројне конвенције, чије су потписнице скоро све земље света. Велики недостатак у раду међународних организација, јесте недостатак јединствене дефиниције тероризма. Овај проблем се јавља због немогућности да се једном дефиницијом обухвати ова сложена појава, а да се при томе не угрозе интереси неких држава.

Међутим и поред непостојања јединствене дефиниције, бројни теоретичари и научници су дали допринос, постављајући своје дефиниције. Постојање великог броја дефиниција указује на сложееност ове појаве.

Према В. Димитријевићу тероризам је акт политичког насиља, чији је предмет изабран да изазива јаке психичке реакције, у првом реду страх ширег круга људи, у нади да ће оне помоћи да се одржи или промени понашање које је важно за постизање политичког циља, ако такав акт није оправдан општим интересима који су одређени независно од њега и ако није извршен по правилима која се уобичајено примењују на друштвене видове вршења власти (Димитријевић, 1987).

Према Р. Гаћиновићу тероризам је организована примена насиља (или претња насиљем) од стране политички мотивисаних извршилаца, који су одлучни да кроз страх, зебњу, дефетизам, и панику намећу своју вољу органима власти и грађанима (Гаћиновић, 2005).

Према М. Мијалковском тероризам представља примену смишљеног, организованог и системнског насиља несувереног (недржавног, невладиног) субјекта (група, банда, организација, политичка странка и сл.) најбруталнијом физичком силом над унапрд одабраном (персоналном) или насумичном жртвом (цивил, полицајац, судија, бојник, политичар...), ради њеног убиства, сакаћења, киднаповања или психичког

злостављања, прироритетно изазове колективне комплексе страха или несигурности, зебње или апатије у средини из које је непосредна жртва напада (Стајић, 2011).

Такође можемо говорити и о сајбер тероризму, као посебном виду тероризма, који као главно средство и објект напада користи рачунар. Сајбер тероризам се односи на нападе на податке, компјутерске системе и програме, а све то с циљем да се изазове осећај страха и несигурности.

Тероризам на Darknet-u не представља посебан облик тероризма, већ само активност чланова терористичке организације на овом делу интернета.

Терористи су више година уназад користили површински инернет како би регрутовали нове чланове, ширили своју пропаганду, прукупљали новчана средства и координирали своје акције и нападе. Међутим због могућности надгледања, праћења и њиховог откривања на површинском интернету, морали су да своје активности пребаце на Darknet-u, који између осталог и нуди анонимност и сигурност од откривања.

Комуникација припадника терористичких организација је знатно сигурнија на Darknet-u, коришћењем различитих форума, причаоница, али и преко својих сајтова. Након терористичког напада у Манчестеру, у коме је на концерту певачице Аријане Гранде страдао велики број људи, терористичка организација ИСИС је на свој сајту на Darknet-u преузела заслугу за тај немио догађај (Time, 2017). На њиховом сајту се такође могу наћи и пропагандни клипови и снимци из борби "за ослобођење".

У току рада сам наводила неке од облика угрожавања безбедности на Darknet-u. Могло би се рећи да су они у блиској повезаности са терористичким организацијама. Терористистичке организација користе Darknet како би куповале експлозиве и оружје, наркотике, али и фотокопирана документа, која им омогућавају да за одређену суму новца постану неко други, држављанин ма које државе на свету и на тај начин несметано пролазе државне границе. Поред тога, терористичке организације Darknet користе и за прикупљање новчаних средстава. Направљњна је страница на Darknet-u под називом

"Fund the Islamic Struggle without Leaving a Trace"[3] која позива доноре да обаве трансакцију на одређеној bitcoin адреси (Weimann).

[3] Подржите исламску борбу без остављања икаквог трага

6. Активност међународне заједнице у борби против свих облика угрожавања на Darknet-u

Из свега наведеног у овом раду очигледно је да постоји свест о томе да је неопходно елиминисати оваква деловања, а ако их није могуће у потпуности елиминисати онда их бар смањити. Акције против деловања на Darknet-u предузете су од стране многобројних међународних организација, јер је схваћено да ово представља велики проблем по читаву међународну организацију и да се само заједничким активним деловањем може елиминисати,

Као прва велика акција против Darknet-а наводи акција америчких власти које је довела до затварања Silkroad-а и хапшења наводног администратора тог маркета, Роса Вилијама Улбрихта 2013. године (Ross Ulbricht). Након дугог и мукотрпног рада америчке власти су успеле да остваре свој план и затворе један од највећих Darknet маркета. Након тога, предузимане су многобројне акције с циљем затварања маркета на Darknet-u. Међу најзначајнијима се могу навести:

- Операција Onymous
- Операција Shrouded Horizon
- Операција Hyperion
- Операција Bayonet

1. Операција " Onymous" (Operation Onymous)

Operation Onymous представља координирану акцију преузету од стране Европола, ФБИ-ја, америчке имиграционе и царинске агенције[4] и Еројуста против маркета на Darknet-u. Спроведена је у новембру 2014. године.

Према подацима преузетим са интернет странице Европола у овој агенцији угашено је 410 сајтова на Darknet-u, заплењено је 180.000 еура у кешу, један милион америчких долара у bitcoin-ima, наркотици, сребро и злато. Поред тога ухапшено је 17 продаваца са маркета на Darknet-u.

2. Операција " Shrouded Horizon" (Operation Shrouded Horizon)

Operation Shrouded Horizon представља координирану акцију 20 држава, под покровитељством ФБИ-ја и Европола. Припреме су трајале дугих 18 месеци, а довеле су до гашења интернет форума за сајбер криминал и Darknet маркета под називом "Darkode". Спроведена је у јулу 2015. године. Агенти су успели приступе сајтовима за које је неопходан претходни позив неког од чланова и на тај начин су прикупљали податке. Овом акцијом ухапшено је 70 лица.

3. Операција "Hyperion"

Operation Hyperion је акција иницирана од стране америчке агенције Five Eyes Law Enforcement Group и чланова Европола и Европске Уније. Спроведена је у октобру 2016 (Law enforcement agencies around the world collaborate on international Darknet marketplace

[4] U.S. Immigration and Customs Enforcement

enforcement operation). За разлику од претходних акција, које су се фокусирале само на продавце, у овој акцији је било ухапшених купаца.

4. Операција "Bayonet"

Акција ФБИ-ја, Америчке агенције за борбу против наркотика[5], холандске националне полиције и Европола затворила је маркете на Darknet-u који су били одговорно за трговину више од 350.000 илегалних супстанци укључујући наркотике, оружје, као и рачунарске вирусе (Massive blow to criminal Dark Web activities after globally coordinated operation, 2017). Ова акција представља једну од најсофистицираних акција усмерних против криминалних активности на Darknet-u. Њом су угашена два водећа маркета на Darknet-u Hansa и AlphaBay (Operation Bayonet).

[5] US Drug Enforcement Agency

7. Закључак

Облици угрожавања које сам навела у свом раду нису новина коју је донео Darknet. Постојале су и пре саме појаве интернета. Међутим стварањем једног таквог места, попут Darknet-a, и немогућност његове контроле олакшало је посао лицима са криминалним тенденцијама, а свакако отежало посао државама у борби против њих.

И поред многобројних акција усмерених на спречавање угрожавања са Darknet-a, гашењем великог броја маркета на Darknet-u, они се поново враћају. Овде се може направити паралела са криминалним активностима ван интернета. Познато нам је да и поред активних напора државних органа, и даље постоје "улични дилери", "уживаоци дечије порнографије" итд.

Могло би се рећи да ће се криминалне активности на Darknet-u дешавати све док се на њима може зарађивати, односно док продавци имају купце. Тешко је замислити свет без криминала, али то никако не сме да нас обесхрабри. Сматрам да је неопходно да државне и међународне организације и даље активно учествују у сузбијању ових облика угрожавања, јер само тако може смањити стопа криминала и обезбедити безбедност и сигурност свих људи.

Литература

1. Преузето 8. октобра, 2017., са http://silkroad7rn2puhj.onion/ (Tor hidden service)
2. Преузето 12. октобра, 2017., са http://luckp47s6xhz26rn.onion/ (Tor hidden service)
3. Преузето 10. октобра, 2017., са http://2ogmrlfzdthnwkez.onion/ (Tor hidden service)
4. Преузето 8. октобра, 2017., са http://op4jvhn65pjv3slt.onion/ (Tor hidden service)
5. *A Complete Guide about the Deep Web*. (2016). Преузето 3. октобра, 2017., са https://www.deepweb-sites.com/how-big-is-the-deep-web/
6. *Ansa*. (2017). Преузето 3. октобра, 2017., са http://www.ansa.it/english/news/2017/02/08/naples-made-fake-uk-passports-on-sale-on-deep-web_f075770b-4231-4960-a2f7-0ec327c74e56.html
7. *Become a citizen of the USA, real USA passport*. Преузето 5. октобра, 2017., са http://xfnwyig7olypdq5r.onion/ (Tor hidden service)
8. *Bitcoin*. Преузето 4. октобра, 2017., са https://sr.wikipedia.org/sr-el/%D0%91%D0%B8%D1%82%D0%BA%D0%BE%D1%98%D0%BD
9. *Bitcoin (USD) Price*. Преузето 12. октобра, 2017., са https://www.coindesk.com/price/
10. Dean. (2015). *Dark Markets: How to Buy Things from the Deep Web's Black Markets*. Преузето 29. септембра 2017., са http://cryptorials.io/dark-markets-how-to-buy-things-from-the-deep-webs-black-markets/
11. *Global Drug Survey 2016*. (2016). Преузето 2. октобра, 2017., са https://www.globaldrugsurvey.com/past-findings/the-global-drug-survey-2016-findings/
12. Johnson B. (2014). *Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools.*

13. *Law enforcement agencies around the world collaborate on international Darknet marketplace enforcement operation*. (2016). Преузето 3. октобра 2017., са https://www.ice.gov/news/releases/law-enforcement-agencies-around-world-collaborate-international-darknet-marketplace

14. *Massive blow to criminal Dark Web activities after globally coordinated operation*. (2017). Преузето 12. октобра, 2017 са https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

15. Matthews, S. (2014). *Q&A With A Deep Web Arms Dealer*. Преузето 1. октобра, 2017., са http://www.vocativ.com/tech/bitcoin/q-deep-web-arms-dealer/

16. *Motherboard*. (2015). Преузето 12. октобра 2017., са https://motherboard.vice.com/en_us/article/vvbazy/my-brief-encounter-with-a-dark-web-human-trafficking-site

17. *Operation Bayonet*. Преузето 12. октобра 2017., са https://en.wikipedia.org/wiki/Operation_Bayonet_(darknet)

18. *Operation Onymous*. Преузето 5. октобра 2017., са https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous

19. *Operation Shrouded Horizon*. Преузето 5. октобра 2017., са https://en.wikipedia.org/wiki/Operation_Shrouded_Horizon

20. Pellerin, C. *DARPA Program Helps to Fight Human Trafficking*. Преузето 10. октобра 2017., са https://www.defense.gov/News/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/

21. *Ross Ulbricht*. Преузето 5. октобра 2017., са https://en.wikipedia.org/wiki/Ross_Ulbricht

22. Sabarinath. (2017). *Darknet vs Dark Web vs Deep Web vs Surface Web*. Преузето 12. октобра 2017., са //techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/

23. *Silkroad*. Преузето 5. октобра 2017., са https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

24. *Slayers assasination and life ruining services*. Преузето 10 октобра, 2017, са http://zy3dkytcaubkq2y3.onion/ (Tor hidden service)

25. *Sweguns* . Преузето 7. октобра, 2017., са http://swegunsh343s3drf.onion (Tor hidden service)

26. *Time*. (2017). Преузето 11 октобра, 2017., са http://time.com/4790201/isis-manchester-concert-terrorist-attack/

27. Weimann, G. *Terrorist Migration to the Dark Web*. Преузето са http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html

28. Winstock A, Barratt M, Ferris J, Maier L. (2017). *Global Drug Survey 2017.*

29. Гаћиновић, Р. (2005). *Дефинисање савременог тероризма.*

30. Димитријевић, В. (1987). *Појам тероризма.* Београд.

31. Марић, М. (2015). *Оперативни системи.* Београд: Математички факултет.

32. Плескоњић, Д. (2010). *Етичко хакерисање и испитивање могућности пробоја*.

33. Протокол Уједињених нација за превенцију, сузбијање и кажњавање трговине људским бићима, нарочито женама и децом, који допуњава Конвенцију Уједињених нација против транснационалног организованог криминалитета из 2000. године. (2000). Палермо.

34. Службени гласник РС, 9/92, 53/93, 67/93, 48/94, 44/98, 39/03, 85/0, 101/05, 27/11, 104/13. (1992). *Закон о оружју и муницији* .

35. Службени гласник РС, 85/05, 88/05, 107/05, 72/09, *111/09, 121/12, 104/13, 108/14, 94/16*. (2005). *Кривични законик* .

36. Стајић, Љ. (2011). *Основи система безбедности.* Нови Сад: Правни факултет.