УНИВЕРЗИТЕТ „СВ.КИРИЛ И МЕТОДИЈ“
ФИЛОЗОФСКИ ФАКУЛТЕТ – СКОПЈЕ

Институт за безбедност, одбрана и мир

Последипломски студии од областа на корпоративна безбедност и безбедносен менаџмент

Магистерски труд

Улогата на темната мрежа во идните сајбер војни

Ментор:
Проф. д-р Тања Милошевска

Изработил:
Марјан Мојсоски
индекс: 5327/20

Скопје, 2022 година

Содржина

1. Вовед

1.1 Проблем на истражување

Во последните години Дарк веб е една од најдискутираните теми во круговите за сајбер безбедност. Фокусот и интересот кон сајбер безбедноста во последните неколку години драстично се зголеми како резултат на негативните ефекти по безбедноста (почнувајќи од индивидуалната безбедност преку безбедноста на бизнис-заедницата, па сѐ до националната безбедност). Брзиот и рапиден развој на интернет технологијата го претвори дигиталниот универзум во едно огромно поле на дејствување. Бројот на интернет корисниците постојано расте како резултат на воведување нови апликации на информатичката технологија. Трендот ќе продолжи како што се развива и технологијата. Сепак, брзиот раст на интернетот го остави подложен истиот на неправилно користење и злоупотреба, што станува значајна закана и предизвик во кибер просторот низ светот.[1] Привлекува внимание посебно „црниот пазар“ на интернет - Темната мрежа, бидејќи претставува скриен простор станувајќи најголема аплицирана анонимна мрежа. Овој успех е поддржан од бројни одлики, карактеристики коишто се вградени во високотехнолошката структура на Темната мрежа, на пр. тајност, анонимност и употреба на криптовалути.

Разбирањето на апликативноста на Дарк веб за иднината на сајбер-војните бара од нас да го гледаме проблемот од повеќе перспективи. Се разбира, постои основната перспектива за национална безбедност што треба да го поттикне нашето основно разбирање - сепак, подеднакво важни се и економските и разузнавачките оперативни перспективи. Од економска перспектива, треба да сметаме дека примарната апликација на Дарк веб, досега беше како пазар што го користеа оние кои сакаат да се занимаваат со недозволена трговија. Способноста да се разбере недозволената трговија на Дарк веб, што се однесува на националната безбедност, бара од нас да ги земеме предвид концептите како што се: понудата, побарувачката, угледот на продавачот, итн.

[1]Ozkaya E, Rafikul, I. (2019*). Inside the Dark Web*, CRC Press, Taylor and Francis Group, USA.

Додека од перспектива на разузнавачки операции, Дарк веб, исто така, може да се гледа како неутрална основа за две страни кои сакаат анонимно да се вклучат во размена на информации, оружје и тајни од областа на националната безбедност.

Постепеното зголемување на барањата на корисниците за зачувување на своите идентитети и приватноста, драстично го дисперзира користењето на интернетот и мрежните технологии. За да ги постигнат барањата на корисниците, истражувачите развија пристапи со што се формира најголемиот дел од Длабоката мрежа. Таканаречениот Дарк веб е во фокусот на медиумите последниве години, редовно во негативен контекст.

Со преземањето на веб-страницата „Патот на свилата“ во октомври 2013 година од страна на ФБИ, Темниот веб влезе во свеста на голем дел од популацијата. Во февруари 2015 година, ФБИ ја отстрани озлогласената веб-страница „Playpen“, која беше домаќин на повеќе од 23.000 детски слики со сексуална злоупотреба на деца и видеа и имаше повеќе од 21.000 корисници.[2]

Реалноста е дека сајбер-проблемите се исто толку важни како и други проблеми со коишто се соочуваат овие системи. Оваа еволуција или подобро речено револуција во сајбер–нападите може да биде вклучена како модерна алатка за индиректна интервенција за тајно уништување на противничката мрежа, покажувајќи ја стратегиската важност на технолошката еволуција во сајбер просторот и на тој начин навестувајќи го полето на развој на идната сајбер-војна.

Како дел од подготовките за терористичките напади во Париз во ноември 2015 година, комуникацијата беше анонимна со користење на софтверот TOR; додека оружјето користено во нападот во Минхен во јули 2016 година, исто така било набавено преку Темната мрежа.

[2]Koch, R. (2019). *Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?* NATO CCD COE Publications, Tallinn.

Покрај дрога, оружје и сексуална злоупотреба на деца, секој вид на информации се продава преку пазарите на Дарк веб: од кредитни картички до сензитивни информации добиени преку протекување податоци или хакерски напади. Вториот начин може да претставува нов предизвик за вооружените сили.[3]

Длабокиот веб е прикажан како сегмент на длабоката веб–темна мрежа, која во принцип е опишана како скриени веб-страници каде што корисниците не можат лесно да добијат пристап до неа без употреба на специјалниот софтвер. Корисниците можат да добијат пристап до Дарк веб со очекување дека ќе можат да ги споделат информациите и датотеката со мал ризик од откривање. [4]Дарк веб помага во објаснувањето на вообичаените заблуди што се појавуваат во рамките на областа што е предмет на истражување. Клучните зборови се индексираат во пребарувачите и корисниците можат лесно да ги прегледуваат индексираните веб-страници.

Дарк веб се однесува на асортиман на веб-страници, што претставуваат енкриптивна мрежа каде не може да се пристапи со конвенционално пребарување на веб-пребарувачите. Скоро сите веб-страници на Дарк веб се користат за да се сокрие нивниот идентитет преку користење на TOR енкриптирање, бидејќи TOR е способен да го скрие идентитетот на веб-страниците како и прикривање на активностите извршени преку веб-страниците. World Wide Web (WWW) е огромен склад на хиперврзани документи, кој содржи корисни информации.

Во моментов, експоненцијалниот развој во областа на информатичката технологија обезбедува можности за пристап до голема количина на информации преку WWW. WWW е широко поделен на два сегмента; површинска мрежа и длабока веб-мрежа или Темна мрежа според длабочината на информациите обезбедени од податоците од веб-страницата.[5]

[3]Koch, R. (2019). *Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?* NATO CCD COE Publications, Tallinn.
[4]Danny Bradbury (2014). Unveiling the dark web. *Network Security* 4(4)*: 14-17*
[5] Chen, H. (2012). *Dark web: Exploring and data mining the dark side of the web*. New York, NY, достапно на:https://www.springer.com/gp/book/9781461415565

Содржината на длабокиот веб е динамично произведена од веб-серверот. За пристап до Дарк веб, корисниците треба да побараат од одредена база на податоци преку интерфејс за пребарување. Во моментов се забележува дека голема количина на податоци за WWW може да се добијат само преку интерфејсот за пребарување. Затоа, големи колични на информации сѐ уште не се видливи за корисниците.

Со оглед на тоа што Темниот веб е најпознат по тоа што е домаќин на нелегална економска трговија, стана јасно дека има многу сериозни импликации за националната безбедност што ќе влијаат врз повеќето нации низ целиот свет. Распространувањето на кибер и кинетичко оружје, олеснување на тероризмот, собирање разузнавачки информации, изнудување, злонамерни услуги за изнајмување на сите овие недозволени активности се случуваат на Темниот веб, а податоците кои ќе бидат анализирани во овој труд сугерираат дека овие активности може да се јавуваат со зголемени стапки во иднина.

Војувањето отсекогаш и секогаш ќе се развива - затоа е разумно професионалците од областа на националната безбедност да бидат свесни за оваа еволуција и да се запознаат со различните технолошки сложености што ќе продолжат да ја обликуваат еволуцијата на војувањето. Темниот веб, како и другите технологии во развој, е една од тие технолошки сложености. Покрај тоа, би било разумно да се земат предвид потенцијалните контрамерки и способности за следење, како што е разузнавањето за потенцијални закани фокусирани на Темната мрежа.

1.2 Предмет на истражување

Експертите по технологија што го пронајдоа интернетот, развија технологија наречена Дарк Веб што не е видлива за корисниците. Поддржувачите велат дека Дарк Веб помага во заштитата на дисидентите во државите со репресивни режими, дозволувајќи им на војската и полицијата да водат тајни операции и да ја зголемат безбедноста за корисниците на веб.[6]

Од друга страна, Дарк Веб е критикуван заради сајбер криминалот, откривање или продавање на податоците и информациите што предизвикуваат штета на организации и поединци.

Пред појавата на Темната мрежа, високоефективните сајбер-експлоатации беа достапни само за напредните влади на националните држави, организирани криминални групи и тесно поврзаните истражувачки заедници. Ова повеќе не е случај, бидејќи ефективните сајбер-експлоатирања сега се монетизираат и се дистрибуираат низ десетици пазари и форуми на Дарк веб. Ова ги покренува прашањата од гледна точка на националната безбедност, бидејќи им овозможува на актерите кои претходно не поседуваа техничка моќ, едноставно да ги купат посакуваните способности.

Анонимноста олеснета преку Дарк веб поттикнува идеално поле за тргување за потенцијалните купувачи и продавачи на оружје. Ова е повеќе од само теоретско - тоа е факт што се докажува преку набљудување постојано и повторно. Ураниум, опасни хемиски соединенија, воено огнено оружје-примерок подмножество од видовите оружја што се наведени на Темната мрежа. Како одговор на овие закани, глобалната заедница за спроведување на законот агресивно се обидува да биде купувач и продавач на оружје на Темната мрежа, и во многу случаи тие беа успешни во спречувањето на потенцијалните напади.

Во 2016 година, Федералното истражно биро на САД (ФБИ) соработуваше со Ирските власти за спроведување на законот за да го спречи милитантот на

---

[6]Robert W. Gehl (2016), Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network, *New Media and Society*, достапно на: https://journals.sagepub.com/doi/full/10.1177/1461444814554900

Ирската Република Армија (ИРА) да набави пиштоли, гранати и пластични експлозиви од пазар на темна веб-страница.[7] И додека заедницата за национална безбедност може да извојува мали победи со овие видови превентивни операции, оние што се заинтересирани за анонимно купување и продавање на кинетичко оружје почнаа да ја менуваат својата методологија.

Владата на Велика Британија воведе и единица за компјутерски криминал за справување со Дарк веб со фокус на разбивање на мрежите на криминалот, на анонимната технологија и на тајните веб-страници. Дарк веб обезбедува платформа за корисниците на интернет за коишто анонимноста е неопходна бидејќи тие не само што обезбедуваат заштита од неовластени корисници, туку исто така, вклучува и криптирање за да се попречи следењето.

За да ја разбереме Темната мрежа во контекст на национална безбедност, треба да се фокусираме првенствено на две работи: трговија и комуникација. Од гледна точка на трговијата, националните безбедносни актери настојуваат да разберат како различни лица или групи ќе ја користат Темната мрежа за да се вклучат во недозволена и/или тајна трговија. Од перспектива на комуникација, професионалците за национална безбедност настојуваат да откријат како овие актери ќе ја искористат Темната мрежа за да спроведат планирање, регрутирање, собирање разузнавачки информации и други активности од интерес.

Во текот на следните години, се проценува дека ќе има две големи еволуции во начините на кои се тргува со кинетичко оружје на Темната мрежа. Првото е дека купувачите и продавачите на оружје за Дарк веб најверојатно ќе го оддалечат својот бизнис од некои повеќе популарни пазари со отворен пристап (како што е Dream Market) и од други пазари за кои е потребен повисок степен на проверка. Ова најверојатно ќе се случи од две основни причини. Првото е дека лицата што се занимаваат со трговија со оружје стануваат повнимателни за тајното присуство на органите на прогонот и можноста да бидат намамени во стапица.

Второто е дека главните пазари веројатно стануваат помалку толерантни за ризикот што го носат со дозволување на списоци со оружје на нивните пазари.

[7]C. Aliens. (2018). "More Details Revealed in The Dublin Explosives Case", *Deep Dot Web*, достапно на: https://www.deepdotweb.com/2018/08/05/more-details-revealed-in-the-dublin-explosives-case/.

Огласите со оружје го привлекоа вниманието на глобалната заедница за спроведување на законот, што резултираше со тајни полицајци кои ги разгледуваат пазарите и бараат траги. Надвор од зголемениот ризик, пазарната маргина за профит за трговија со оружје е релативно ниска во споредба со профитните маржи на други недозволени стоки со голем обем, како што се дрога и измама. Според две студии спроведени од РАНД, се проценува дека глобалната продажба на дрога на Дарк веб изнесува помеѓу 12 и 21,1 милиони американски долари месечно во 2016година[8], додека глобалната трговија со оружје изнесуваше 80 илјади долари месечно во 2017 година.[9]

Втората голема еволуција што најверојатно ќе ја анализираме е транзицијата подалеку од тргување и испраќање опипливо физичко оружје кон дигитална трговија и размена на информации за оружје.

Во наредните години, Темната мрежа ќе биде повеќе експлоатирана за операции со извор на разузнавање, активности од внатрешна закана и изнуда. Постојат две основни причини за ова - првата е вродениот дизајн на Дарк веб и неговата способност да ја олесни двонасочната анонимност. Втората причина е зголемената количина на податоци достапни на Темната мрежа што може да ги користат разузнавачите за изнуда или за принудување извори.

Без оглед на средствата што се користат за подобро разбирање на оваа закана, сеопфатната цел треба да биде: да се создаде зголемена колективна свест и зголемување на заштитата и ефикасноста на национална безбедност. Сакаме да ја искористиме оваа свест за да ја намалиме можноста за стратешко изненадување, како и да го олесниме предвидливото разбирање за тоа како нашите противници најверојатно ќе го користат Дарк вебот во текот на нивните малициозни операции.

Иако оваа свест не мора нужно да ги спречи националните безбедносни закани позиционирани од Темната мрежа, таа секако може да е во центарот на вниманието на ова прашање и да олесни поголем простор за тоа како глобалната заедница може да одговори на овие нови закани.

[8] Taking Stock of the Online Drugs Trade", (2016), RAND Corporation, достапно на: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.
[9] "International arms trade on the dark web", (2017), RAND Corporation, достапно на: https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html.

1.3 Досегашни истражувања

Во научната литература во Македонија се проучуваат одредени аспекти на сајбер-заканите и сајбер-нападите, изработени од автори што се однесуваат на поврзаност со сајбер тероризмот, но Дарк Веб како проблематика е малку истражувана.

Општо земено, Дарк веб е нова проблематика во светот, па и кај нас е во фаза на истражување, а тоа ќе биде предмет и на идните генерации. Нелегалните мрежни пазари, како на мрежната површина, така и на Темната мрежа, им овозможуваат на криминалните продавачи да ги истражат сите начини на недозволена стока, со оние од посериозна природа што обично се наоѓаат подлабоко во Темната мрежа. Многу од овие недозволени стоки и услуги, како што се алатки за компјутерски криминал или лажни документи, се можности за понатамошен криминал.

Идејата за истражувањето е резултат на поттикот да се дојде до одредени научни и практични сознанија, како и да се осознаат начините и методите кои придонесуваат кон една комплетна анализа, за да се дознае што всушност се прави на тоа поле, за да се формира целосна слика за Дарк веб мрежата. Ова истражување коешто е планирано да се спроведе, ќе го заземе вистинскиот аспект во однос на зголемување на истражувањата во оваа чувствителна област.

Поради фактот што проблематиката е актуелна, а севкупноста на сите елементи е во корелација со последните настани во светот, нејзината динамика како истражувачки проблем го заслужува потребното внимание.

Со оглед на недостатокот на научна опсервација за Дарк Веб од оваа перспектива и недостиг на анализа на начините на кои овој проблем го покажува (и на тој начин влијанието што таков приказ може да го има врз колективната свест на општеството), анализата на импликациите од сајбер-заканите и Дарк веб мрежата е основна определба на овој труд за да понуди свој придонес кон постојните истражувања.

1.4 Цели и задачи

Општата цел на ова истражување е научна дескрипција, анализа и идентификација на важноста на Дарк веб во водењето на идните сајбер-војни.

Посебни цели:

- Анализа на податоци за активностите што се помогнати преку Дарк Веб.
- Да се идентификуваат начините што ги намалуваат негативните влијанија на Дарк Веб.
- Да се откријат процесите што ќе помогнат во користење на Дарк Веб на начин што ќе биде поконструктивен.
- Да ги испитаа тенденциите на развој, можните решенија и потенцијалните фактори на ризик.
- Да се види какво е моменталното користење на Дарк Веб во Македонија.
- Воспоставување на стандардни оперативни процедури во Македонија за справување со нелегалните веб активности.
- Да се увиди која е улогата на регулацијата за растот на Темната мрежа и инвестирање во технологија во контекст на лични, граѓански и економски слободи во општеството.

Со оглед на целите, основни задачи на истражувањето се следниве:

- Да се утврди дали е потребна поголема соработка помеѓу разузнавачките агенции и организации во делот на новата транснационална закана Дарк веб.
- Да се идентификува динамиката на манифестирање на активностите преку Дарк Веб како сериозна закана за националната безбедност на државите.
- Да се утврди нивото и степенот на загрозеност на информацискатa критична инфраструктура од активностите на Дарк Веб.
- Да се одговори на дилемата која е причината и покрај развиените современи методи, да се реализираат активности преку Дарк Веб.
- Да се идентификуваат стратегии коишто можат да се применат од страна на соодветните служби за да остварат контрола над Темната мрежа.
- Да се подобри непосредната комуникација помеѓу директните извршители коишто учествуваат во справување со заканите што доаѓаат поради дејствувањето на Дарк Веб.

1.5 Дефинирање на основните поими

- **Длабок веб**

Длабокиот веб „се однесува на сите интернет-информации или податоци што се недостапни од пребарувачот и ги вклучуваат сите веб-страници, интернет, мрежи и мрежни заедници кои се намерно и/или ненамерно скриени, невидливи или недостапни за роботите на пребарувачот“. Терминот Длабок веб, „има асоцијација на длабоки морски/океански опкружувања, кои се практично невидливи и недостапни“. Овие скриени делови на интернет се познати како Длабок веб.

Длабоката мрежа е приближно 400-500 пати помасовна од површинската мрежа. Затоа, Длабокиот веб „содржи податоци што динамички ги создава апликација, неповрзани или самостојни веб-страници/веб-страници, не-HTML содржини и податоци што се приватно чувани и класифицирани како доверливи. Некои проценуваат дека големината на Длабоката мрежа е многу пати поголема од видливата или површинската мрежа“.

- **Безбедност на информации**

Безбедноста на информациите подразбира заштита на информацијата од низа закани, сѐ со цел да се обезбеди континуитет на работењето, да се минимализира потенцијална штета, и да се максимизираат резултатите.

- **Дарк нет**

Од техничка и историска гледна точка, терминот „Darknet“ се користи за да се опише делот од просторот за интернет-адреси што е способен да се пренасочи до друга мрежа, но не и во употреба. Ова мора да се разликува од адресите, кои не треба да се користат по дефиниција. Една од првите употреби на терминот во однос на дигиталната содржина може да се најде во написот за заштита на содржината. Таму се опишува Дарк нет како „колекција на мрежи и технологии што се користат за споделување дигитални содржини“.

Денес, терминот главно се користи за мрежни преклопувања кои обезбедуваат анонимна мрежна конекција и услуги. Мрежа на преклопување е слој на виртуелна мрежна топологија на врвот на физичкиот слој, кој директно се поврзува со корисниците. Софтверот TOR е пример за мрежна покривка и најголема и најчесто користена мрежа за анонимизација; но има многу други, како што се: I2P, Freenet или ZeroNet. Важно е да се признае дека терминот Дарк нет првично се однесува на самата мрежа како техничка основа како протоколот и уредите; но не и содржината што може да се транспортира преку мрежата или може да се најде на соодветните сервери.[10]

- **Сајбер одбрана**

Сајбер одбрана - проактивна мерка за откривање или добивање информации во врска со сајбер-упад, сајбер-напад или сајбер-операција или за утврдување на потеклото на операцијата што вклучува инволвирање превентивна или сајбер контра операција против изворот.

- **Сајбер-простор**

Сајбер-просторот претставува глобален домен во областа на информациите и се состои од независна мрежа на информациски системи и инфраструктура, вклучувајќи интернет, телекомуникациски и компјутерски мрежи.

- **Сајбер-криминал**

Сајбер-криминал, познат и под називот електронски криминал, компјутерски криминал и слично, кој опфаќа криминални активности спроведени со користење на компјутери и интернет, најчесто финансиски мотивирани. Компјутерскиот криминал вклучува кражба на идентитет и измама, меѓу другите активности. Компјутерскиот криминал се разликува од

[10] KOCH, R. (2019). *Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations*? NATO CCD COE Publications, Tallinn.

другите форми на малициозни сајбер активности, кои имаат политички, воени или мотиви на шпионажа.

Сајбер-криминалот може да опфати кражба на интелектуална сопственост, злоупотреба на патент, трговска тајна и сл., но исто така вклучува и напади против компјутери со цел намерно нарушување на нивното функционирање или недозволено копирање на класифицирани информации складирани во компјутерските системи.

- **Сајбер-војна**

Сајбер-војна или „наменска употреба на компјутерски системи со цел да се прекинат активностите на непријателска земја или напад на нејзините комуникациски системи“. Акт на војна во и околу виртуелниот простор со средства коишто се предоминантно поврзани со информатичката технологија.

- **Сајбер безбедност**

Сајбер безбедност претставува активности и мерки за заштита на информациските системи кои го формираат сајбер просторот од напади, обезбедување доверливост, интегритет и достапност на информации и системи, откривање на напади и сајбер безбедносни инциденти, активирање на механизми за контра-одговор и обновување на системите до состојба во која се наоѓале пред сајбер инцидентот.

- **Сајбер-закана**

Сајбер-закана е злонамерен чин кој се обидува да ги оштети податоците, да украде податоци или да го наруши дигиталниот живот воопшто. Сајбер-заканите вклучуваат компјутерски вируси, пробивање податоци, напади на Denial of Service (DoS) и други вектори на напади. Сајбер-заканите, исто така, се однесуваат на можноста за успешен сајбер-напад кој има за цел да добие неовластен пристап, оштетување, нарушување или крадење на информатичка технологија, компјутерска мрежа, интелектуална сопственост или која било друга форма на чувствителни податоци. Сајбер-заканите може да доаѓаат од организации, од доверливи

корисници или од оддалечени локации од непознати страни[11], односно може да се однесува на потенцијалната причина за инцидент во сајбер просторот што може да предизвика оштетување на некоја институција или систем.

1.6 Основна хипотетичка рамка

Врз основа на општиот пристап на проблемот за Дарк веб како растечка закана за националната безбедност и врз основа на веќе поставените цели во ова истражување ќе ја поставам следнава општа хипотеза:

Улогата на Темната мрежа ќе има значајни негативни импликации врз безбедноста, особено во начинот на водење на идните сајбер-војни.

Посебни хипотези:

- ✓ Распространетото ширење на способностите преку Темната мрежа им овозможува на актерите да го искористат сопственото техничко разбирање за експлоатирање на сајбер просторот за да реализираат сајбер операции и закани кои се таинствени и поопасни од претходните.
- ✓ Во иднина, одредени државни и недржавни групи актери со закани ќе сакаат да ги забрзаат своите способности за сајбер-војна, преку експлоатирање на Темната мрежа за да ги добијат саканите услуги.
- ✓ Меѓу-институционалниот и мулти-дисциплинарниот пристап со вклучување на сите засегнати страни е од клучно значење за да се обезбеди ефикасен одговор на активностите на Дарк Веб.
- ✓ Унапредувањето на соработката со регионалните и меѓународните полициски организации е од суштинско значење за справување со Дарк веб.
- ✓ Воспоставување ефикасни процедури за пријавување и истражување на Дарк Веб имплицира намалување на негативните импликации врз безбедноста.

[11]Tunggal A. T. (2021). What is Cyber Threat? достапно на: https://www.upguard.com/blog/cyber-threat

- ✓ Активното меѓународно учество во справување со глобалниот предизвик од сајбер-заканите ќе придонесе за зголемување на државните капацитети за справување со сајбер-ризиците.
- ✓ Преку соработка на сите засегнати страни за унифицирање безбедносни норми, стандардизирање на соработката ќе се воспостави задолжително ниво на заштита за субјектите.
- ✓ Создавање на национална платформа/систем за размена на информации во врска со закани, инциденти и непосредните опасности ќе резултира кон подобрување на заштитата од дејствувањето на Дарк веб.

Варијабли

Предикторска варијабла (независна варијабла)

-Дарк веб мрежа,

Критериумска варијабла (зависна варијабла)

-Постигнати резултати во спречување на незаконските активности преку Темната мрежа.

1.7 Научна и општествена оправданост на истражувањето

Научната оправданост на ова истражување се согледува во придонесот на верификување на научно недоволно познати и проучени специфични факти и да даде насока за подобрување на меѓународната соработка и изнаоѓање на нови форми и методи за превенирање и сузбивање на активностите преку Дарк веб мрежата.

Општествената оправданост се состои во тоа што истражувањето би помогнало да се согледаат можностите на заедничко дејствување во насока на намалување на бројот на потенцијални криминални активности.

Трудот ќе ја согледува општествената реалност низ призмата на сајбер-безбедноста и сајбер-заканите, каде се апострофираат определени специфични

димензии, се респектира комплексноста на проблемите што се истражуваат и се поврзани со сајбер-безбедноста, но и се нагласуваат посебните научни аспекти.

1.8.Методи и техники на истражувањето

Во контекст на современите научно-методолошки пристапи на истражување со комбинирање на повеќе истражувачки методи, во истражувањето ќе настојувам со примена на неколку методолошки постапки на собирање, анализа и интерпретација на податоците да се добие една систематизирана целина.

Компаративниот метод на анализа се користи со цел да се изврши делумна квалитативна и квантитативна селекција и анализа на прибраните податоци и врз основа на тоа да се воопштат релевантните факти за потврдување или негирање на поставените тези. Овој метод се користи за споредување на сите податоци добиени со претходно користење на статистички методи и анализа на содржината кој се однесуваат на бројните показатели за состојбата со активностите преку Дарк веб мрежата.

Покрај квалитативната анализа на релевантни теориски извори, како основна методолошка постапка, односно техника за собирање на податоци ќе се користи анализа на содржина на публикации, извештаи, конференциски материјали, статистички показатели, извештаи и анализи на невладини организации, агенции за испитување на јавното мислење, тинк-тенкови и државни институции итн., а како методолошки постапки за анализа и интерпретација на податоците ќе се применат аналитичко-синтетички метод и компаративен метод на анализа.

Преку анализа и интерпретација на податоците во ова истражување се очекува да се добијат квантитативни и квалитативни податоци, со кои преку соодветна обработка ќе се добие верификација на хипотезите и ќе се оствари целта на истражувањето.

2. Појмовно – терминолошко определување на Дарк веб Темна мрежа

Интернетот овозможи формирање на глобално дигитално општество кое ги надминува границите, без разлика на националности, правни јурисдикции, раса или религија. Ова општество, и покрај својата аморфна природа, сепак претставува поединци обврзани со законите на нивната земја. Ова е можно бидејќи онлајн идентитетите, главно IP адресите, се поврзани со поединци или веб-страници што ги поседуваат. Користејќи ги атрибутите јавни наспроти приватни, отчетни наспроти анонимни, интернетот може да се подели во три широки категории:

- ✓ Површинската мрежа е јавна бидејќи пристапот не е ограничен со проверка или плаќање, индексирана е од пребарувачите, додека засегнатите страни се препознатливи и затоа подлежат на спроведување на законот.
- ✓ Длабоката мрежа - делови од интернет кои не се јавно достап (т.е. приватно), не се индексирани од пребарувачите. Пристапот е ограничен поради барања за автентикација или затоа што е дел од внатрешна мрежа. Отчетноста на некој начин е уште посилна отколку на веб-страницата со оглед на автентикација на барања.
- ✓ Темната мрежа - подмножество на интернет кое не е индексирано од пребарувачите, бидејќи бара употреба на специјален софтвер за пристап. Се состои од јавни и приватни елементи (т.е. достапни јавно или само оние со акредитиви) под услов да се користи точниот софтвер. Клучната разлика помеѓу темната веб површинска и длабока мрежа лежи во недостатокот на отчетност. Корисниците се неидентификувани за мрежата, или за секој што следи, и нивните постапки се ефективно анонимизирани.

Понатаму, темниот веб овозможува хостирање на веб-услуги (скриени услуги) кои остануваат анонимни во однос на нивната вистинска IP адреса, а со тоа и локацијата, дури и за корисниците што ги користат веб–услуги. Најистакнатата манифестација на Темната мрежа (мрежата TOR) го насочува сообраќајот преку интернет преку повеќе јазли, секој од нив свесен за испраќачот и дестинацијата во нивната непосредна близина и на тој начин се несвесни за оригиналниот испраќач

и дестинацијата на тој сообраќај. Во Темната мрежа постои систем кој е децентрализиран по природа без централни сервери или точка на контрола, па затоа е тешко да се направат затворени. Протоколот TOR користи шифрирана врска со секоја дестинација преку повеќе јазли (или релеи) што овозможува прелистувачот TOR да обезбеди анонимност дури и кога прелистувањето на веб – страници е на површинска мрежа.

Овој систем, кога се комбинира со криптографија со јавен клуч и слоевитоста на сообраќајот на таков начин што секој учесник во мрежата никогаш нема целосно познавање за идентитетот на секој канал за комуникација од крај до крај. За многу корисници, главната причина за користење на мрежата за преклопување како што е TOR не е само за анонимен пристап до редовни веб-страници, туку за пристап до голем број на веб-страници кои инаку не се достапни на површината, освен само преку мрежата.[12]

Термините Дарк нет (Darknet), Длабок веб (Deep Web) и Дарк веб (Dark Web) се мешаат или се користат наизменично. Поради тоа може да се злоупотребат термините, податоците и евалуациите да се неправилно распоредени и да ја прикријат фактичката состојба.[13]

Длабок веб. Длабокиот веб „се однесува на сите интернет-информации или податоци што се недостапни од пребарувачот и ги вклучуваат сите веб-страници, интрнет, мрежи и мрежни заедници кои се намерно и/или ненамерно скриени, невидливи или недостапни за роботите на пребарувачот“.

Терминот Длабок веб, „има асоцијација на длабоки морски/океански опкружувања, кои се практично невидливи и недостапни“.[14] Овие скриени делови на интернет се познати како Длабок веб. Длабоката мрежа е приближно 400-500 пати помасовна од површинската мрежа.[15] Затоа, Длабокиот веб „содржи податоци што динамички ги создава апликација, неповрзани или самостојни веб-

[12]Длабока интернет мрежа. Невидлив интернет, достапно на интернет страницата: https://bitserv.ru/mk/deep-internet-network-invisible-internet/
[13]Милошевска, Т. (2020), Дарк веб- Нова транснационална безбедносна закана, *Годишен зборник*, вол.73, Филозофски факултет, Скопје.
[14] Janseen, D. (2018). Deep Web. *Techopedia*.
[15] Wilson Center Report. (2015). “*The Deep Web and the Darknet: A Look Inside the Internet’s Massive Black Box”*, достапно на: https://www.wilsoncenter.org/sites/default/files/deepweb-report_october_2015.pdf.

страници/веб-страници, не-HTML содржини и податоци што се приватно чувани и класифицирани како доверливи. Некои проценуваат дека големината на Длабоката мрежа е многу пати поголема од видливата или површинската мрежа.

Дарк нет. Од техничка и историска гледна точка, терминот „Darknet“ се користи за да се опише делот од просторот за интернет-адреси што е способен да се пренасочи до друга мрежа, но не и во употреба. Ова мора да се разликува од адресите, кои не треба да се користат по дефиниција. Една од првите употреби на терминот во однос на дигиталната содржина може да се најде во написот за заштита на содржината. Таму се опишува Дарк нет како колекција на мрежи и технологии што се користат за споделување дигитални содржини.[16]

Денес, терминот главно се користи за мрежни преклопувања кои обезбедуваат анонимна мрежна конекција и услуги. Мрежа на преклопување е слој на виртуелна мрежна топологија на врвот на физичкиот слој, кој директно се поврзува со корисниците.[17]

Софтверот TOR претставува пример за мрежна покривка и е најголема и најчесто користена мрежа за анонимизација; но има многу други, како што се I2P, Freenet или ZeroNet. TOR, исто така, обезбедува различни услуги (скриени услуги) како што се хостирање веб-страници кои се достапни само во рамките на TOR мрежата. Корисниците на мрежата TOR можат да се поврзат со компјутери, т.е. сервери кои ги нудат овие тајни услуги, така што ниту серверот ниту корисникот не ја знаат локацијата на вториот. Ова практично им овозможува на корисниците на TOR да креираат веб-страница каде што луѓето можат да објавуваат материјал без да се грижат за цензурата, бидејќи никој не може да утврди кој е „сопственикот“ на страницата, ниту „сопственикот“ на корисниците што ја користат страницата.

TOR во суштина користи P2P (peer-to-peer) поврзување. Тоа е децентрализиран комуникациски модел во кој секоја страна има иста способност и секоја страна може да започне комуникација со другата страна. За разлика од моделот сервер/клиент, во кој клиентот бара пристап на серверот, што може да

[16] Biddle, P. at al. (2002). *The Darknet and the Future of Content Protection*. In ACM Workshop on Digital Rights Management, Springer-Verlag Berlin Heidelberg.
[17] Zhang, X. (2003). *System/Application Designs, Optimization and Implementations on Overlay Networks*. High Performance Computing and Software Lab. Ohio State University.

биде одобрен или одбиен, P2P моделот на сите страни во процесот им дава можност да се однесуваат и како сервер и како клиент. Освен за комуникација, TOR се користи и за купување преку интернет поради зголемената безбедност.[18]

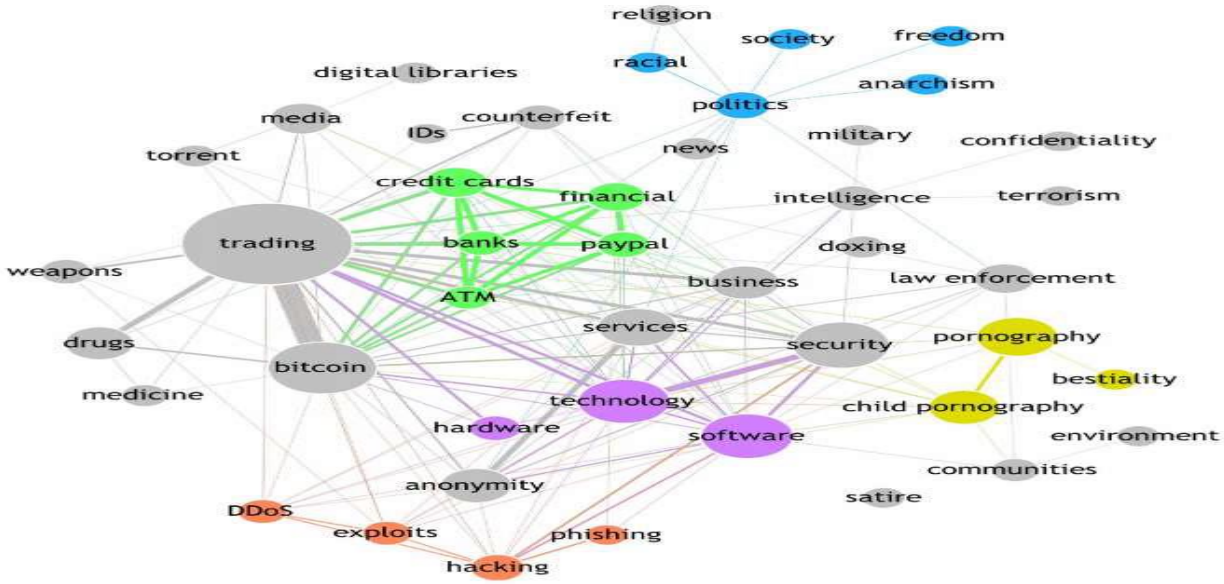
Важно е да се признае дека терминот Дарк нет првично се однесува на самата мрежа како техничка основа како протоколот и уредите; но не и содржината што може да се транспортира преку мрежата или може да се најде на соодветните сервери.

Најдлабоките слоеви на Длабокиот веб, сегмент познат како „Темна мрежа“, содржат содржини кои намерно се скриени, вклучително и незаконски и антисоцијални информации. Темната мрежа може да се дефинира како дел од Длабокиот веб, до кој може да се пристапи само преку специјализирани прелистувачи (како прелистувачот TOR). Една неодамнешна студија[19] откри дека 57% од Дарк нет е окупиран од нелегални содржини како порнографија, недозволени финансии, центри за наркотици, трговија со оружје, фалсификувана валута, терористичка комуникација и многу повеќе.

Постоењето на дигитален простор кој ги опфаќа горенаведените функции, луѓе и технологии би можело да сугерираат дека Темната мрежа е феномен што произлегува од потребата за тајност и анонимност помеѓу членовите на заедницата, слична на онаа на црниот пазар од физичкиот свет што постои од потребата за нерегулирана размена на стоки и услуги помеѓу поединци. Ветувањето за анонимност на Темната мрежа се отвора за легитимни употреби (на пример, за цивили кои бараат заштита од неодговорни корпорации, војници кои се инволвирани во тајни служби за команда и контрола, новинари кои вршат операции во земји без пристап до слободни медиуми и говор) како и незаконски активности (на пример, изнајмување хакери, приватна комуникација, координација за напади, изнајмување ботнети со променлива големина за да започне дистрибуирано одбивање на напади на услуги и заложување на украдени информации.[20]

[18]Abdulmuttaleb A., (2017) *Critical Analysis of the emerging Dark Web*, Cardiff Metropolitan University, p.6
[19] Moore, D., Rid, T. (2016). Cryptopolitik and the Darknet. *Survival,* London, 58, 7–38.
[20]Gupta, Maynard & Ahmad, Perth, (2019) *WA The Dark Web Phenomenon*, Australasian Conference on Information Systems, p.4

Во некои земји е неопходна употреба на Темната мрежа, додека во други не е неопходна поради варијацијата во правниот пејзаж меѓу нациите. Понатаму, поединци кои сакаат да останат анонимни во физичкиот свет може да имаат личност која ги претставува преку повеќекратни услуги преку интернет.



сл.3 Таксономија на скриените услуги на Темната мрежа[21]

Пазарите како „Патот на свилата“, „Ханза“ и „Алфа Беј“ се популарни со текот на годините бидејќи дозволија трговија на сомнителни стоки како недозволена дрога, оружје, украдени идентитети, украдени податоци за кредитна картичка, сексуална злоупотреба на деца и друго. „Патот на свилата“ беше еден од првите големи вакви пазари што достигна продажба над 1,2 милиони американски долари месечно, главно се состои од контролирани супстанции и наркотици. Оружјето е исто така популарна стока на такви пазари, но се засенети од продажбата на недозволени наркотици.

Украдените информации исто така се наоѓаат на продажба на овие пазари, се обезбедува анонимност на криминалецот и неговите контакти. Овие податоци може да вклучуваат продажба поврзана со финансиска измама, документи, на пр.

[21] Martijn Spitters, Stefan Verbruggen, Mark van Staalduinen (2014). *Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services*, IEEE Joint Intelligence and Security Informatics Conference

детали за кредитна картичка или кражба на идентитет што овозможува документи како медицинска евиденција иако овие обично имаат поголем рок на траење.[22]

Дерегулираната и анонимна природа на Темната мрежа е привлечна за голем број малициозни актери вклучувајќи терористички групи и хакери. Темната мрежа овозможува анонимни комуникациски активности вклучувајќи и регрутирање.

Терористичките групи можат да ја шират својата идеологија, однесување, регрутирање, споделување знаење, обучување, рекламирање, собирање средства, насочување и формирање заедници во целина без грижа за географска поделба или дури и присуство на локален водач. Исто така, Темната мрежа овозможува анонимна комуникација помеѓу хакери кои споделуваат информации.

Скриените услуги на TOR можат да помагаат во софистицирани напади, вклучително и одржување на канали за команда и контрола (C2) помеѓу напаѓачите и жртвите. Понудата за анонимност на TOR (нејзината тешкотија да се затвори) е идеална за C2 сервери и ова е една од најпопуларните достапни скриени услуги. Националните држави ја изразуваат својата загриженост за нивната потреба да се подготват за војна во дигиталното подрачје, особено онаму каде што ова војување влијае врз критичната инфраструктура и индустриските системи за контрола со потенцијал да има негативни исходи од реалниот свет. Оваа леснотија на влегување во суштината на сајбер-криминалецот дополнително се овозможува со оглед на асиметријата на воената средина.

И покрај фактот што сајбер-криминалците не се толку добро финансирани или опремени како организациите што ги таргетираат, тие имаат предност на дигиталното бојно поле.

Во сајбер-просторот оружјето може да биде кодирано, или лесно купено од Темната мрежа. По истиот принцип, одвраќањето повеќе не е домен на владите, како што понекогаш може да станат и недржавни актери, активни учесници во сајбер-војната против заедничките непријатели. Агенциите за спроведување на законот и хактивистичките групи ширум светот беа активни во намалувањето на активностите на терористичките групи на површината на вебот.

[22]Gupta, Maynard & Ahmad (2019), *The Dark Web Phenomenon*, Australasian Conference on Information Systems, p.4

Спроведувањето на законот, безбедноста на производите и услугите се редовни набљудувачи на сајбер-заедницата во Темната мрежа. Антивирусните програми и други безбедносни компоненти ги штитат своите корисници од малициозен софтвер врз основа на потписи добиени од минатите напади. Сепак, има поместување кон проактивен пристап кон безбедноста кога свесноста за ситуацијата е интегрирана во системот за управување со ризици и дел од свесноста за ситуацијата е собирање и обработка на податоци што може да помогне во управување со безбедноста.

Оваа идеја доведе до зголемување на практиката во разузнавањето за сајбер-заканите што вклучува собирање на податоци за истражување и сајбер-криминални активности, особено на форумите на Темната мрежа.[23]

Одбрани непријателски земји и нестабилни региони развиваат способности за развој на ОМУ, вклучувајќи ги Иран, Северна Кореја, Пакистан, Индија и други земји на Блискиот Исток. Иако нивните способности се пониски, нивото на закана е многу повисоко. Со собирање и анализирање (користење техники за мапирање на знаење) поврзани со публикации за нуклеарно оружје (списанија, написи, извештаи, написи за печат, итн.) што се генерирани од научници и истражувачи во овие региони со висок ризик, тие се способни да го идентификуваат „невидливиот колец на нуклеарни научници“ и нивните способности. Иако многу земји и институции покажаа силни способности во нуклеарните истражувања, нивното знаење, процеси, материјали и капацитети се недостапни за повеќето надворешни лица.

Во одделни земји од Блискиот Исток и муслиманските држави, локалниот нуклеарен персонал може да има поголеми шанси да биде принуден или под влијание на локалните радикални групи. Така, нивните објекти може да имаат поголема пристапност до непријателските агенти, што претставуваа значителна закана. Слично на тоа, во земјите од СССР од поранешниот источен блок, нуклеарни материјали и know-how може да бидат подостапни за локалните криминални групи и мафиите како недозволени цели. Потребно е да се направи систематска анализа

[23]Gupta, Maynard & Ahmad (2019), *The Dark Web Phenomenon*, Australasian Conference on Information Systems, p.5.

за пристапност на институциите и капацитетите во различни земји и региони со висок ризик.

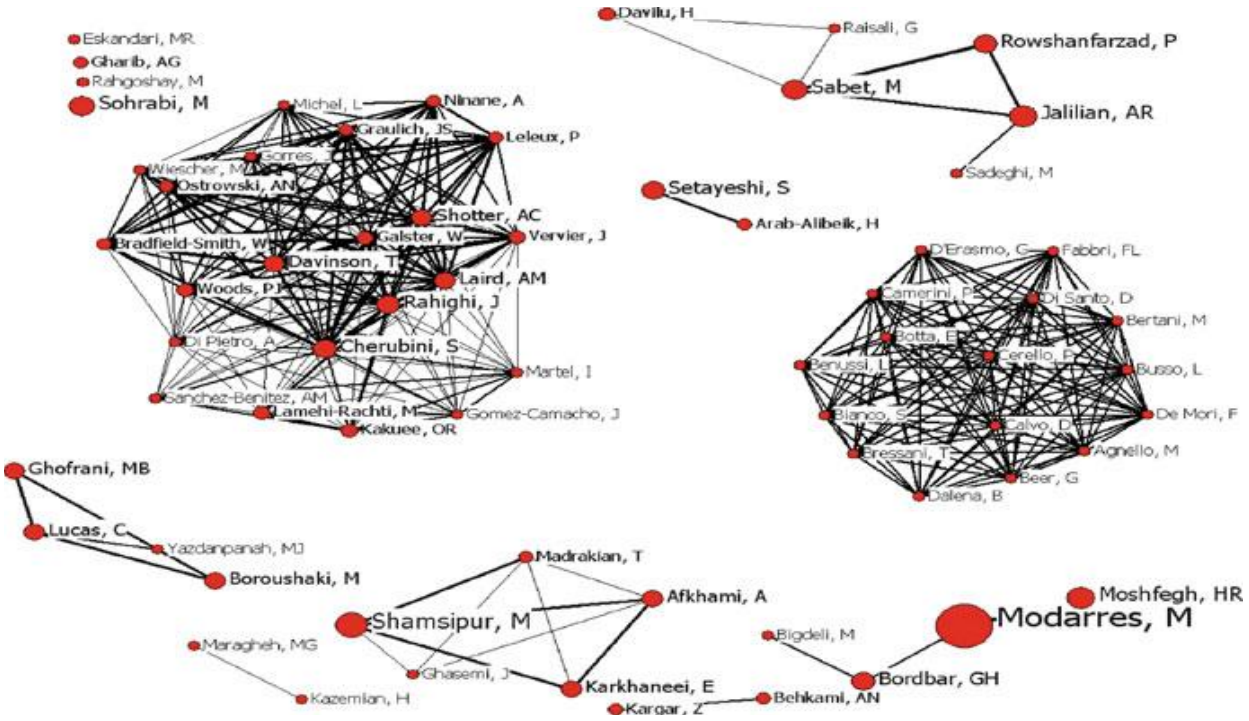
Во прилог на способноста и пристапноста, потенцијалната деструктивна намера на избраните радикални, екстремистички и терористички групи треба подобро да се проучат. Одредени терористички организации имаат повеќе високообразовани регрути и можат да настапуваат со пософистицирани и координирани операции (на пример, Ал Каеда). Кај многу терористи, веб–страници, форуми и блогови, прирачници за обука и инструкции за креирање експлозиви[24], био/хемиски агенси, па дури и нуклеарни бомби може да бидат лесно пронајдени. На овие темни мрежи, на сајтовите и форумите често се дискутираат и разменуваат радикални и насилни идеи за важноста кон глобалниот џихад и други деструктивни акти.

Веруваме дека се фокусирани техники за индексирање веб-страници коишто може да биде исклучително корисни за идентификување на намерата за нуклеарна закана на актерите во сајбер просторот на Темната мрежа.

Екстремистичките и терористичките групи често користат интернет за да промовираат омраза и насилство. Интернетот нуди сеприсутни, брзи, евтини и анонимни средства за комуникација за екстремистички групи. Во многу студии со анализа на содржина на Темната мрежа се пронајдени докази за идеолошко споделување на ресурси, собирање средства, пропаганда, обука и вработување.

Во други студии, беа анализирани насилството и омразата што имаат значително присуство во американски и блискоисточни форуми за екстремистички групи.[25] Гореспоменатите студии презентираат важни откритија за анализа на содржина кои обезбедуваат увид во динамиката на комуникација и пропаганда за ширење на форуми на Темната мрежа. Сепак, има ограничени податоци за идентификување и анализа на содржина која се однесува на нуклеарни закани и закани од ОМУ.

[24]H. Chen, (2010) *Dark Web: Exploring and Data Mining the Dark Side of the Web*, p.66
[25]Abbasi, A. and Chen, H. (2008), "Analysis of Affect Intensities in Extremist Group Forums," In: *Terrorism Informatics,* E. Reid and H. Chen, Eds., Springer, pp. 285–307.



Сл.5 Нуклеарна мрежа на темната мрежа

Фокусиран систем за индексирање за нуклеарна содржина на Темната мрежа содржи фазата на идентификација на локалитетот која има за цел да ги идентификува екстремистичките групи и нивните веб–страници.

Исто така, планирано е преку пребарување на големи пребарувачи да се идентификуваат други веб–страници со користење на внимателно развиена лексика од арапски и англиски нуклеарни клучни зборови. Фазата на обработка на страницата има три компоненти: пристапност, структура и генерација на обвивки. Компонентата за пристапност се занимава со стекнување и одржување, пристап до веб–страници и форуми на Темната мрежа. Структурната компонента е дизајнирана да се идентификува мапирањето на URL–то и да се измисли нарачување на URL–то за простор за индексирање со користење на релевантни карактеристики и техники.

Многу форуми на Темната мрежа не дозволуваат анонимни пристап. Со цел да овозможи пристап и да се соберат информации од тие форуми, мора да се создаде корисничка идентификација и лозинка, да се испрати барање за апликација до веб–

администраторот и да се почека добивање дозвола/регистрација за да се пристапи на форумот. Прелиминарна студија за Темната мрежа разви лексика од клучни зборови на англиски и арапски јазик поврзани со нуклеарната енергија на пример, „нуклеарна",„ физија",„критична маса" итн. Со користењето на „пајак" во процесот, се идентификуваа 128 арапски веб–страници и 95 англиски веб–страници сајтови со потенцијално релевантна нуклеарна содржина. Поголемиот дел од веб-страниците се однесуваат за меѓународните нуклеарни политики, особено за нуклеарните судири меѓу Западот и Северна Кореја и Иран. Други веб–страници се однесуваат за првата Ирачка нуклеарна програма. На пример, една од веб–страниците објави интервју со Ирачки нуклеарни научници кои учествувале во нуклеарката на поранешниот ирачки режим програма за оружје. Покрај тоа, некои џихадисти размислуваат за нуклеарното оружје да биде важна компонента во нивното идно работење.

Иако е значително потешко за откривање податоци за нуклеарна технологија генерирани од тероризам, во студијата се идентификувани неколку „буквари" напишани специјално за џихадисти. Овој сет лекции се најде на „Енциклопедија за обука и подготовка", веб–страница посветена да им обезбеди на идните џихадисти основна воена обука и корисни прирачници.

Исто така, се лоцира НТМ-работилница од 19 часови за нуклеарна технологија. Лекциите се собрани во 14 датотеки pdf формат со вкупно 477 страници. Целта на ова упатство е да ги научи муџахедините за основите на нуклеарната и ракетната технологија. Се потпираат на разни западни веб–извори и референци. Темите што се дискутираат во овој нуклеарен „буквар" за џихад се: вовед во нуклеарна физика, природно зрачење, нуклеарни карактеристики на некои елементи, нуклеарна бомба, нуклеарен материјал што се користи во бомбата, подготовка на радиум нуклеарна бомба, нуклеарни и ЕМ бомби и основна ракетна технологија.

3. Незаконски активности и услуги на корисниците на Темната мрежа

Нелегалните мрежни пазари, како на мрежната површина, така и на Темната мрежа, им овозможуваат на криминалните продавачи да ги истражат сите начини на тргување со недозволени производи. Многу од овие недозволени стоки и услуги, како што се алатки за компјутерски криминал или лажни документи, се можности за понатамошен криминал.

Интернет криминалците можат да ги злоупотребат поединците и организациите и тие тоа можат да го сторат без оглед на границите.

Активностите како што се трговија со дрога, оружје, злоупотреба на деца, трговија со чувствителни информации, малициозен софтвер и шпионски производи, споделување на софтвер, искористување информации што хактивистите ги откриваат во компјутерски системи или изнајмување на Ботнет, што е целосно опремена мрежа поврзана на интернет каде што хакерите можат да дејствуваат за да извршат нарушување на безбедноста во широк опсег. Дополнително има документи за размена, лажни лични карти, украдени кредитни картички, медицински досиеја на пациенти и сите други лични информации што можат да се идентификуваат.

Исто така, вклучува финансиска измама, рекламирање на криминални идеологии, дури и врбување на напаѓачи и многу повеќе.[26]

[26]Милошевска, Т. (2020), Дарк веб- Нова транснационална безбедносна закана, *Годишен зборник*, вол.73, Филозофски факултет, Скопје

Улога во поширок контекст	Специфични случаи	Опис
Улога-пазар	Незаконска трговија со наркотици	Цел опсег на наркотици од марихуана до кокаин се продаваат на платформи на eBay, како на пр. Патот на свилата 3.0[27]
	Малвер и злоупотреба-нулти ден+познати ранливости на пазарот	Експлоатација насочена на широк спектар на системи – од специфичен софтвер со мала популарност до распространети грешки во оперативниот систем како на пр. WannaCry Ransomware, Eternal Blue exploit[28]
	Кредитна картичка, идентитет, пробиени податоци што се тргуваат на пазарите	Украдени информации за кредитни картички, медицински профили, лични информации за идентификација (PII) кои овозможуваат идентификување на крадецот[29]
	Злоупотреба на деца, овозможени од социјалните платформи, понудени или одделна продажба	Слики и видеа за сексуална злоупотреба на деца, достапни за продажба. На пр. на сега веќе непостојната Playpen12.[30]
	Трговија со оружје	Продажба на оружје особено во земји каде е забрането[31]

[27]Tzanetakis, (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time, *International journal on drug policy*, p.176-186

[28]Armin, J. at al. (2015). 0-day vulnerabilities and cybercrime, in: Availability, Reliability and Security (ARES), 10th *International Conference On*.

[29]Denic, N. V. (2017). *Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web,* thesis presented to the Faculty of the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.

[30]Kirkpatrick, K. (2017). Financing the Dark Web. *Communication*. ACM 60, 21–22.

[31]Rhumorbarbe, D. at all., (2018). Characterising the online weapons trafficking on cryptomarkets. *Forensic Science Int*ernational 283, 16–20.

Улога во поширок контекст	Специфични случаи	Опис
Комуникациска платформа	Форум за дискусија	Размена на идеи, знаење, пропаганда, вработување, обука. Користено од страна на хакери, терористи, новинари, граѓани чувствителни на одредени теми[32]
	Разговор онлајн комуникација	Инстант пораки/чет помогнати од TOR, пр. TorChat13, или енкриптиран софтвер за комуникација, пр. Telegram14 и Signal15, кој е познат дека се употребува за приватна комуникација во реален момент[33]

Улога во поширок контекст	Специфични случаи	Опис
Овозможувач на кибер криминал	Сервис за малициозен софтвер/бизнис-модел за криминални услуги	DDoS и Ransomware е достапен за употреба како услуга и е хостиран како TOR скриени услуги[34]
	Сервери за команда и контрола (C2) распоредени како скриени услуги	Ботнет се контролираат од C2 услугите хостирани како TOR скриени услуги[35]
	Терористички операции спроведени во врска со други улоги	Врбување, обука, радикализација, планирање, собирање средства за познати терористички организации, на пр. Исламската држава ИСИС[36]

[32]Sapienza, A. at al. (2018). *Early Warnings of Cyber Threats in Online Discussions*. ar Xiv Prepr. arXiv1801.09781

[33]Maddox, A. at al. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde.' *Information, Communication and Society*. 19, 111–126, достапно на: https://doi.org/10.1080/1369118X.2015.1093531

[34]Huang, K. at al. (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*.

[35]Owen, G. Savage, N. (2016). Empirical analysis of Tor hidden services. IET *Information Security* 10, 113–118.

[36]Broadhurst, R. (2017). *Cyber Terrorism Research Review Cyber Terrorism*: Research Review Research Report of the Australian National University, достапно на: https://doi.org/10.13140/RG.2.2.19282.96964.

Улога во поширок контекст	Специфични случаи	Опис
Како извор на разузнавање за закани	Форуми за скенирање и места за разузнавање	Проценка за вид на напади кои може да бидат иманентни, засновани на информации кои се продаваат или разменуваат на форумите.[37]

Улога во поширок контекст	Специфични случаи	Опис
Овозможување анонимни финансиски трансакции	Употреба на биткоин преку TOR за анонимност	Додадено ниво на анонимност и претпазливост.[38]
	Перење пари на криптовалути преку Tumbling услуги	Специфични услуги за перење пари, на пр., преку конвертирање во биткоини[39]

Улога во поширок контекст	Специфични случаи	Опис
Како Прокси до површински веб	Избегнување цензура преку блокови за избегнување	Цивили вклучени во етичко однесување додека ја штитат приватноста, на пр. заобиколувајќи го штитот на Кина[40]
	Заштита од прогон од страна на локалните власти со применување анонимност	Новинари кои пишуваат за чувствителни теми што се однесуваат на земја која е позната по угнетувачки режим[41]

[37]Robertson, J. at al. (2017). *Dark web Cyber Threat Intelligence Mining*. Cambridge: University Press.
[38]DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep DarkWeb. *University of Illionois Law Review*.
[39]Dalins, J. at al. (2017). Criminal motivation on the dark web: A categorisation mode for law enforcement. Digital Investigation.
[40]Chertoff M., A (2017). Public policy perspective of the Dark Web, *Journal Cyber Policy*, p.28.
[41]Moore, D., Rid, T. (2016). Cryptopolitik and the Darknet. *Survival* (Lond). 58, 7–38.

Според Европскиот центар за мониторинг на наркотици и зависности од дрога[42] и Европол[43], Германија, Холандија и Велика Британија биле најважните земји во однос на снабдувањето со дрога преку Темната мрежа со седиште во ЕУ, во однос на приходите од продажба и обемот. Други истражувања покажуваат дека продавачите на одредени наркотици, како канабис и кокаин, првенствено се наоѓаат во мал број на високоактивни земји потрошувачи. Ова дополнително укажува на тоа дека повеќето продавачи на пазарот на Темната мрежа се „локални трговци на мало“ кои функционираат како „последна милја“ на рутите за трговија со дрога. Ова е поткрепено со други истражувања дека пазарите во Темната мрежа најмногу се користат за продажба на пазарот со среден или низок обем или продажба директно на потрошувачите.

Но, бидејќи трговијата со недозволена стока е една од најзначајните активности што се одвива на Длабоката мрежа, таа стана суштинска во контекст на висока анонимност, која може да гарантира доверба и углед кај продавачите и купувачите, без да се потпира на надворешен авторитет како банкарска институција во електронската трговија. Се предвидува пораст на нови, комплетно децентрализирани места кои се потпираат на технологијата блок-синџир кои биткоинот и другите криптовалути веќе ги користат за транспорт и складирање.

Постојат примери кои покажуваат дека Темната мрежа е совршена место за сајбер-криминал. Ова е единственото место каде што истовремено корисниците можат да станат сопственици на различни видови малициозен софтвер, но и нивни жртви. Сите се користат за дистрибуција на малициозен софтвер познати методи на фишинг и фарминг. Една голема група малициозен софтвер што може да се најде на Темната мрежа е CryptoLocker малициозен софтвер. Овие малициозни програми ги извршуваат жртвите по пристап до датотеките и шифрирање на истото. По шифрирањето на датотеките, жртвата се пренасочува кон страницата каде што е побарано да настапи плаќање ако сака да ја врати контролата врз своите податоци. Многу често има барања за плаќање, како и информации што е потребно да се

[42] The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) (2018), достапно на: https://www.emcdda.europa.eu/emcdda-home-page_en
[43] EUROPOL. (2018). *Internet Organized Crime Threat Assessment*, European Union Agency for Law Enforcement Cooperation, достапно на: www.europol.europa.eu.

изврши трансакција напишана на мајчин јазик, јазикот на жртвата. Улогата на TOR во таквите трансакции е да е домаќин на страници за плаќање со цел плаќање со користење биткоини кои се многу вообичаена валута за плаќање услуги во Темната мрежа.[44]

Постојат податоци дека припадниците на групата Исламска држава во Ирак и Левант преку користење на Темната мрежа обезбедиле вооружување за нападите во Париз и во Брисел. Организациите како што се ИСИЛ и Ал Каеда користат темна мрежа за активности кои не се директни напади преку интернет, но се во функција на основните цели и се посредни средства за терор и тероризам. Еден од видовите на користење интернет во терористички цели се однесува на врбување и регрутирање на нови сили, главно помлада популација, со ширење на пропаганден материјал како што се видео снимки во кои се опишуваат целите за кои се борат, начинот на борба и значењето на нивната војна. Во прилог на регрутирање на нови членови на Темната мрежа многу често се користат услуги во функција на тероризам и постигнување сигурна комуникација.

Сепак, овие терористички групи мигрирале на темната мрежа каде што:

- а) нивните поддржувачи можат слободно да ги изразат нивните мислења анонимно;
- б) нивното дејствување може да продолжи да се финансира преку виртуелни валути и
- в) Темната мрежа служи како потенцијален центар за регрутирање и терен за обука.

Ова е комуникација слична на социјалните мрежи и форуми, со таа разлика што следењето на овој тип на комуникација е речиси невозможно. Терористите исто така ја користат Темната мрежа за да добијат средства од нивните организации, перење пари, купување муниција и експлозиви.[45] Веб-порталите на темната мрежа се заштитени на различни начини. Еден од основните начини е да се проверат посетителите кои според однесувањето отстапуваат од стандардната шема.

[44]V. Ciancaglini, M. Balduzzi, R. McArdle, M. Rosler (2019), "Below the Surface: Exploring the Deep Web", *Trend Micro*, pp. 1-48.
[45]G. Weimann, (2016). "Terrorist Migration to the Dark Web," *Perspectives on terrorism*, Vol. 10, no. 3.

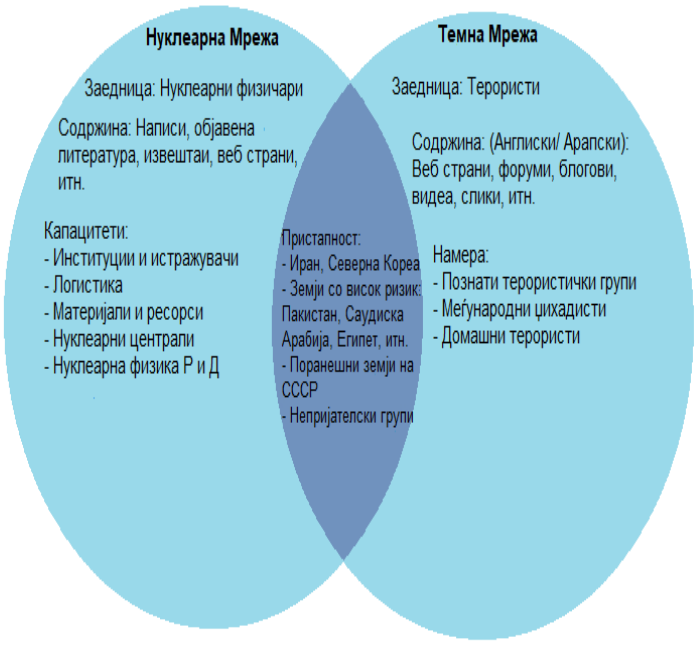
3.1. Оружје за масовно уништување на Темната мрежа

Моделот на способност-пристапност-намера неопходен е да се развие и имплементира за да се идентификуваат и анализираат:

- уникатните способности на земјите, институциите и истражувачи за развојот на нуклеарно оружје за уништување на масовно уништување;
- пристапноста на нуклеарните капацитети во земји со висок ризик (на пример, Иран, Северна Кореја и други земји на Блискиот Исток) и од потенцијални меѓународни и домашни терористички групи, и
- наведена намера (и закана) на одредени непријателски земји или терористички групи при добивање и користење на нуклеарни материјали.

Целта е развивање на база на знаење за „Нуклеарна мрежа“ за да ги претставува главните земји со висок ризик, организации, институции, истражувачи и нивните нуклеарни способности. Го искористуваат високо успешниот и меѓународно познат проект „Dark Web“, кој собира меѓународни генерирани џихадистички содржини (веб-страници, форуми, блогови, итн.) на интернет, за да се идентификуваат терористи и екстремистички групи и членови кои можеби ја изразиле својата незаконска намера да развијат или да користат такви нуклеарни способности за ОМУ.

Целта е да се направи рамка за способноста и пристапноста за овој вид оружје и каква е поставеноста во земјите со висок ризик, како и во екстремистичките и терористичките групи.



сл.6 Способност и пристапноста до ОМУ

Одделни непријателски земји и нестабилни региони развиваат способности за развој на ОМУ, вклучувајќи ги Иран, Северна Кореја, Пакистан, Индија и други земји на Блискиот Исток. Иако нивните способности се пониски, нивото на закана е многу повисоко. Со собирање и анализирање (користење техники за мапирање на знаење) поврзани со публикации за нуклеарно оружје (списанија, написи, извештаи, написи за печат, итн.) што се генерирани од научници и истражувачи во овие региони со висок ризик, тие се способни да го идентификуваат „невидливиот колец на нуклеарни научници“ и нивните способности.

Иако многу земји и институции покажаа силни способности во нуклеарните истражувања, нивното знаење, процеси, материјали и капацитети се недостапни за повеќето надворешни лица. Во одделни земји од Блискиот Исток и муслиманските држави, локалниот нуклеарен персонал може да има поголеми шанси да биде принуден или под влијание на локалните радикални групи. Така, нивните објекти

може да имаат поголема пристапност до непријателските агенти, што претставуваа значителна закана.

Слично на тоа, во земјите од СССР од поранешниот источен блок, нуклеарни материјали и know-how може да бидат подостапни за локалните криминални групи и мафиите како недозволени цели. Потребно е да се направи систематска анализа за пристапност на институциите и капацитетите во различни земји и региони со висок ризик.

Во прилог на способноста и пристапноста, потенцијалната деструктивна намера на избраните радикални, екстремистички и терористички групи треба подобро да се проучат. Одредени терористички организации имаат повеќе високообразовани регрути и можат да настапуваат со пософистицирани и координирани операции (на пример, Ал Каеда). Кај многу терористи, веб-страници, форуми и блогови, приручници за обука и инструкции за креирање експлозиви[46], био/хемиски агенси, па дури и нуклеарни бомби може да бидат лесно пронајдени. На овие темни мрежи, на сајтовите и форумите често се дискутираат и разменуваат радикални и насилни идеи за важност кон глобалниот џихад и други деструктивни акти. Веруваме дека се фокусирани техники за индексирање веб-страници кои може да биде исклучително корисни за идентификување на намерата за нуклеарна закана на актерите во сајбер просторот на Темната мрежа.

Екстремистичките и терористичките групи често користат интернет за да промовираат омраза и насилство. Интернетот нуди сеприсутни, брзи, евтини и анонимни средства за комуникација за екстремистички групи. Во многу студии со анализа на содржина на Темната мрежа се пронајдени докази за идеолошко споделување на ресурси, собирање средства, пропаганда, обука и врбување.

[46]H. Chen (2010). *Dark Web: Exploring and Data Mining the Dark Side of the Web*, Springer, p.66

3.2. Онлајн платформи-таргет на терористите

Од крајот на 90-тите години, терористите се активни на разни мрежни платформи.[47] Меѓутоа, беше откриено дека „Површината“ е премногу ризична за терористите кои бараат анонимност: тие би можеле да бидат набљудувани, проследени и пронајдени. Многу од терористичките веб-страници и социјалните медиуми на Површинскиот веб се следат од службите за борба против тероризам и честопати се затворени или пробиени. Спротивно на тоа, на Темната мрежа, децентрализираните и анонимни мрежи помагаат во избегнување на апсењето и затворањето на овие терористички платформи. „Активностите на ИСИС на површинските мрежи сега се следат внимателно, а одлуката на голем број влади да ја симнат или да ја филтрираат екстремистичката содржина ги принуди џихадистите да бараат нови безбедни засолништа на интернет“.[48]

Ова доведе до нивна миграција кон Темната мрежа и го направија нивното однесување уште поотпорно за да бидат нарушени. Поддржувачите сега можат слободно да ги искажат своите мислења анонимно; групите се со помала веројатност да бидат жртви на хактивисти кои се обидуваат да ги затворат веб-страниците поврзани со тероризам, а нивното работење може да продолжи да се финансира преку виртуелни валути. Покрај тоа, Темната мрежа служи како потенцијален центар за врбување и терен за обука на новоформираните групи или терористи „осамени волци“.[49]

По нападите во Париз во ноември 2015 година, ИСИС се сврте кон Темната мрежа да шири вести и пропаганда во очигледен обид да ги заштити идентитетите на приврзаниците на групата и да ја заштити нејзината содржина од хактивисти.

Овој потег следуваше откако стотици веб-страници поврзани со ИСИС беа урнати како дел од кампањата Операција Париз што ја започна аморфниот

[47]Weimann, G. (2017). *Going Darker-The challenge of Dark Net Terrorism*, Wilson Center, Washington DC, USA.
[48]Berton, B. (2015). “*The dark side of the web: ISIL’s one-stop shop?”*. Report of the European Union Insti-tute for Security Studies, достапно на: http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf.
[49]Brynielsson, J. at al. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists, Security Informatics, no.11.

хакерски колектив „Анонимус“. Медиумскиот центар на ИСИС, Ал-Хајат Медија Центар, објави линк и објаснувања за тоа како да се стигне до нивната нова страница на Темната мрежа на форум поврзан со ИСИС.[50]

Во април 2018 година, извештајот насловен „Терор во мракот“, ги сумира наодите од студијата која ја открива зголемената употреба на Темната мрежа од страна на терористичките групи. Наодите илустрираат како терористите и екстремистите создаваат сè поголем број безбедни засолништа на Темната мрежа за да закажат идни напади, да соберат средства и да регрутираат нови следбеници. Овој извештај ги истакнува следниве употреби на Темната мрежа за терористички цели:

1. Терористите ја користат Темната мрежа за да се сокријат: Следењето на површинската мрежа од страна на компаниите за социјални медиуми и безбедносните службеници резултираше во побрза стапка на отстранување на екстремистичката содржина од платформите за социјални медиуми. Во корелација со ова е зголемената употреба од страна на терористичките мрежи на Дарк нет за комуникација, радикализација и планирање напади.

2. Терористите ја користат Темната мрежа за регрутирање: Додека почетниот контакт може да се направи на површинските веб-платформи, понатамошните инструкции често се даваат на апликациите за криптирање од крај до крај, како што е Телеграм за тоа како да се пристапи до џихадистичките веб-страници на Темната мрежа.

3. Терористите ја користат Темната мрежа како резервоар на пропаганда: Отстранувањето на екстремистичката и терористичката содржина од мрежната површина го зголемува ризикот материјалот на терористичките организации да се изгуби. Голем дел од овој материјал подоцна се појавува во Темната мрежа.[51]

4. Терористите користат виртуелни валути за да избегнат откривање и прибирање финансиски средства: Терористите, како криминалци, користат

[50]Милошевска, Т. (2020), Дарк веб- Нова транснационална безбедносна закана, *Годишен зборник*, вол.73, Филозофски факултет, Скопје.
[51] Weimann, G. (2016). “Going Dark: Terrorism on the Dark Web”, *Studies in Conflict & Terrorism* 39, 195-206, достапно на:
http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546

криптовалути, бидејќи тоа обезбедува иста форма на анонимност во финансискиот амбиент како што е криптирањето за комуникациските системи.[52]

Со оглед на тоа што Темниот веб е најпознат по тоа што е домаќин на нелегална економска трговија, стана јасно дека Темниот веб има и некои многу сериозни импликации за национална безбедност што ќе влијаат врз повеќето нации низ целиот свет. Распространувањето на кибер и кинетичко оружје, олеснување на тероризмот, собирање разузнавачки информации, изнудување, злонамерни услуги за изнајмување на сите овие недозволени активности се случуваат на Темниот веб, а доказите дадени во овој труд сугерираат дека овие активности може да се јавуваат со зголемени стапки во иднина.[53]

Вмреженото глобално општество што е овозможено преку интернет и придружните дигитални технологии и платформите за социјални медиуми создадоа прифатлив, географски и временски неограничен и полуанонимен простор каде што размената на дијалог, идеи и повици за акција е зголемена.

Иако истражувањата за употреба на Интернет од страна на терористичките организации се достапни во изобилие, корелација на платформи за социјални медиуми, понапредна технологија, темна мрежа и нивна експлоатација од многу демографски помлади терористички организации обезбеди нов пејсаж за истражување не само во организацијата на овие групи во современата дигитална ера, туку и нивни цели, намери и нивно афектно убедување преку интернет со цел да ја оствари својата мисија.

[52]Weimann, G. (2016). "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism* 39, 195-206, достапно:
http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546
[53]Rivera, J. Archy, W. (2019). The Role of the Dark Web in Future Cyber Wars toCome, *Small War Journal*, достапно нат: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-com.

4. Механизми за оспособување на темната мрежа преку употреба на криптовалути

TOR не беше единствениот развоен концепт што овозможи создавање и пристап до Темната мрежа. Постојат две главни услуги што служат за практични цели во овозможувањето на Темната мрежа. Тоа се Hidden Wiki и Биткоин. Секој од нив дава решение што овозможува Темната мрежа да биде достапна и употреблива за оние што ја бараат. Раниот предизвик за Темната мрежа беше тоа што беше тешко да се најдат скриените страници. Hidden Wiki го донесе првиот бран корисници во 2004 година. Оваа страница содржи каталог на сите веб-страници на Темниот веб-сајт што се моментално активни, повратни информации од корисниците на тие страници и информации за тоа до што може да се пристапи преку секоја страница.

Друг начин да се најдат сајтови е со користење на пребарувачи специфични за TOR, како што се Ахмија, која ги индексира сите скриени страници што може да ги најде, и Грамс, која конкретно ги наоѓа скриените сајтови кои продаваат недозволени лекови, оружје и фалсификувани пари.[54] Со цел да се спроведат вистински трансакции, пазарите на Темната мрежа исто така, почнаа да користат валута, биткоин, кој е псевдоним и е толку тежок за следење како TOR. Биткоинот стана стандардна валута на Темната мрежа.

На терористите им се неопходни значителни финансиски средства за извршување напади и други активности. Доколку терористичките групи се подобро финансирани во целина, може да има почести, поуспешни и поголеми напади.[55] Постојат неколку причини што ја поддржуваат оваа хипотеза.

[54]Finklea, K. (2015). *The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement*, CRS Report R41927 p.35
[55]Acharya, A (2009). *Targeting Terorist Financing: International Cooperation and New Regimes*, New York: Routhledge.

Прво, повеќе средства за операции веројатно ќе доведат до зголемено финансирање на структурите што ги овозможуваат овие напади, кои вклучуваат регрутирање и обука на напаѓачи и инспирирање на потенцијални осамени волци.

Второ, групите кои се соочуваат со помал монетарен притисок, исто така може да бидат по подготвени да ризикуваат, како што се поголеми или поризични напади.[56]

И на крај, а можеби и повеќе спорно, зголемените средства можат да се користат директно за дополнителни и поголеми напади. Можеби е тешко да се поврзат директно зголемените средства со терористички напади, иако во специфични документирани случаи „литературата често опишува недостиг на готовина како проблем за терористички операции“.[57]

Дали и како терористичките организации би користеле систем на криптовалута зависи од достапната технологија и нејзините својства како и од потребите и можностите на организацијата. Поновите криптовалути може да се појават со својства што терористичките организации ги сметаат за поприврлечни од оние на моментално достапните криптовалути. На пр. ако идната криптовалута обезбедува подобра анонимност од Биткоин за големи трансакции и е пошироко усвоена од Zcash, тогаш терористичките организации би можеле да бидат подготвени да ја користат таа валута за специфични активности. Затоа, важно е да се разгледаат одделни терористички групи за да се анализира што би требало од криптовалутите и да се споредат тие потреби со својствата на досегашните криптовалути.

Биткоинот постојано го користат купувачите и потрошувачите на недозволени добра и услуги на Темната мрежа. Во извештајот под наслов „Терористичка употреба на виртуелни валути: содржана потенцијална закана“ се наведува дека терористичките организации ги користеле криптовалутите за да го

[56]Shapiro, J.N. (2012). Terrorist Decision-Making Insight from Economics and Political Science, *Perspectives on Terrorism*, Vol.6 No.4-5.
[57]Oftedal, E. (2015). *The financing of Jihadi Terorist Cells in Europe*, Norway: Forsvarets Forskningsinstitutt.

поддржат опстанокот на нивните организации. На пр. терористичката организација во појасот Газа ги искористи криптовалутите за финансирање на нивните операции, како и членовите и приврзаниците на Исламската држава во Ирак и Сирија (ИСИС) кои особено ги користеа криптовалутите евидентирани во Индонезија и САД.

Забележувајќи понатаму дека значителното и ненадејно губење на нивната физичка територија, како и ширењето на опсегот на воените операции може да го ограничат нивниот пристап и да ги откажат пресметувањата на нивните финансии преку географските области и границите или традиционалната финансиска трансакција наречена хавала што се однесува на физичката финансиска трансакција со користење на локален брокер за трансфер на пари помеѓу локации.[58]

Така, овој феномен потенцијално ги охрабрува терористичките организации да ја истражуваат новата технологија што може да ја поддржи нивната способност да ги движат средствата преку криптовалутите.

Постојат различни начини на кои може да се користат виртуелните криптовалути од страна на терористичките групи. Организациите можат да ја користат Темната мрежа за добивање на оружје, вклучувајќи традиционално огнено оружје, експлозиви, хемиски и биолошки токсини, плаќајќи ги со виртуелни криптовалути.

Виртуелните криптовалути исто така може да олеснат други активности за недозволени приходи од терористичките групи; виртуелни барања за криптовалута за време на киднапирање за откуп. Слично на тоа, ако терористичките организации се насочат кон повеќе дигитални напади или сајбер тероризам, виртуелните криптовалути може да станат покорисни за овие организации, бидејќи дозволуваат набавка на дигитално оружје како што е малициозен софтвер. Очигледно, виртуелните криптовалути не се клучни за ниту една од овие активности, но тие

[58]Ward, A. (2018) *Bitcoin and the Dark Web: The New Terorist Threat*? RAND Corporation, January, достапно на: http://www.rand.org/blog/2018/01bitcoin-and -the-dark-web-new-terrorist-threat.html

можат да ги направат овие трансакции полесни од традиционалните плаќања со картички или банкарските трансфери.[59]

Зголемената употреба на криптовалути на комплементарни и соседни пазари може да укаже на нивната зголемена одржливост меѓу терористичките организации. Некои операции за фалсификување започнаа да користат темни мрежи и постои значителна трговија со украдени кредитни картички и идентитети на овие операции.[60]

Улога во поширок контекст	Специфични случаи	Опис
Овозможување на анонимни финансиски трансакции	Употреба на Биткоин преку TOR за анонимност	Додадено ниво на анонимност и претпазливост[61]
	Перење пари на криптовалути преку Tumbling услуги	Специфични услуги за перење на пари, на пр. преку конвертирање во биткоини[62]

Табела 4

Постојат неколку недозволени цели на искористување на криптовалутите од терористички организации, како што е набавка на дрога, продажба на наркотици, оружје и дозволување на недозволени услуги во Темната мрежа. Покрај тоа, терористичките организации започнаа, односно промовираа сопствени донации преку криптовалутите. Може да се заклучи дека криптовалутите може да се претворат во исплата на откуп. Покрај тоа, постојат неколку карактеристики на криптовалути кои обезбедуваат предности за корисниците, односно се подобри од

[59]Enternmann, E, Willem van derBerg (2018). *Terorist Financing and Virtual Cirrencies: Different Sides of the Same Bitcoin?* International Centre for Countering Terrorism, Hague.
[60]Aliens, C. (2016), Darknet Bust: Global Law Enforcement Raids Massive Counterfeiting Organization, *Deep Dot.Web*, December 17.
[61]DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. *University Illionois Law Review*.1267.
[62]Dalins, J.at. al. (2017) Criminal motivation on the dark web: A categorization model for law enforcement. *Digital Investigitation*.

готовината или кредит, разменливи за стоки и услуги, конвертибилност и стабилност на вредноста.[63]

Терористичките мрежи се приспособија на технологијата, вршејќи сложени финансиски трансакции во дигиталниот свет, вклучително и преку криптовалути.[64]Врз основа на студијата спроведена од RAND Европа насловена „Зад завесата: недозволена трговија со огнено оружје, распрскувачки материи и муниција на мрачната мрежа“, постои директна врска помеѓу терористичките напади во Париз и Минхен како и со оружјето кое било набавено преку Темната мрежа со криптовалути.

Студијата покажала дека имало дваесет и четири пазари на француски и британски криптовалути на „Темната мрежа“ во текот на септември 2016 година, каде што 75 проценти од трансакциите докажале дека реализираат недозволена трговија со оружје.[65] Оружјето што го користеле напаѓачите може да биде поврзано со пропагандата на ИСИС која повикувала на ширење на поедноставни напади со употреба на возила, огнено оружје, хемиско оружје и ножеви. Покрај тоа, организацијата поврзана со Ал –Каеда, имено al- Sadagah, користела Фејсбук и Телеграм за да ја започне својата финансиска кампања преку Биткоин.[66]

Во 2020 година, Работната група за финансиска акција (FATF), меѓувладино тело, го потенцираше можното зголемување на терористичкиот интерес за криптовалутата, особено за време на пандемијата COVID -19. Во мај, FATF објави извештај во кој се тврди дека пандемијата на коронавирус може да доведе до „зголемување на злоупотребата на онлајн финансиски услуги и виртуелни средства за преместување и прикривање на недозволени средства“. Помалку од еден месец по објавувањето на Министерството за правда на САД, FATF објави друг извештај

[63]Everette J. (2017) *Public-Private Analytic Exchange Program: Risks and Vulnerability of Virtual Currency*, Washington, Director of National Intelligence.
[64]The United States Department of Justice (2020), Office of Public Affairs, Global Disruption of Three Terror Finance Cyber –Enabled Campaigns, 13 August.
[65]Everette J. (2017). Public-Private Analytic Exchange Program: Risks and Vulnerability of Virtual Currency, Washington, Director of National Intelligence.
[66]Malik, N. (2018). How Criminals and Terrorists Use Cryptocurrency: And How To Stop It, Forbes, 31 August, достапно на: http://www.forbes.com/sites/nikitamalik/2018/08/31 how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it//

за индикатори со црвен аларм, истакнувајќи дека виртуелните средства може да се користат од финансиери на тероризам и перачи на пари.

Индикаторите се движат од уникатни модели на трансакции до профили на географски ризик што може да укажуваат на злоупотреба на виртуелните средства. За единиците за финансиско разузнавање, давателите на услуги за виртуелни средства и финансиски институции, овие индикатори обезбедуваат корисни упатства за спротивставување на употребата на криптовалута од низа недозволени актери. И покрај упатствата на ФАТФ и потегот од август 2020 година на САД за запленување и барање за одземање на финансиските средства на Хамас, Ал Каеда и ИСИС, терористите сè повеќе користат криптовалута за да собираат и складираат богатство.

Овој пат е особено веројатен заради веројатното континуирано потпирање на виртуелно деловно работење, дури и откако ќе се дистрибуираат вакцините за КОВИД- 19 во текот на 2021 година. Бидејќи повеќе потрошувачи користат криптовалути, можностите за терористите ќе се зголемуваат, бидејќи тие бараат покривање и прикривање на зголемениот обем на поважните трансакции.

Генерално, употребата на криптовалути треба да се гледа како дел од општата промена кон тероризмот преку интернет.[67]

[67]Casadei B.(2019) Terorist Use of Cryptocurrencies- A Blockchain Compliance White Paper, Blockchain Consultus, London, United Kingdom

5. Поим за сајбер војување

Голем број автори се обиделе да ја објаснат природата сајбер-нападите, но никој од нив не успеал да дојде до појасен заклучок каква ќе биде нивната природа во иднина.[68] Од историска перспектива, секој технолошки напредок доведе до создавање нови концепти што станаа многу важни за теоретичарите по национална безбедност. По авијацијата, нуклеарното и термонуклеарното оружје и дефинирање на универзумот како простор каде што може да се случат конфликти, „сајбер“ стана нов популарен термин во литературата за безбедносни прашања.

Иако оригиналните креатори на Интернет, како глобалната мрежа која го лансираше сајбер како феномен, се видоа само позитивни аспекти во однос на полесно вмрежување и размена на податоци, сајбер исто така донесе и голем број нови безбедносни предизвици и закани, меѓу нив, заканата од конфликт меѓу државите во сајбер-сферата. Има согласност дека сајбер-нападите навистина претставуваат реална опасност за националната безбедност и дека тоа е „совршено стратешко оружје“ за државите, бидејќи отвора нови можности за војување.[69]

Само површинскиот преглед на промените за оваа област зборува за тоа дека на сила се значајни подготовки за потенцијални конфликти во оваа сфера. Некои проценки укажуваат на тоа дека повеќе од 140 држави развиле офанзивни сајбер способности, додека голем број од нив создава и воени сајбер единици како Велика Британија која развива „широк спектар на воени сајбер капацитети, вклучително и способност за напади“.[70]

Кларк и Кнејк го дефинираат сајбер војувањето како „неодобрен влез во име или со поддршка на владата на една држава во мрежата на друга држава или која било друга активност што влијае на компјутерскиот систем, со цел да додаде, промени или фалсификува податоци или да предизвика прекин на податоците или

[68]Libicki, Martin (2011). C. Cyber War as a Confidence Game, *Strategic Studies Quarterly* no. 5
[69] Geers, Kenneth. (2013). Sun Tzu and Cyber War (NATO Cooperative Cyber Defence Centre of Excellence; Libicki, Cyber War as a Confidence Game; Schmidt, Eric & Cohen, Jared. *The New Digital Age: Reshaping the Future of People, Nations and Business*, John Murray Publishers.
[70]Iasiello Emilio (2015). Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs*. Vol.7.

штета на системот, мрежниот уред или на објектите што го контролираат компјутерскиот систем.[71] Џозеф Нај сметал дека сајбер војувањето ги вклучува само оние напади кои „имаат ефект што ги засилуваат или се еднакви на кинетичкото (конвенционално) насилство.[72]

Сингер и Фридман[73] се на ставот дека постојат два критериуми по кои се одредува дали нападот може да се смета како елемент на војна. Првиот критериум е дали во нападот е употребена соодветна сила што одговара на конвенционалното војување, додека вториот критериум е постоење насока и мерливост, односно постоење „насочена и намерна врска меѓу причината и последицата“. Со други зборови, мора да постои јасен доказ дека дадениот напад е дел од пристапот на одредена држава што сака да го загрози функционалниот систем на државата што е цел, вклучувајќи и безбедност на нејзините граѓани, како и употребата на сила што одговара на конвенционалната војна.

5.1 Сајбер војување-предизвик на модерното време

Сајбер војувањето е концепт на војување каде што спротивставените страни ги користат сите неопходни средства за постигнување на своите цели, за што физичкиот свет стана премногу мал во добата на хибридната војна. Поради секојдневниот развој, еволуцијата на технологијата и секојдневниот проток на информации, растечкиот виртуелен сајбер простор се користи како ново воено поле што може да стане главно боиште за војување.

Во новото доба на сајбер војувањето, сајбер просторот го замени класичното физичко боиште, со огромен виртуелен простор каде што се применуваат информатичката технологија и електромагнетниот спектар, а што во голема мерка

[71]Clarke, Richard A. & Knake, Robert K. (2010) *Cyber War. The Next Threat to National Security and What to Do About It*, Harper Collins e books, 109.
[72] Nye, Joseph S. Jr, (2010), Nuclear Lessons for Cybersecurity. *Strategic Studies Quarterly* 5 no.4, 21.
[73] Peter W. Singer, Allan Friedman. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York: Oxford University Press.

влијаат на физичкиот свет. Информатичката и комуникациската технологија се менуваат и унапредуваат секој ден, па во сајбер просторот брзо се зголемува бројот на безбедносни ризици, предизвици и закани. Се поставува прашањето, како може да се дефинира ова ново бојно поле, кои закони за него се применуваат и каде се неговите граници. Со оглед на напредекот на технологијата, дали сајбер просторот станува главно бојно поле што во претстојните години ќе го користат актерите.

Сајбер војувањето главно се користи како термин од 2007 година и постојано добива нови дефиниции затоа што постојат нови закани што се развиваат и во поглед на она што официјално се нарекува хибридна војна во Либан, во 2007 година, 2014 година во Украина, активностите на ИСИС, севернокорејските активности и американско-руските односи во последните неколку години, можеме да видиме еволуција на термини, посебно што не го користат само западните земји, туку и руската доктрина се приспособува на овој концепт. Сајбер војувањето ја достигна новата фаза во својот развој, од употреба на сите аспекти за победа над спротивставените страни, до користење на пософистицирани аспекти како примарната, сајбер-војна, информациското војување, со помала употреба на конвенционалните сили и други аспекти на хибридното војување.

Сајбер војувањето и информациското војување се поврзани со хибридното војување или се сметаат за негов дел, иако денес тие можат да се одделат и да се водат одделно од конвенционалното војување и другите аспекти на хибридните војни. Постојат два начина на кои сајбер просторот може да се користи како воено поле, по пат на сајбер војување и информациско војување. Главен метод на сајбер-војната се сајбер-нападите, додека главните актери се „паметните" системи, војници со сајбер вештини и хакери, а главни цели претставуваат ИКТ системите и критичната инфраструктура.

Додека сајбер-криминалците традиционално се фокусираат на таргетирање на корпорации преку напади со откуп и кражба, фокусот се префрли на оној кој краде и продава податоци, а информациите за поширокота јавност се производот што се продава. Во февруари 2021 година, заканувачки актер понуди база на податоци од над 500 милиони сметки на Facebook, филтрирани по држави,

за продажба на форма Темната мрежа. Фактот дека беше поделен на земји доби позитивни коментари од повеќе членови на форумот поради новата погодност што ја нуди на пазарот за украдени податоци. Ова беше голем потег во насока кон пакување и продажба на лични податоци украдени од компаниите на социјалните медиуми.[74]

Главниот метод на информациска војна би бил искористување на ранливи информации и социјален инженеринг или објавување/протекување информации, главни актери се разузнавачите, хакерите, медиумите и аналитичарите, а главни цели би биле луѓето, медиумите, ранливите информациски системи, ИКТ системи и општеството во целина. Примерите вклучуваат доверливи документи на MK-9 Reaper UAV, тактики за ублажување и прирачници што ги продаваат хакери на темната мрежа кои користеле различни ингеренции за пристап до ранливите американски мрежи Netgear. Хакерот користел едноставни методи на инфилтрација за да пристапи до компјутерот на американскиот капетан и да извезува податоци за апликации со податоци за пристап, а откако ги симнал доверливите документи, ги продавал на Темната мрежа.

Во август 2021 година, друг заканувачки актер протекол милиони записи на корисници на LinkedIn, исто така филтрирани по држави, на форум на Dark Web (оригиналната база на податоци беше протечена во јуни 2021 година). Во текот на истиот месец, друг актер понудил да продаде украдени записи на LinkedIn филтрирани по професија, вклучително и сметки на LinkedIn од 12,9 милиони ИТ персонал, 6,7 милиони професионалци за човечки ресурси и 4,8 милиони директори за финансии. Друго забележително прекршување на извршните сметки се случи кон крајот на 2020 година, кога заканувачки актер понуди да продаде пристап до сметките на е-пошта на стотици директори, вклучително и финансиски директори.[75]

---

[74] Aaaron Holmes (2021) 533 million Facebook users' phone numbers and personal data have been leaked online, *Insider*, достапно на: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.

[75] Cognyte CTI Research Group (2021), *2021 Linkendin Breach: Cyber criminals are the new heradhunters,* достапно на: https://www.cognyte.com/blog/2021-linkedin-breach-cybercriminals-are-the-new-headhunters/#

Прекршувањето на податоците се состоеше од записи кои вклучуваа различни полиња, како што се име, презиме, име на компанија, ознака, ID на е-пошта (регистриран во LinkedIn), земја и врска на профилот на LinkedIn. Заканувачкиот актер, исто така, обезбедил списоци што ги сумираат информациите кои се однесуваат на застапените земји и професии. Понатамошното испитување на активноста на актерот откри дека тој се фокусирал на записите од украдените бази на податоци. Фактот што актерот ја поделил својата база на податоци на LinkedIn конкретно на човечки ресурси (HR), информатичка технологија (ИТ) и финансиски персонал може да укаже дека овие вработени се со поголема веројатност да бидат цел на сајбер престапници.

Септември 2021. Сајбер-напад против Обединетите нации се случил во април 2021 година, таргетирајќи ги корисниците во мрежата на ОН за дополнително долгорочно собирање разузнавачки информации. Хакерот можел да пристапи до нивните мрежи преку украдени кориснички акредитиви купени на Темната мрежа.[76]

Ова покажува дека човечкиот фактор сè уште е оној со најголем ризик за безбедноста на информациите и дека социјалните инженери можат да „хакнат“ во секое време и каде било. Протекувањето на овие документи ќе предизвика големи штети на системот, додека кражбата на пристапните податоци на службените лица е предупредување за системот за информациска безбедност.

Во глобалното безбедносно опкружување кое брзо се менува, не смееме да ги заборавиме терористичките и организираните криминални организации, како и големиот број слободни актери кои играат значајна улога во денешната глобална безбедност.

Бојното поле во сајбер просторот сè повеќе ги заменува редовните боишта, а веројатно е дека во иднина ќе гледаме хибридна војна со примарен аспект на сајбер-војната, проследена со асиметрични закани, конвенционално војување и други. Државите и другите актери се поподготвени да користат тајни акции и да се кријат

[76] Center for Strategic and International Strudies (2022), *Significant Cyber Incidents*, достапно на: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

во анонимноста на сајбер просторот, наместо да распоредуваат единици на физичкото бојно поле.

Во ерата на хибридното војување, растечкиот мултиполарен свет е во еден вид безбедносна неизвесност, каде што границите меѓу мирот и војната секојдневно се менуваат и се замаглуваат бидејќи има многу актери во хибридната војна и ништо не е толку едноставно како порано. Сè уште не сме сведоци на сите отворени сајбер-војни каде едната страна целосно би ја уништила информацискатa критична инфраструктура на спротивната страна, но тоа е нешто за што се подготвуваат големите сили.

Едно е сигурно, основната работа што треба да се направи е да се вклучи обука во областа на безбедносната култура со акцент на свеста за сајбер безбедноста и информациите за безбедноста на информациите, бидејќи луѓето се најслабата алка во сајбер-војната. Државите и меѓународните организации сè уште имаат голема улога, а прво треба да се развие сеопфатен закон за сајбер просторот, а потребна е само политичка волја.[77]

5.2 Улогата на Темната мрежа во идните сајбер-војни

Војувањето се менува постојано, односно како што се проширува војувањето, така се зголемуваат и областите за кои се војува. Се поставува прашањето како темната мрежа преку интернетот влијае на националната безбедност, во последната декада, попрецизно како Темната мрежа, преку шверцот со оружје, тероризмот, изнуда, малициозни софтвери има безбедносни импликации. Да се разбере Темната мрежа во идните сајбер војувања бара од сите аспекти да се разгледува проблемот од повеќекратна перспектива. Секако, од подеднаква важност се економските и разузнавачките оперативни перспективи. Темната мрежа може да се набљудува како природна основа на две страни кои се анонимно вклучени во размена на информации, оружје и национални безбедносни тајни.

[77]Tisma, M. (2020). Hibridno ratovanje i bojno polje, Odbrana i bezbednost, Analiza sa distance, достапно на: https://odbranaibezbednost.rs/2020/02/11/hibridno-ratovanje-i-bojno-polje/

Еден од примарните предизвици за професионалците од областа на националната безбедност, при анализа на темната мрежа, е тешкотијата да се постигне заедничко разбирливо решение за тоа што значи самиот термин. Терминот „Темна мрежа“ е двосмислен и често се поистоветува со другите термини како што е „Длабока мрежа“ или „Криминално подземје“. Потребно е да се разбере како Темната мрежа може да влијае на национално – безбедносните интереси на националните држави низ целата планета.

Области на Интернет	„Површинска мрежа“	„Длабока мрежа“	„Темна мрежа“
дефиниција	Секој дел на интернет што е пристапен и е индексиран преку конвенционални средства за пребарување (Google, Yahoo, Bing)	Содржи податоци што динамички ги создава апликација, неповрзани или самостојни веб-страници/веб-страници, не-HTML содржини и податоци што се приватно чувани и класифицирани како доверливи	Дел од интернет што не само што не може да се индексира, и нема пристап преку стандарни пребарувачи (Expolorer, Chome, Firefox)
Веб примери	Секој вебсајт што може да се пристапи преку отворен пребарувач	Секој вебсајт на кој се пристапува со логирање (некои социјални медиуми, видео стрим). Оваа категорија вклучува и „подземни“ форуми	Секој вебсајт што завршува со .2р домејн. Обично, овие имиња не се зборови од речник, туку комбинација од букви и бројки заради анонимност.

Табела 5[78]

[78] Clearing Up Confusion - Deep Web Vs. Dark Web - Brightplanet", (2014), *Brightplanet*, достапно на: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.

Да бидеме појасни, и Surface Web и Deep Web имаат важност за националната безбедност во нивните сопствени погледи. Разузнавачките агенции ширум светот редовно го користат разузнавањето со отворен код (OSINT) што се наоѓа на Surface Web; додека Deep Web е локација на избор за оние сајбер криминалци кои сакаат да се вклучат во купување и продавање на украдени податоци за идентитетот, како што се броеви за социјално осигурување и други лични информации за идентификација. Сепак, за целите на овој труд, ќе се фокусираме единствено на Темниот веб, како што е дефинирано со цел да се биде достапен само преку специјален протокол за прелистување на интернет, како што е The Onion Router (TOR).

Како што е претходно опишано, Темната мрежа е достапна само преку неконвенционални прелистувачи, особено TOR и I2P (од кои попопуларно средство е TOR). TOR обезбедува анонимност преку насочување на интернет сообраќајот преку други „TOR јазли“ или компјутери користејќи го прелистувачот. Овој сообраќај отскокнува низ TOR јазлите додека на крајот не замине преку „излезен јазол“. Ова во суштина создава „onion“ или повеќеслојна анонимност.[79]

За да се разбере Темната мрежа во контекст на националната безбедност, треба да се фокусираме на две варијабли: комерцијалниот аспект и комуникацијата. Од комерцијален аспект, професионалците за национална безбедност сакаат да разберат како различни актери ќе ја користат Темната мрежа за да се вклучат во недозволена и/или тајна трговија. Од комуникациска перспектива, професионалците за национална безбедност сакаат да разберат како овие актери ќе ја користат Темната мрежа за да спроведат планирање, регрутирање, собирање разузнавачки информации и други активности од интерес.

[79]The Tor Project, Inc, *Torproject.Org*, достапно на: https://www.torproject.org/

Постојат две општи локации на Темната мрежа:

Пазари: Локации на Темната мрежа каде што поединците можат да бидат активни за да се вклучат во недозволена/тајна трговија.

Форуми: Локации на Темната мрежа каде што поединци настојуваат да се вклучат во „безбедни“ дискусии кои се однесуваат на различни прашања.

Еден од примарните предизвици што ги поставува Темната мрежа за професионалците за национална безбедност е издвојување на „бучавата“ од прашања од легитимна национална безбедност. Со оглед на тоа што годишниот приход од компјутерски криминал се проценува на приближно 1,5 трилиони американски долари[80] и имајќи го предвид постоењето на 7.000-30.000 TOR-страници, знаејќи каде да бараме, нашиот фокус потребно е да биде насочен на одредени области.

Во однос на пазарите, професионалците за национална безбедност треба да имаат свест во врска со недозволените добра и услуги на Темната мрежа кои би можеле да им наштетат на националните безбедносни интереси.

Следната табела е наш обид да ги „дестилираме” прашањата за националната безбедност од прашања кои не се однесуваат на националната безбедност:

Локација на интерес	Пазар	Форуми
Примери за национална безбедносна релевантност	✓ Пролиферација-Кинетичко оружје (пиштоли, пушки, експлозиви) ✓ Разузнавање-Информации (изнуда, класифицирани податоци)	✓ Регрутирање ✓ Комуникација ✓ Финансирање и оспособување ✓ Планирање ✓ Таргетирање

[80]Jona, Sam, (2018) "Cybercrime Revenue Estimated to Be $1.5 Trillion", *Deep Dot Web*, достапно на: ttps://www.deepdotweb.com/2018/05/05/cybercrime-revenue-estimated-to-be-1-5-trillion/.

	✓ Капацитети- хакирачки услуги (експлоатација, DDos услуги, изнајмување хакери итн. ✓ Материјали-документи за идентификација, украдени сметки итн.	
Други примери кои не се од национална безбедносна релевантност	• Дроги: фалсификувани легални дроги и недозволени дроги • Фалсификувани стоки: парични сметки, трговски карти, ниско-буџетна технологија, злато, лабораториски материјали, е-книги, брендирана облека. • Софтвер- лажни пакети, безбедносна заштита/малициозни средства • Лични информации- ингеренции на ниско ниво, кредитни/дебитни картички, банкарски сметки итн.	• Игри • Вести • Прашања/одговори • Покер/казино игри • Стоки и шопинг • Работни места

Табела 7[81]

Откако ќе ги разбереме локациите на интерес и видовите прашања на Темната мрежа, професионалците за национална безбедност потоа треба да ги разгледаат типовите на актери со кои веројатно ќе се сретнат.

[81] Jason Rivera and Wanda Archy (2019). The Role of the Dark Web in Future Cyber Wars to Come, *Small Wars Journal,* достапно на: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-come

Вид актер	Нација-држава	Држава - спонзор на криминалци	Тероризам	Внатрешни Закани	Хактивизам	Истражувачи спроведувачи на законот
Дефи ни-ција	Актер директно вработен од државата за да работи за нејзини интереси	Државата ги поддржува, но не се официјално вработени од неа	Актер што применува насилство за политички цели.	Актер со пристап до тајни податоци што ќе и наштети на спонзорира-ње на држава[82]	Актер кој презема акција против држава за политички цели[83]	Професионалци што имаат личност на Темната Мрежа заради истрага
Мотив и/ цели	Шпионажа Извидување	Финансиска добивка, изнуда, безбедносна комуникација	Регрутирање финасирање на безбедносна комуникација	Финсиска добивка одмазда его	Его социјални/ политички цели закана	-Безбедносна истрага, -спроведување на законот со одобение од државата за разузнавачки цели
Пр.	Кина Русија	Евгениј Богачев[84] „Темниот господар“[85]	ИСИС Ал-Каеда	Едвард Сноуден Џулијан Асанж	Анонимуси [86] Лулз Сек[87]	Владеење на правото, Агенти, воен персонал, разузнавачи

[82]What Is an Insider Threat? An Insider Threat Definition"(2018), *Digital Guardian*, достапно на: https://digitalguardian.com/blog/what-insider-threat-insider-threat-definition.
[83]Hacktivist | Definition of Hacktivist in English by Oxford Dictionaries", Oxford Dictionaries, достапно на: https://en.oxforddictionaries.com/definition/hacktivist.
[84] Богачев е наводниот Zeus Trojan и во моментов е баран од ФБИ Federal Bureau of Investigation, достапно на: https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev.)
[85] The Dark Overlord е финансиски водена личност која го изнудила здравствениот сектор и Нетфликс (Cox, Joseph (2018). "After Arrest In Serbia, Netflix Hackers 'The Dark Overlord' Say They're Still Going", *Motherboard,* достапно на: https://motherboard.vice.com/en_us/article/mbkex8/dark-overlord-arrest-serbia-netflix-hackers.)
[86] Anonymous е хактивистичка група со глобални операции насочени кон владите и корпорациите преку DDoS напади Geneva Sands (2016). "What To Know About The Worldwide Hacker Group 'Anonymous'", *ABC News*, достапно на: https://abcnews.go.com/US/worldwide-hacker-group-anonymous/ story?id=37761302.)
[87] LulzSec е хактивистичка група која сака да „привлече внимание“ и да ги „засрами сопствениците на веб-страниците“, Charles Arthur (2013). "Lulzsec: What They Did, Who They Were And How They Were Caught", *The Guardian*, достапно на: https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail.)

5.3. Примери на сајбер војување

5.3.1. Продажба на чувствителни документи за беспилотно летало

Видови прашања: пролиферација и разузнавање
Тип на актер: Внатрешна закана

Во 2018 година, безбедносните истражувачи во Recorded Future откриja продажен список на пазарот за информации на Темната мрежа за беспилотно летало MQ-9 Reaper што го користат американските воздухопловни сили.[88] Продавачот изјави дека очекува исплата за доверливи информации.[89] Беспилотното летало Reaper е широко користен воен капацитет на САД кој е распореден низ целиот свет како поддршка на историски и тековни операции за вонредни состојби. Покрај чувствителните документи за беспилотното летало Reaper, продавачот навел и неколку други документи, вклучувајќи прирачник за тенкот М1 Абрамс и тактики за поразување на импровизирани експлозивни направи (IEDs).[90]

Тимовите за воена реакција ќе ги утврдат точните последици од двете прекршувања. Сепак, фактот што еден хакер со умерени технички вештини можел да идентификува неколку ранливи воени цели и да ексфилтрира високо чувствителни информации за една недела е вознемирувачки преглед на тоа што може да постигне порешителна и организирана група со супериорни технички и финансиски ресурси.

[88]Barysevich, Andrei (2018). "Military Reaper Drone Documents Leaked on The Dark Web", *Recorded Future*, достапно на: https://www.recordedfuture.com/reaper-drone-documents-leaked/.
[89]Stolen Drone Files Sold on Dark Web"(2018). *BBC News*, достапно на: https://www.bbc.com/news/technology-44807091
[90]"Cybersecurity Incidents", U.S. Office Of Personnel Management, достапно на: https://www.opm.gov/cybersecurity/cybersecurity-incidents

5.3.2. Канцеларија за управување со персоналот на Соединетите Американски Држави

Тип на прашање: Разузнавање
Видови актери: нација-држава и криминалци спонзорирани од државата

Во 2015 година, ОПМ објави дека била жртва на прекршување на податоците што резултирало со кражба на приближно 21,5 милиони записи на лица кои аплицирале за безбедносен сертификат во САД.[91]

Информациите содржани во тие 21,5 милиони записи вклучуваат целосни имиња, датуми на раѓање, адреси на домот, броеви за социјално осигурување и „исто така досиеја за безбедносно одобрение што содржат опширни детали за пријателите, семејството, врските и финансиите за низа високо чувствителни владини работни места“.[92] Ова имплицира дека тој што ги украл податоците ефективно поседува не само список на американски лица, поседување безбедносен сертификат и организацијата за која работат или работеле, но и локацијата каде што живее секој од овие лица комбинирани со податоци кои потенцијално би можеле да се користат за олеснување на идните уцени (блиски семејни и лични контакти, криминални и финансиски досиеја итн.).

Овие податоци потоа биле предадени на сајбер-криминалци кои се обиделе да ги монетизираат украдените податоци на форумот на Темната мрежа наречен „Пекол“, каде што продавачот(ите) ги наведоа личните податоци за продажба, вклучувајќи ги броевите за социјално осигурување и личните односи на жртвите од повреда на податоците на ОПМ.[93]

[91]Stone, Jeff (2015), "The Dark Net Is Selling Hacked OPM Information, And It Could Be Worth $140M: Report", *International Business Times*, достапно на: https://www.ibtimes.com/dark-net-selling-hacked-opm-information-it-could-be-worth-140m-report-1989911.
[92]Ibid
[93]Stone, Jeff (2015) "The Dark Net Is Selling Hacked OPM Information, And It Could Be Worth $140M: Report", *International Business Times*, достапно на: https://www.ibtimes.com/dark-net-selling-hacked-opm-information-it-could-be-worth-140m-report-1989911.

5.3.3 Терористичка употреба на Темната мрежа за вклучување во финансирање и набавка на оружје

Тип на прашање: Капацитети

Тип на актер: Терорист

Во декември 2018 година, израелските власти поднесоа кривична пријава против поединец по име Ахмед Сарсур за неговиот обид да ја искористи Темната мрежа за да набави оружје и да обезбеди финансиска поддршка на терористите во Сирија.[94]

Според судските документи, дејствијата на Сарсур вклучувале обид за купување експлозиви, изнајмување снајперисти и обезбедување финансиска поддршка.[95] Дополнителните известувања на CNN покажуваат дека ова не е само изолиран инцидент, туку и појава што се повторува. Во септември 2018 година, CNN објави дека веб-страницата на TOR наречена „SadaqaCoins“ била отворена на Темната мрежа, со наведената цел на страницата да биде „да го поддржи Џихадот преку обезбедување безбедна платформа помеѓу финансиерите и организаторите на проектот“.[96]

[94] "Kafr Qasem Resident Indicted for Financing and Purchasing Weapons for Terrorist on Dark Web"(2018), *Deep Dot Web*, достапно на: https://www.deepdotweb.com/2018/12/01/kafr-qasem-resident-indicted-for-financing-and-purchasing-weapons-for-terrorist-on-dark-web

[95] Ibid

[96] "Crypto Crowdfunding Terrorists: Marketplace for Jihadist Crowdfunding Found on Dark Web" (2018), *CCN*, достапно на: https://www.ccn.com/crypto-crowdfunding-terrorists-marketplace-for-jihadist-crowdfunding-found-on-dark-web/.

5.3.4. Зеро-ден експлоатирање

Тип на прашање: Пролиферација
Тип на актер: Сите

Од гледна точка на националната безбедност, неконтролираното ширење на експлоатирањата во зеро-ден предизвикува многу загриженост, бидејќи овие способности историски покажаа дека значително влијаат на аренатa за национална безбедност. Stuxnet, наводна американско-израелска можност за малициозен софтвер дизајниран да ги попречи иранските центрифуги за збогатување ураниум во Натанц,[97] е можеби најпознатиот пример за тоа како зеро-денови може значително да влијаат на националните безбедносни интереси на националните држави.

Според повеќето проценки на националната безбедносна истражувачка заедница, Stuxnet потенцијално ја одложи иранската нуклеарна програма за неколку години,[98] што го демонстрираше потенцијалот за национална безбедност на нулта-дневните експлоатации.

Од откривањето на Stuxnet, сајбер-криминалците со желба да заработат, преку нивната способност да развијат експлоатирања во информатичката технологија, особено нулта-дневна експлоатација, силно ги користат пазарите на Темната мрежа за да најдат потенцијални купувачи за нивните способности.

[97]Zetter, Kim. "An Unprecedented Look at Stuxnet (2014), The World's First Digital Weapon", *WIRED*, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[98]Warrick, Joby. (2011). “Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack”, *Washington Post*, достапно на: http://www.washingtonpost.com/wpdyn/content/article/2011/02/15/AR2011021505395.html?noredirect=on.

5.3.5. Напад на колонијалниот нафтовод

На 7-ми Мај 2021 година, еден од најразорните сајбер-напади на инфраструктурата беше нападот на Колонијален нафтовод во САД. Најголемиот гасовод во САД и оној што снабдуваше повеќе од 45% од гасот, дизелот и авионското гориво на источниот брег беше принуден целосно да ги затвори своите мрежи и операции. Иако успеаја да ја вратат функцијата на системот, до 18-ти мај, речиси 11.000 бензински пумпи сè уште беа без бензин. Хакерската група Dark Side, исто така, украла повеќе од 100 GB податоци од серверите на компанијата пред нападот и ја предала контролата дури откако Colonial платила 5 милиони долари во криптовалута.[99] Уште позначајно, просечната цена во САД за гас по галон се зголеми на национално ниво до највисоката цена во последните шест години. Векторот за напад сè уште е засега непознат.[100]

[99] William Turton, Michael Riley, Jennifer Jacobs. (2021). "Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom", *Bloomberg*.
[100] Analysis of top 11 cyber attacks on critical infrastructure (2021), достапно на: https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/

6. Нови трендови на закани за националната безбедност

Многу е веројатно дека постојат категории на закани од Темната мрежа и можни трендови што не се опфатени. Свесни сме дека пејзажот на заканата може да се смени, бидејќи новите технологии како што се квантното пресметување, дигиталната валута и 3-Д печатењето продолжуваат да се развиваат. Во продолжение ќе прикажеме кои се заканите по националната безбедност што се развиени на Темната мрежа:

Закани по националната безбедност развиени на темната мрежа		
Пролиферација	*Разузнавање*	*Капацитет*
-Ширење на кинетичко и дигитално оружје -национална безбедносна технологија	-разузнавачки информации изворни операции и изнуда -онлајн операции	-обезбедување услуги за материјали за промовирање на целите на противникот
-Оружје/експлозиви -сајбер експлоатации -Оружје за масовно уништување -класифицирани технологии	-изворни операции -внатрешни закани -контраразузнавање -изнуда -разузнавачки колекции	-поддршка на тероризмот -фалсификување на идентитет -перење пари -атентати -хакирање како услуга

Табела 9[101]

[101] Jason Rivera and Wanda Archy (2019). The Role of the Dark Web in Future Cyber Wars to Come, *Small Wars Journal,* достапно на: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-come

6.1 Пролиферација - кинетичко оружје

Анонимноста олеснета преку Темната мрежа поттикнува идеално тргување за потенцијалните купувачи и продавачи на опасно оружје. Ова е повеќе од само теоретско - тоа е факт што се докажува преку набљудување. Ураниум, опасни хемиски соединенија, огнено оружје од воена класа А, ова се примероци од типовите оружја што се наведени на темната мрежа. Како одговор на ова, глобалната заедница за спроведување на законот агресивно бараше купувачи и продавачи на оружје да бидат на Темната мрежа - и во многу случаи тие беа успешни во спречување на потенцијални напади. Во 2016 година, американското Федерално биро за истраги (ФБИ) соработуваше со ирските органи за спроведување на законот за да спречи милитант на Ирската републичка армија (ИРА) да набавува пиштоли, гранати и пластични експлозиви од пазарот на Темната мрежа.[102]

И додека заедницата за национална безбедност може да извојува помали победи со овие типови на превентивни операции, заинтересираните за анонимно купување и продавање на кинетичко оружје почнаа да ја менуваат својата методологија. Во текот на следните години, се проценува дека ќе има две големи еволуции на начините на тргување со кинетичко оружје на Темната мрежа.

Првиот е дека купувачите и продавачите на оружје на темната мрежа најверојатно ќе го преселат својот бизнис подалеку од некои од попопуларните пазари со отворен пристап (како што е Dream Market) и ќе преминат на други пазари за кои е потребен повисок степен на проверка за да влезат (како на пр. Демонски форум и форуми за корисници на ОГ). Ова најверојатно ќе се случи поради две основни причини. Првата е дека поединците кои се занимаваат со трговија со оружје стануваат сè повнимателни од тајното присуство на органите за спроведување на законот и можноста тие да бидат намамени во стапица.

[102]"Taking Stock of the Online Drugs Trade" (2016), RAND Corporation, достапно на: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.

Втората е дека главните пазари веројатно стануваат помалку толерантни кон ризикот што го прават со тоа што дозволуваат огласи за оружје на нивните пазари. Списоците за оружје историски го привлекуваат вниманието на глобалната заедница за спроведување на законот, што резултираше со тајни службеници кои ги разгледуваат пазарите во потрага по потенцијални информации. Надвор од зголемениот ризик, профитната маржа на пазарот за трговијата со оружје е релативно ниска во споредба со профитните маржи на други нелегални стоки со голем обем, како што се дрогата и измамата. Според две студии спроведени од RAND, глобалната продажба на дрога на Темната мрежа се проценува на помеѓу 12 и 21,1 милиони долари месечно во 2016 година,[103] додека глобалната трговија со оружје изнесувала 80 илјади долари месечно во 2017 година.

Втората голема еволуција што веројатно ќе се забележи е преминот од тргување и испраќање опипливо физичко оружје кон дигитална трговија и размена на информации за оружјето. Новите технологии како 3-Д печатењето овозможуваат да се продаваат шеми и инструкции за склопување преку интернет, дозволувајќи им на купувачот и на продавачот да го избегнат ризикот од физичко испраќање на компонентите на оружјето преку товарна пошта.

До неодамна, во Соединетите Американски Држави беше незаконски за развивачите на шеми за оружје за печатење 3-Д да го дистрибуираат својот производ онлајн поради прекршување на регулативите за меѓународниот сообраќај со оружје (ИТАР). Меѓутоа, во јуни 2018 година, Врховниот суд на САД пресуди во корист на компанијата наречена Wilson and Defense Distributed, дозволувајќи им да „објавуваат планови, датотеки и 3-Д цртежи во која било форма и ги ослободува од ограничувањата за извозот“.[104]

Оваа пресуда, не само што ќе ги поттикне претприемачите со 3-Д оружје да го шират својот бизнис на глобално ниво, туку и ќе им олесни на купувачите и продавачите на оружје да тргуваат со оружје, истовремено намалувајќи го ризикот

[103]“International arms trade on the dark web” (2017), RAND Corporation, достапно на: https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html.
[104] Williams, David. (2018)"Americans Will Soon Be Able to Legally Download 3-D Printed Guns", *CNN* https://www.cnn.com/2018/07/19/us/3d-printed-gun-settlement-trnd/index.html.

од откривање од страна на глобалните органи за спроведување на законот. И како и другите недозволени пазари, Темната мрежа најверојатно ќе биде примарен излез за тргување со шеми за 3-Д оружје.

6.2 Пролиферација - сајбер експлоатации

Пред појавата на Темната мрежа, високо ефективни сајбер-експлоатации беа достапни само за напредните влади на националните држави, организирани криминални групи и тесно поврзани истражувачки заедници. Ова повеќе не е случај, бидејќи ефективните сајбер-експлоатации сега во голема мера се монетизираат и се дистрибуираат низ десетици пазари и форуми на Темната мрежа. Ова покренува прашања од гледна точка на националната безбедност, бидејќи им овозможува на актерите кои претходно не поседувале техничка моќ едноставно да ги купат своите посакувани капацитети. Во продолжение се прикажани некои од тековните и идните импликации од широко распространетата пролиферација на експлоатирања на Темната мрежа:

- **Препакување на експлоатите на националните држави:** развивачите и дистрибутерите на малициозен софтвер на Темната мрежа ќе продолжат да ги пакуваат и пренаменуваат експлоатирањата што ги користат националните држави. Постојат неколку причини поради кои овие подвизи ќе продолжат да се зголемуваат во популарност - првата е тоа што тие се испробани и вистински способности кои беа успешно искористени од најнапредните национални држави во светот. Втората е дека постои психолошка привлечност за прикачување на изјавата за брендирање „користена од нацијата-држава“ како дел од маркетиншкиот трик што го користат продавачите на овие експлоатирања.

- **Зголемен пристап до националните држави и недржавните групи:** Помалку развиените национални држави-агресори, како што се Северна Кореја или Иран, кои историски немаа пристап до моќни сајбер-експлоатации, сега имаат поголем степен на пристап до напредни

капацитети. Слично на тоа, групите актери кои обично немаа пристап до напредни технологии, како што се терористичките организации, сега можат едноставно да ја купат посакуваната способност.

- **Експоненцијално ширење на знаењето:** додека актерите работеа во затворени силоси, раширената пролиферација на капацитети преку Темната мрежа им овозможува на експлоататорите да го искористат сопственото техничко разбирање на експлоатирањата за да направат сајбер-експлоатирања што се потајни и поопасни од претходните.

- **Зголемените профитни маржи се еднакви на зголемен поттик за развој на експлоатации:** во 2014 година беше утврдено дека сајбер црниот пазар е попрофитабилен од глобалната трговија со дрога.[105] Вкупната глобална цена на компјутерскиот криминал во 2017 година изнесуваше до 600 милијарди долари[106], тренд кој продолжи да ги поттикнува програмерите да создаваат експлоатирања за продажба на Темната мрежа.

6.3 Разузнавање - изворни операции, закани од внатре и изнудување

Во следните години, Темната мрежа ќе биде сè повеќе користена за операции со извори на разузнавачки информации, активности за инсајдерски закани и изнудување.

Постојат две основни причини за ова - првата е инхерентниот дизајн на Темната мрежа и неговата способност да ја олесни двонасочната анонимност. Втората причина е зголемениот број на податоци достапни на Темната мрежа кои можат да ги користат разузнавачите за изнуда или за принудување извори.

[105]Callahan, Michael (2014) "Hackonomics: A First-of-Its-Kind Economic Analysis of the Cyber Black Markets," *Juniper Networks*, достапно на: https://forums.juniper.net/t5/Security/Hackonomics-A-First-of-Its-Kind-Economic-Analysis-of-the-Cyber/ba-p/234262.
[106]Lau, Lynette. (2018) "Cybercrime 'pandemic' may have cost the world $600 billion last year", *CNBC*, достапно на: https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html.

Во однос на зголемената анонимност, средбата практично под маската на анонимна личност овозможува повисок степен на безбедност и за разузнавачите и за нивните извори. Изворна средба и меѓу разузнавачот и тајниот извор е значителен ризик за двете страни - особено за изворот. Во 2017 година, „Њујорк тајмс“ објави дека кинеската влада или убила или затворила помеѓу 18-20 извори на ЦИА во периодот од 2010 до 2012 година.[107] Тоа е во просек од речиси 10 луѓе годишно – и тоа е само за операциите на ЦИА во Кина. Колку голема веројатност ќе биде оваа бројка кога ќе се земе предвид не само ЦИА, туку и сите тајни разузнавачки служби кои работат низ сите земји, низ повеќето нации во светот. Поради оваа причина, разузнавачките служби веројатно сè повеќе ќе бараат потенцијални информации и ќе исполнат можности користејќи ја Темната мрежа со цел да постигнат повисок степен на безбедност.

Втората причина поради која Темната мрежа најверојатно ќе биде интересна за разузнавачите е зголемената количина на достапни податоци што разузнавачите можат да ги користат за да изнудат потенцијални извори за информации. Со комбинирање на информациите добиени од нарушувањата на сајбер-безбедноста што се случуваат на редовна основа и со спојување на истите со други информации што може да се користат за изнудување поединец, професионалецот за национална безбедност може да биде сведок на бран претстојни обиди за изнуда. Што ако организацијата за собирање разузнавачки податоци поседува две збирки податоци: една база на податоци што ги содржи информациите украдени од прекршувањето на ОПМ на американската влада и друга база на податоци вклучува идентитети на поединци кои биле компромитирани. Повикувајќи се на овие две збирки податоци, организацијата за собирање разузнавачки информации би можела да извлече листа на поединци кои се на позиции за национална безбедност, да ги одреди видовите информации до кои може да имаат пристап врз основа на нивната историја на вработување, а потоа да ги уценува избраните поединци да се откажат од информациите за Темната мрежа.

[107]Mazzetti, Mark; et al. (2017) "Killing C.I.A. Informants, China Crippled U.S. Spying Operations", *The New York Time*, достапно на: https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html.

6.4 Тероризам

Како што глобалниот конфликт помеѓу слободното општество и тероризмот трае до 21 век, терористите продолжуваат да ги приспособуваат своите методологии како одговор на промените во тактиките за национална безбедност и еволуцијата на технологијата. Во овој момент општо е познато дека НАТО и неговите сојузници ја поседуваат технолошката предност да можат да следат што би се сметале за „отворени“ комуникации (на пример, телефонски комуникации, радио, површинска мрежа итн.).

Терористичките организации, исто така, почнаа да го сфаќаат ова и ги префрлаат своите техники за комуникација на технолошки средства кои обезбедуваат повисоки степени на анонимност, како што е употребата на TOR.[108] Покрај префрлањето на техниките за комуникација на анонимни средства, професионалците за национална безбедност, исто така треба да разберат како терористичките организации ќе ја користат Темната мрежа за да ги постигнат своите насилни и политички цели. Во иднина, веродостојно е дека терористите ќе ги користат пазарите на Темната мрежа за да купуваат материјали што овозможуваат да помогнат во извршувањето на нивните цели.

Покрај оружјето и финансирањето, овозможувањето материјали како што се фалсификувани идентификации, комуникациски уреди што не се припишуваат и фалсификувани документи може да послужат за олеснување на целите на терористичката организација преку поттикнување на способноста за патување, водење безбедна комуникација, утврдување доказ за престој итн. е особено загрижувачко кога размислуваме за импликациите за тоа како потенцијален терорист би можел да ги искористи овие материјали што овозможуваат да усвои псевдоличност со цел да избегне откривање од властите. Во просторот за списоци со фалсификувани документи на повеќето пазари, може да се најдат различни

[108]Weise, Elizabeth (2017). “Terrorists use the Dark Web to hide,” *USA Today*, 2017, достапно на: https://www.usatoday.com/story/tech/news/2017/03/27/terrorists-use-dark-web-hide-london-whatsapp-encryption/99698672/.

фалсификувани документи кои вклучуваат фалсификат на: пасоши, возачки дозволи, сметки за комунални услуги, даночни формулари, зелени картони итн.

Во некои случаи, продавачите на Темната мрежа покажаа способност да се продаваат легитимни документи за идентификација наспроти фалсификуваните. Во 2017 година, поединец кој можеби е на списокот за следење терористи се обидел да добие легитимен пасош од Темна мрежа од продавач на фалсификувани идентификации. Овој продавач тврди дека продава вистински пасоши од европските земји што може да ги набави преку неговата наводна поврзаност со „корумпирани поединци“ во агенциите за издавање пасоши на овие европски земји. Во онлајн разговор помеѓу продавачот и потенцијалниот купувач, продавачот силно го одби барањето за купување, наведувајќи дека верувал дека потенцијалниот купувач бил на списокот за следење.[109]

6.5 Малициозни услуги за изнајмување

Темната мрежа е дом на разновидни различни малициозни услуги кои би можеле да ги користат потенцијалните актери кои сакаат да предизвикаат штета. Како и другите аспекти на Темната мрежа, одвојувањето на бучавата и стеснувањето на нашиот фокус е од клучно значење за разбирање на природата на заканата.

Следната табела илустрира малициозни услуги пронајдени на темната мрежа и ги дели тие услуги на национална безбедност и ненационална безбедносна релевантност:

[109]Conversation between Dark Web vendor and an individual potentially affiliated with terrorism"(2018), Complaints Board, достапно на: https://www.complaintsboard.com/complaints/fake-id-passports-fake-id-passports-c735014.html?page=2#comments/.

Примери за услуги со национална безбедосна релевантност	Примери за услуги на Темна мрежа со ненационална безбедосна релевантност
- Хакрирање како услуга - Социјален инженеринг како услуга - Атентати - Трговија со луѓе - Киднапирање - Фалсификување идентитет - Фалсификување имот - Перење пари	- Следачи на социјални медиуми - Готовинска исплата - Зголемена трговија на интернет - Стоки на попуст - Продажба на кредитни/дебитни картички - Откривање идентитет

Табела 10[110]

Како што е наведено претходно, развивање и извршување на напредни сајбер технологии повеќе не е потребно за актерите да извршуваат софистицирани напади. Како и малициозниот софтвер што е наменет и продаден на Темна мрежа за профит, актерите сега можат да купуваат малициозни услуги за изнајмување преку продавниците на Темната мрежа. До овие места може да се пристапи преку TOR и се расфрлани на различни локации низ криминалното подземје.

Малициозните услуги за изнајмување им овозможуваат на групите актери со релативно ниско ниво на сајбер способности во суштина да го трасираат својот пат кон остварувањето на нивните цели. Оваа можност може потенцијално да објасни како Северна Кореја можеше да ја забрза зрелоста на својата програма за сајбер-војна во последните неколку години. Пред нападот на Sony Pictures во 2014 година, Северна Кореја не се сметаше за голема сајбер супер сила. Оттогаш, серија високо софистицирани напади и се припишуваат на севернокорејската влада, вклучително

[110] Jason Rivera and Wanda Archy (2019). The Role of the Dark Web in Future Cyber Wars to Come, *Small Wars Journal,* достапно на: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-come.

и Wannacry Ransomware Attack, SWIFT Network Bank Heist, напади на криптовалути од висок профил и различни други сложени напади.[111]

Во претходните години, пред 2014 година била манифестирана мала способност за да подоцна стане една од најистакнатите сајбер-закани во светот, постои голема можност дека малициозните услуги за изнајмување одиграле значајна улога во зголемувањето на сајбер способностите на Северна Кореја. Во иднина, проценуваме дека другите државни и недржавни групи актери кои сакаат да ги забрзаат своите способности за сајбер војување, на крајот може да се свртат кон Темната мрежа за да ги добијат саканите услуги.

[111]North Korea's APT 38 hacking group behind bank heists of over $100 million", (2018) ZD-Net, достапно на: https://www.zdnet.com/article/north-korea-s-apt38-hacking-group-behind-bank-heists-of-over-100-million/.

7. Меѓународно-правни аспекти на сајбер војувањето

Специфичната природа на сајбер просторот, неговата специфична структура и нематеријалност, го прават комплексен за обезбедување. Со регулирањето на конфликтите меѓу државите примарно се занимава меѓународното право за вооружени конфликти. Секој конфликт, општо, ги има следните клучни елементи: учесници и нивни мотиви, средства и методи на војување. Бидејќи мотивите на сите меѓународни конфликти примарно зависат од политичката волја, конечната цел на секој учесник во конфликтите е иста, без оглед на опкружувањето каде што конфликтот се одвива: да се потчини состојбата и однесувањето на противникот по своја волја".[112]

Тргнувајќи од поимната определба и јазичниот метод на толкување како примарен за правната наука, современите речници терминот „сајбер" го дефинираат како: „во врска со, или карактеристика на културата на компјутери, информатичката технологија, и виртуелната реалност: сајбер ера" (Оксфорд речници онлајн речник), или како „на, во врска со, или оние кои вклучуваат компјутери или компјутерски мрежи (како интернет)" (Merriam-Webster, онлајн речник). Во македонскиот јазик се користи терминот „сајбер" како интернационализам. Многу често како заменски се употребува терминот „компјутерски", но истиот не ја отсликува доволно комплексноста на темата - бидејќи „сајбер" во целокупната смисла е многу повеќе од „компјутери". Често се наметнува дилемата дали е тоа посебна петта димензија на војувањето или нова димензија на постоечките четири, а таквата аналогија е применлива соодветно и во другите сфери на човечкото живеење и делување.

Во поглед на видовите средства, учесниците и методите со кои се водат конфликтите, разликата меѓу традиционалните и сајбер конфликтите е суштинска. Причината за таа разлика е примарно од технолошка природа, додека нејзините последици примарно се од правна и организациона природа. Во поглед на

[112]Carl von Clausewitz, On War, trans. J.J. Graham (London, UK: Nicholas Trubner, 1873), Book I, Chapter 1, para 2, http://www.gutenberg.org/files/1946/1946-h/1946-h.htm#link2HCH0001

Меѓународното право на вооружените судири, последици се отежнато откривање на агресијата, сторителите и утврдување на околности неопходни за одредување дали е агресија во надлежност на меѓународното право. Причината за ова е природата на применетите технологии, средини и односи на учесниците.

Во сајбер просторот се извршуваат низа незаконски активности: од кражба на податоци и финансиски малверзации по електронски пат, до оневозможување на услуги, шпионажа, загрозување на критичната инфраструктура и директен напад на нуклеарна програма - дијапазонот е навистина широк. Токму затоа е многу тешко да се дадат конкретни и специфични правни одговори, кои би ги задоволиле барањата на различните предизвици.

Структурата на сајбер просторот, а посебно природата на интернетот е спротивна на потребата да биде контролирана. Првото клучно правно прашање би било: чија е јурисдикцијата? Одговорот на тоа прашање во себе ги крие одговорите за правната рамка и импликациите за акција. Но како би можел сајбер просторот да потпадне под чија било јурисдикција? Евентуално може да се зборува за јурисдикција врз инфраструктурата која го овозможува постоењето на сајбер просторот, но во суштина, тој не е фиксна категорија. Светот составен од битови и бајтови, не може да се измери, лоцира и алоцира во класичното значење на поимите. Од друга страна, сајбер просторот е место каде што најмногу „се кршат копјата“ во судир помеѓу барањата за безбедност и приватност, а човековите права концептуално се на удар. Во отсутство на консензуален правен одговор, останува да се постигне максимална апликабилност на постоечките правни режими во зависност од конкретната ситуација, односно да се врши посебна анализа за поедничените случаи. Дополнително од различните фактички ситуации кои бараат различни апликабилни правни режими треба да се земат предвид различните пристапи кон сајбер културата и културниот релативитет како таков, зависноста на едно конкретно општество од сајбер просторот, неговата резилиентност кон

заканите, намерата на потенцијалните напаѓачи, како и ефектите и последиците измерени во конкретна штета од евентуален напад.[113]

Вокабуларот кој се употребува во овој домен, исто така, не е унифициран, што остава дополнителен простор за толкување.

Најчесто употребуваните може да се класифицираат во неколку категории:

а) Сајбер-напад, термин кој покрива широк спектар на активности со различен карактер и цел, дури и активности кои би можеле да го активираат членот 5 од Договорот од Вашингтон, односно да испровоцираат воен одговор во смисла на колективна самоодбрана на земјите членки на НАТО.[114]

б) Сајбер-војна или „наменска употреба на компјутерски системи со цел да се прекинат активностите на непријателска земја или напад на нејзините комуникациски системи“[115]. За да се утврди состојба на сајбер-војна, мора да има атрибуција (припишливост) на дејствијата кон владини агенти или државни органи.

в) Сајбер војување (warfare) претставува хибриден термин кој има за цел да опфати поширок спектар на агресивни дејствија. За разлика од војната или кривичните дела, терминот „војување“ не претставува правна категорија. Токму затоа и е често употребуван – опфаќа поширок спектар на дејствија, особено во контекст на современите хибридни и асиметрични безбедносни закани, кои често се наоаѓаат во меѓупросторот на криминалот и војната. Контекстот во кој се употребува најчесто вклучува држава или сојуз на држави како субјект и/или како барем една страна. Иако поограничен, како синоним се употребува и терминот електронско војување, кој Талинскиот прирачник го дефинира како „Употреба на електромагнетните полиња (ЕМ) или насочена енергија за искористување на електромагнетниот спектар. Тоа може да вклучува пресретнување или

[113] Весна Поповска (2016). Правни аспекти на сајбер безбедноста, год. 6, бр.6, *Годишен зборник*, Универзитет Гоце Делчев, Штип.
[114] Достапно на http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/
[115] Достапно на https://www.newamerica.org/cyber-global/compilation-of-existingcybersecurity-and-information-security-related-definitions/

идентификација на емисиите, вклучување на енергија, спречување на непријателската употреба на ЕМ спектар од една спротивна страна, како и активности за да се обезбеди ефикасно вклучување на ЕМ спектар од страна на државата корисник“.

На пример, дигиталните технологии дозволуваат неограничено дуплирање на податоци; софтверот инхерентно содржи недостатоци коишто можат да бидат злоупотребени за да се загрози безбедноста на системот; истите средства и методи на изведба на сајбер-нападите се користат и од поединци и од држави, во мир и во војна. Ова не е типично за употребата на сила во физичката средина во која се организира, применува и при манифестација на забележлива воена сила поради спектакуларните ефекти од дејството на системите за воено оружје, како и поради развој на технологија за нивно откривање и следење. Традиционалното право за вооружени конфликти е систем кој има за цел да ги регулира меѓународните вооружени конфликти, да се обезбеди мир и да се намалат жртвите и уништувањата за време на конфликтот.

Вооружените конфликти постојано развиваат технологии и нови форми на војување. Традиционалното право со тек на време мора да е еластично во интерпретација за да може да ги опфати сите нови ситуации што ги носи новата технологија, а тоа доведува до нееднаква примена на принципите, нормите и прописите. Ситемот на меѓународното право мора да обезбеди мир и да ги намали последиците од примена на вооружена сила и конфликти насекаде во светот, и во секој момент, на ефикасен начин, инаку неговата цел не може да биде исполнета.

Имајќи ја предвид примената на правото во сајбер конфликтите, во правен и политички поглед, би било поприфатливо решението за сајбер право[116], со преземање на прифатливи и практично применливи концепти на меѓународното право, но и другите гранки на правото. Конфликтите во сајбер просторот се случуваат во услови на војна, но и во состојба на мир и затоа е потребна

[116]Mirjana Drakulić, Ratimir Drakulić, (2010) Evropska perspektiva regulisanja Internet usluga: izazov tradicionalnom evropskom pravu “, *Telekomunikacije*, no. 6

комбинација од примена на разни практични концепти и пристапи за регулирање на конфликтите во сајбер просторот.

Во случај на интеграција и вклучување на различни принципи и системи кои имаат поинакви извори, во ново сајбер право, можно е да се дојде до нов пристап што претставува поволно и ефикасно решение што е лесно остварливо и поприфатливо за поширок круг меѓународни актери. Со неговото воведување не се нарушуваат постоечките концепти на традиционалното право, туку тие се поефикасни во соодветниот, конзистентен и практично применлив модел.[117]

Таквиот пристап бара нов комплексен, мултидисциплинарен и интердисциплинарен пристап што ги почитува сите специфичности на сајбер просторот и појавите во него. На тој начин, формата и содржината на правото се приспособуваат на реалните проблеми и феномени во сајбер просторот што тоа право го регулира, при што се одбегнува потребата од бавно променливиот традиционален правен систем кој формално се приспособува на новите појави во реалниот свет. Таквиот пристап може да биде од посебна корист во областите во кои се среќаваат динамични промени во односите и состојбите, како примената на компјутерските науки и информатичко-комуникациската технологија во конфликтите во сајбер просторот.

Сепак, развојот на кој било нов систем на меѓународното право е бавен, бидејќи за неговиот развој и усвојување е потребно долго и бавно усогласување со консензус меѓу бројните заинтересирани страни со различни интереси. Затоа решението треба да се бара во постоечките области на правото. Правен инструмент за ова одамна постои во Виенската конвенција за договорно право.[118]

Практичната примена овозможува на правото висок степен на прифаќање од страна на основните носители на суверената власт во меѓународните односи, а тоа се државите. При тоа се можни различни степени и концепти на остварување на

[117]Drakulic, Mirjana (1996). "*Osnovi kompjuterskog prava*." Drustvo operacionih istrazivača Jugoslovije, DOPIS, Belgrade.
[118]Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, 8 I.L.M. 679.

соработка. Тие опфаќаат различни нивоа и пристапи: национални, меѓународни односно саморегулација.

Во поглед на сајбер војувањето и сајбер-војните, значајно е изготвувањето на Талинскиот прирачник за меѓународно право релевантен при сајбер војување,[119] изготвен од група на експерти, со намера да обезбеди одговори и кодификација.[120] Во принцип, се сведува на поделба на режимите и апликабилност на jus ad bellum и jus in bello, односно на „правото да се оди во војна“ и правото кое е апликабилно во војна, навраќајќи се на општите принципи на меѓународното право.

Во отсуство на прецизна правна рамка и реално тешко постиглив консензус околу истата, клучните актери се фокусираат многу повеќе на развој на „политики“ (policy) како modus operandi за делување и реакција. Зголемена посветеност на политиката може да се види во завршните согледувања од самитот во Букурешт во 2008 година, во која НАТО членките ги истакнаа своите заложби за усвојување на политики за сајбер одбрана, во смисла на „потреба на НАТО и земјите да ги заштитат клучните информациски системи; да споделат најдобри практики; и за да се обезбеди способност да им помогне на земјите сојузнички, на барање, да се спротивстават на сајбер-напад”.[121] НАТО ја постави сајбер одбраната како клучен приоритет во својот нов стратешки концепт од 2010 година[122] и продолжи со континуираните залагања за интегрална сајбер одбрана.[123]

При тоа од клучна важност е пристапот на изградба на заеднички систем на договори и поклопување на интересите на клучните страни. За да меѓународното право биде ефикасно и применливо, нужно е да биде прифатено за широк круг на држави.

---

[119] Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). Cambridge University Press.
[120] Прирачникот е достапен на https://ccdcoe.org/tallinn-manual.html
[121] NATO. (2008). Bucharest Summit Declaration para. 47 (Apr. 3).
[122] NATO. (2010). Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, достапно на: http://www.nato.int/nato_static/assets/pdf/pdf_publications/ 20120214_strategic-concept-2010-eng. p.
[123] Достапно на http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

7.1. Утврдување на одговорност кај државите за сајбер-напад

За регулирање на сајбер војувањето, клучно е прашањето за можноста за идентификување на напаѓачите и утврдување на одговорност на државите за сајбер-напад. Според правото за вооружени конфликти, се подразбира дека во состојба на конфликти се субјектите на меѓународното право,[124] но тоа е многу тешко да се процени.

Во овој дел, на сајбер просторот му недостигаат кохерентни, договорни и обичајни правни правила. Креирањето на мултилатерални договори согласно со Виенската конвенција за договорно право е сложен процес, но пред сè клучниот проблем лежи во специфичноста на сајбер просторот и неподобноста за негово регулирање, како и физичките тешкотии - во смисла на сопственост врз инфраструктурата, на пример.

Сајбер-нападите можат да покренат поединци од територија на трета држава, а тие можат да имаат одложено дејство, можат да бидат пренасочени на сервери на други држави и можат да бидат покренати од повеќе различни позиции. Затоа, за утврдување на потеклото на нападот, покрај сајбер форензика, потребно е да се применат и други меѓународно прифатливи методи на докажување на одговорност на некои држави.

До неодамана, во светот преовладувало мислењето дека меѓународното право е засновано на односите меѓу државите со исти права.[125] Во тој дух, самоодбраната е средство што овозможува на една држава самата да се заштити од вооружен напад на друга држава, додека насилството што го преземаат недржавни субјекти кон некоја држава, нејзините граѓани или имот е во надлежност на кривичното право.[126]

---

[124]III Хашка конвенција о започињању непријатељстава из 1907. године, http://www.icrc.org/ihl.nsf/FULL/190

[125]Michael N. Schmitt, (2007) 21st Century Conflict: Can the Law Survive? “, 8(2) Melbourn Journal of International Law 24, достапно на: http://www.austlii.edu.au/au/journals/MelbJIL/2007/24.html

[126] Antonio Cassese, (2001) “Terrorism Is Also Disrupting Some Crucial Legal Categories of International Law”, *European Journal of International Law*, Vol 12, No.5, стр. 993–1001, достапно на: https://www.unodc.org/tldb/bibliography/Biblio_Internat_law_Cassese_2001.pdf

Но, иако со тоа правило се ограничува можноста за терористички активности со одобрение или знаење на државните орган, во духот на современите безбедносни предизвици и технолошки развој, посебно во областа на сајбер војувањето, се јавува потребата од редефинирање на постоечката интерпретација на употреба на сила во меѓународните односи, посебно во случаите на нарушување на државниот суверенитет. Транснационалните активности на државите во сајбер просторот што се однесуваат на внатрешните работи лесно може да предизвикаат кршење на меѓународно правните принципи на почитување на суверенитетот на државите и немешање во внатрешните работи.[127]

Бидејќи природата на сајбер-нападот е специфична, докажувањето на одговорност на државите е сложен проблем. Иако секој сајбер-напад што го покренала некоја држава морал да подлежи на правни последици што произлегуваат од чл. 4 од Повелбата на ОН[128], доколку по природата и интензитетот достигне ниво на напад. Таа околност ја отежнува примената на постоечкото меѓународно право и подрачјето на сајбер војувањето останува нерегулирано, па единствен можен пат во иднина е создавање на специфични меѓународни прописи со кои ќе се дефинираат елементите на сајбер војувањето и принципите на државната одгоровност.

Регулирањето на сајбер војувањето и создавањето нови правила бараат и највлијателните фактори на меѓународната заедница. Според тоа, неопходно е тие прописи да бидат усогласени со постоечкото меѓународно право, а општите правни претпоставки за владеење во текот на сајбер војувањето можат да се изведат од досегашната меѓународна пракса во слични ситуации.

За утврдување на врската меѓу државите и поединците во текот на конфликтот во праксата постојат два карактеристични случаи, врз чија основа настанаа стандардите за проценка на степенот на умешност на државите во некој

[127]Декларација о принципима у међународном праву из 1970. године, (http://daccessdds.un.org/doc/RESOLUTION/GEN/NR0/348/90/IMG/NR034890.pdf?OpenElement
[128]Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), International Court of Justice, достапно на: http://www.icj-cij.org/docket/index.php?p1=3&k=f4&p3=4&case=91

конфликт. Тоа се начела на целосна контрола и начело на ефективна контрола.[129] Тест „целосна контрола“, според одредбите на чл.4 од Нацрт правилата за одговорност на државите за меѓународно противправните дела претставува главна околност за утврдување одговорност на некоја држава е дејствувањето на нејзините формални органи.

Но, во пракса ретко се случува некоја држава отворено противправно да дејствува во конфликт така што користи свои официјални органи. Во тие прилики обично станува збор за неформални сили под контрола на државите, како што се платени или паравоени сили.[130] Таква ситуација е веројатна и во сајбер војувањето во кое, поради можноста за прикривање на вистинскиот напаѓач, очекува ангажирање неформални, националистички или политички група или приватни компании.

Ако државата основала група, суштински е да ја контролира, одбрала и поставила водач и ги насочила активностите и ако припадниците на групата сториле недозволени дела, тогаш во комбинација со принципот на командна одговорност, таа држава, одговорна за последиците од нападот што ја преземала таа група, дури и доколку државното раководство немало намера да ги предизвика тие последици, ниту сознанието за постоење на намерата.

Тој стандард се однесува на одговорност на државите за сопствените органи или некоја група се поистоветува со државата во поглед на последиците од дејствувањето. Примената на тој принцип ја зголемува веројатноста за утврдување државна одговорност во случај на сајбер војување, но со тоа не се решаваат сите проблеми, затоа што организирањето на борбените групи суштински се разликува од ангажирање на сајбер напаѓачи.

---

[129]Antonio Cassese (2007) The Nicaraqua and Tadić Test Revisited in light of the ICJ Judgment on Genocide in Bosnia (2010), *The European Journal of International Law,* Vol. 18 no. 4, достапно на: www.ejil.org/pdfs/18/4/233.pdf. Scott J. Shackelford, “State Responsibility for Cyber Attacks: Competing Standards for A Growing Problem”; Derek Jinks (2003) „State Responsibility for the Acts of Private Armed Groups “, *Chicago Journal of International Law*, Vol. 4, достапно на: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=391641

[130] James Risen, Mark Mazeti (2009). „Blackwater Guards Tied to Secret C.I.A. Raids “, *The New York Times*.

Поради непостоење на очигледна врска меѓу сајбер напаѓачот и потеклото на државата и фактот дека досега се преземени повеќе акции во сајбер просторот за кои постои сомневање, но не и докази за потеклото на нападот, примената на тие тестови може да биде важен патоказ за евентуален иден систем на регулирање на сајбер војувањето.

Изборот на начело што ќе се примени во сајбер војувањето зависи од ситуацијата, но поверојатна е примената на начелото за ефективна контрола поради можното прикривање на потеклото на сајбер нападот. Тоа значи дека за да се утврди одговорност на државата за сајбер-напад доволно е да се утврди дали постои нејзина оперативна одговорност, без докажување на целосна контрола на напаѓачот. Примената на тој принцип е погодна во случај на масовни DDoS напади, како што е нападот на Естонија и Грузија, но не е погодна за пософистицирани напади, како што е примената на компјутерскиот црв Stuxnet, што претставува многу сериозна закана.

Поради утврдување на достигнатото ниво на сајбер-напади и одговорност на државите за напад, во сајбер војувањето постојат и други карактеристични проблеми. Еден од нив е проблемот со вклучување во конфликт на неутрални држави, затоа што сајбер-нападот може да патува низ инфраструктурата на повеќе суверени држави преминувајќи ги нивните неутрални граници. Со тоа се зголемува веројатноста за ширење на конфликтот, па прашањето за суверенитетот на државите во сајбер војувањето има посебна важност. Доктрината на државна одговорност долго постои во меѓународното право, но стана ирелевантна за одредување на одговорност во случај на сајбер-напад.

Според неа, секоја држава е должна да спречи напад на друга земја на сопствената територија. Ако не е во можност да спречи напад, или не сака, тогаш државата се смета одговорна за тој напад. Но, практичната проценка на државната одговорност зависи од природата на нападот и околностите во одредена ситуација. Постојат и ставови ако државата има ефективна контрола над одредени напади, тогаш има и способност да ја насочи сопствената активност кон нив заради остварување на свое влијание. Ако државата нема ефективна контрола над актерите

на нападот, прашање е дали остварува општа контрола над нив. Прашањето за проценка на одговорноста на државата за сајбер-напади е неодредено.

Постојат и екстремни ставови дека некои држави може да се сметаат за одговорни за сајбер-напад на основа на тоа дали усвоила ефикасни закони со помош на кои ќе се спречи високотехнолошки или сајбер криминал, дали доволно активно ги применува тие закони и дали соработува со жртвите во текот на истрагата за сајбер инцидентите.

Како пример за противтезата на таквите ставови може да се сметаат напади што по природа немаат географско потекло. За да се одреди легалноста на воениот одговор, потребно е да се анализираат следните прашања:

- ✓ Дали употребата на сила како одговор во согласност со принципот на воена неопходност, т.е. дали инцидентот, освен на воен начин, може да се реши поинаку?
- ✓ Дали природата на планираниот одговор е пропорционална на нападот?
- ✓ Ако е, дали нивото на сила што се користи е претерана во однос на важноста на воените резултати што сакаат да се постигнат?
- ✓ Дали во текот на планираната употреба на сила адекватно се разликуваат воените цели и цивилното население и добра?

Сите поставени прашања произлегуваат од основните принципи на правата за време на вооружени судири. На нив тешко може да се одговори во контекст на конфликтите во сајбер просторот.

Очигледно не постои консензус околу можната примена на постоечкото право на вооружените конфликти во меѓународната заедница, а многу е дискутабилно прашањето дали и на кој начин создавањето нови прописи за сајбер војувањето може да помогне, сè додека не се дефинираат основните поими во врска со кои се засноваат субјективни ставови засновани на нејасни факти.

Справувањето со безбедносните сајбер-закани бара специфицирани знаења и мултидисциплинарен пристап. Правната рамка не е кохерентна, ниту пак, со

оглед на постојаниот напредок е возможно да се постигне конечен и унифициран правен одговор. Уште потешки се практичните импликации и обидот да се спроведе доследно истата.

7.2. Утврдување на одговорност кај недржавни актери при сајбер-напад

Иако голем број од дневните сајбер-напади се спроведена од недржавни актери, поранешната перцепција беше дека недржавните актери може да биде одговорни за одредено мнозинство на сајбер-напади, но дека државните актери се најголемата сајбер-закана. Само државите можеа да ги мобилизираат потребните средства за инвестирање во голема и долгорочна работа потребна за да реализираат сајбер-напади кои би можеле да предизвикаат реална штета од големи размери за општествата.[131]

Сепак, во последните неколку години се повеќе и повеќе внимание е посветено на хибриден вид на актери во сајбер просторот: држави кои користат недржавни актери за нивните сајбер операции.

Односите помеѓу овие „сајбер прокси“ или „сајбер платеници“ и на државните службеници со кои соработуваат се разликуваат широко, но сепак, тие имаат една заедничка работа: држави кои нарачуваат сајбер-операции од недржавните актери можат уште полесно да заобиколат атрибуција и потенцијал вклучени последици.[132]

Додека проблемот со припишувањето и следствено на леснотијата со која се негира секое вклучување е една од „придобивките“ на сајбер-напади воопшто, ангажирањето недржавни актери ја подобрува оваа „наметка на невидливоста“ за да наведува уште повеќе; државите негираат какво било знаење за активностите од страна на таканаречен независен оперативен актер, со што на жртвите им е уште потешко да преземат контрамерки.

[131] Adam Segal (2017). *The hacked world order. How nations fight, trade, maneuver, and manipulate in the digital age,* Public Affairs.
[132] Tim Maurer (2018). *Cyber mercenaries*, Cambridge University Press.

Додека државите имаат на располагање различни алатки да одговорат на големи сајбер-напади спроведени од државни актери, има помалку јасност за ефикасно справување со недржавни сајбер-напаѓачи. Ова делумно се должи на немањето договор во меѓународните односи за концептот на „due diligence“ во сајбер просторот.

Due diligence значи обврска за државите да преземат мерки за да обезбедат дека нивните територии не се користат од ниту еден актер за нанесување штети на другите држави.[133] Ако некоја држава не успее да ги исполни своите обврски за длабинска анализа, жртвата држава може да прибегне, кога е соодветно, на контрамерки како што се правните процедури или самоодбрана. Сепак, во сајбер доменот овој концепт е помалку јасен во споредба со на пример, терористи кои оперираат од одредена територија.

Во сајбер-просторот воопшто нема граници; хакери во одредена земјата може добро да користат сервери и друга дигитална инфраструктура во други земји за нивните операции.

Во 2015 година, Групата на Обединетите нации на Владини експерти кои се занимаваат со меѓународни прашања за сајбер безбедност признаа дека длабинската анализа е применлива во сајбер просторот, но мислења за импликациите и спроведувањето на концептот се разликуваат.[134]

Различни држави се двоумат околу практичната примена на принципот Due diligence кон сајбер активностите поради соодветните обврски кои би ги очекувале; особено поврзани држави, кои се поранливи да имаат сајбер-напади врз нивната критична инфраструктура, стравуваат дека тие ќе го понесат најтешкиот товар што им следува и затоа спречуваат договор по прашањето во меѓународните форуми како Обединетите нации. Тоа не значи дека државата-жртва не може да го искористи принципот Due diligence за да побара друга држава да стави крај на злонамерната сајбер активност која се спроведува од нејзината територија, но сепак

[133] Michael N. Schmitt (2015) 'In defense of due diligence in cyberspace', *Yale Law Journal Forum*, Vol. 125, pp. 68-81.
[134] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Document A/70/174, 22 July 2015, paragraph 13h

е донекаде нејасно што тоа практично значи според меѓународното право доколку државата не го стори тоа, односно не постапи по тоа барање.

Справувањето со недржавни актери во сајбер-просторот е предизвик за државите кои се соочуваат со големи размери од сајбер-напади. Особено што сè повеќе и повеќе држави како да се кријат зад т.н независни недржавни актери, корисно е да се добие поголема јасност за тоа како може да се справи со такви актери.

Државите имаат неколку достапни опции за политика за одговор на сајбер-напад кој му се припишува на недржавен актер (односно недржавни или всушност поддржани од држава). Овие опции се:

1) Барање државата домаќин да преземе акција;
2) Градење капацитети за да и помогне на државата-домаќин во преземањето акција;
3) Дипломатска акција;
4) Правни мерки;
5) Санкции;
6) Одмазда во сајбер просторот и
6) Конвенционална воена одмазда.[135]

Сепак, особено последните две политички опции треба да се користат со воздржаност, бидејќи тие содржат ризик од ескалација во случај државата да е домаќин (и/или поддржува) недржавни актери. Дополнително, секој одговор на сајбер-напад, се разбира, треба да биде пропорционален.

[135] Sico Van Der Meer (2020). *How states could respond to non-state cyber-attackers*, Clingendael Institute, Netherlands Institute of International Relations.

8. Заклучок

Комплесноста на виртуелниот сајбер простор и безбедносните закани кои од него произлегуваат, предизвикува реални ефекти во сите аспекти на секојдневното живеење.

Овој труд направи преглед на тоа како Темната мрежа влијаеше на националната безбедност до денес и ги разгледа потенцијалните средства преку кои може да ја обликува еволуцијата на заканите за националната безбедност во годините што доаѓаат. Со оглед на тоа што Темната мрежа е најпозната по тоа што е домаќин на недозволена економска трговија, стана јасно дека Темната мрежа има и некои многу сериозни импликации за националната безбедност што ќе влијаат на повеќето нации низ целиот свет.

Пролиферацијата на сајбер и кинетичко оружје, олеснување на тероризмот, собирање разузнавачки информации, изнуда, злонамерни услуги за изнајмување - сите овие недозволени активности се случуваат на Темната мрежа, а доказите сугерираат дека овие активности може да се случуваат со зголемени стапки во наредната иднина.

Војувањето отсекогаш и секогаш ќе продолжи да се развива - затоа е разумно професионалците за национална безбедност да бидат свесни за оваа еволуција и да се запознаат со различните технолошки сложености што ќе продолжат да ја обликуваат еволуцијата на војувањето.

Темната мрежа, како и другите технологии коишто се појавуваат, е една од тие технолошки сложености. Темната мрежа потенцијално би можела да влијае на нивните соодветни области на одговорност. Згора на тоа, би било разумно да се земат предвид потенцијалните контрамерки и способностите за следење, како што е интелигенцијата за закани фокусирана на Темната мрежа, кои би можеле да се применат за подобро разбирање на заканите поврзани со темната мрежа. Без оглед на средствата што се користат за подобро разбирање на оваа закана што се појавува, главна цел треба да биде да се создаде зголемена колективна свест кај националната безбедносна заедница.

Сакаме да ја искористиме оваа свест и за да ја намалиме можноста за стратешко изненадување, како и да го олесниме предвидливото разбирање за тоа како нашите противници веројатно ќе ја користат Темната мрежа во текот на нивните сопствени злонамерни операции.

И иако оваа свест можеби не мора нужно да ги спречи заканите за националната безбедност од темната мрежа, таа секако може да го насочи вниманието на ова прашање и да олесни поголем разговор за тоа како глобалната заедница може да се справи со овие закани кои се појавуваат.

Ако ја земеме предвид општата хипотеза што беше поставена во овој труд, а тоа е: Улогата на Темната мрежа ќе има значајни негативни импликации врз безбедноста, особено во начинот на водење на идните сајбер-војни, може да се каже дека е потврдена со содржината во овој труд. Констатираме дека Темната мрежа е основната појдовна база за водење на скриени сајбер-војни што ја напаѓаат критичната инфраструктура на државите кои се цел на интерес на поединци или групи кои заради остварување на своите интереси, пред сѐ финансиски, со што ќе наштетат на виталните функции на поедини национални држави и влади.

Распространетото ширење на способностите преку Темната мрежа им овозможува на актерите да го искористат сопственото техничко разбирање за експлоатирање на сајбер просторот за да реализираат сајбер операции и закани кои се таинствени и поопасни од претходните. Токму знаењето и напредната технологија придонесуваат да се експлоатира сајбер просторот и да се извршат операции кои се тајни и се различни од аспект на степенот на опасност, за да ги остварат своите разурнувачки цели.

Во иднина, одредени државни и недржавни групи актери со закани ќе сакаат да ги забрзаат своите способности за сајбер-војна, преку експлоатирање на темната мрежа за да ги добијат саканите услуги. Темната мрежа е всушност, основата, просторот каде што одредени актери, со развиени технички и технолошки знаења, преку закани сакаат да предизвикаат сајбер-војни заради свои интереси.

Меѓу-институционалниот и мулти-дисциплинарниот пристап со вклучување на сите засегнати страни е од клучно значење за да се обезбеди ефикасен одговор на активностите на Дарк Веб. И секако, поаѓајќи од оваа посебна хипотеза, за предизвикување војна потребни се најмалку двајца, две држави, при што ако едната страна нападне, другата секогаш ги презема сите средства, за да даде свој соодветен одговор на тоа, а Дарк-Веб/Темната мрежа е просторот каде што се одвиваат тие активности. Унапредувањето на соработката со регионалните и меѓународните полициски организации е од суштинско значење за справување со Дарк веб.

Воспоставување ефикасни процедури за пријавување и истражување на Темната мрежа имплицира намалување на негативните импликации врз безбедноста. Ефикасноста на процедурите зависи од нивната примена во практиката што доведува да се намалат штетните последици по безбедноста што е клучно во справувањето со овој проблем.

Активното меѓународно учество во справување со глобалниот предизвик од сајбер-заканите ќе придонесе за зголемување на државните капацитети за справување со сајбер-ризиците. Токму вклученоста на меѓународно ниво во справувањето со овој проблем овозможува засегнатоста на државите да стане поголема во процесот на намалување на сајбер-заканите и ризиците.

Преку соработка на сите засегнати страни за унифицирање безбедносни норми, стандардизирање на соработката ќе се воспостави задолжително ниво на заштита за субјектите. Во самиот труд, соработката на сите страни, вклучени во овој нов предизвик се покажа како клучна во борбата против овој проблем што воедно воспоставува заштита за сите засегнати страни.

Создавање на национална платформа/систем за размена на информации во врска со закани, инциденти и непосредните опасности ќе резултира кон подобрување на заштитата од дејствувањето на Дарк веб. Во справувањето на некој проблем, ако повеќе страни на национално ниво се справуваат со некој проблем, тие креираат платформа, како заеднички простор за размена на информации,

искуства во врска со заканите, ризиците и инцидентите и тоа придонесува за зголемување на безбедноста и заштита од активностите на Дарк Веб.

Со брзото зголемување на количината и сложеноста на сајбер-заканите кои се појавуваат од различни делови на интернет, организациите сè повеќе ги истражуваат сајбер-заканите како еден од виталните системи на нивното оперативно постоење. Се користат повеќе извори на информации, аналитика и знаење за носителите на одлуки да преземат соодветни активности против сајбер-заканите. Еден од најважните извори е Темната мрежа, која сè повеќе привлекува голем интерес од истражувачите поради нејзината поврзаност со сајбер-заканите презентирани на различни видови платформи како што се форуми (дискусии, упатства и средства) и пазари (понудени производи и услуги).

Оваа еволуција или подобро речено револуција во сајбер-нападите, може да биде видена како модерна алатка за индиректна интервенција за тајно уништување на противничката мрежа и критичната воена инфраструктура, покажувајќи ја стратегиската важност на технолошката еволуција во сајбер просторот и на тој начин навестувајќи го полето на развој на идната сајбер-војна.

9. Користена литература

1. Aaaron Holmes (2021) 533 million Facebook users' phone numbers and personal data have been leaked online, *Insider*, достапно на: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.
2. Abbasi, A. and Chen, H. (2008), "Analysis of Affect Intensities in Extremist Group Forums," In: *Terrorism Informatics,* E. Reid and H. Chen, Eds., Springer.
3. Abdulmuttaleb A., (2017) *Critical Analysis of the emerging Dark Web*, Cardiff Metropolitan University.
4. Acharya, A (2009). *Targeting Terorist Financing: International Cooperation and New Regimes*, New York: Routhledge.
5. Aliens, C. (2016), Darknet Bust: Global Law Enforcement Raids Massive Counterfeiting Organization, *Deep Dot.Web*, December 17.
6. Analysis of top 11 cyber attacks on critical infrastructure (2021), достапно на: https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
7. Antonio Cassese (2007) The Nicaraqua and Tadić Test Revisited in light of the ICJ Judgment on Genocide in Bosnia (2010), *The European Journal of International Law,* Vol. 18 no. 4, достапно на: www.ejil.org/pdfs/18/4/233.pdf.
8. Antonio Cassese, (2001) "Terrorism Is Also Disrupting Some Crucial Legal Categories of International Law", *European Journal of International Law*, Vol 12, No.5, стр. 993–1001, достапно на: https://www.unodc.org/tldb/bibliography/Biblio_Internat_law_Cassese_2001.pdf
9. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), International Court of Justice, достапно на: http://www.icj-cij.org/docket/index.php?p1=3&k=f4&p3=4&case=91
10. Armin, J. at al. (2015). 0-day vulnerabilities and cybercrime, in: Availability, Reliability and Security (ARES), 10th *International Conference On*.

11. Barysevich, Andrei (2018). "Military Reaper Drone Documents Leaked on The Dark Web", *Recorded Future*, достапно на: https://www.recordedfuture.com/reaper-drone-documents-leaked/.
12. Berton, B. (2015). "*The dark side of the web: ISIL's one-stop shop?"*. Report of the European Union Insti-tute for Security Studies, достапно на: http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf.
13. Biddle, P. at al. (2002). *The Darknet and the Future of Content Protection*. In ACM Workshop on Digital Rights Management, Springer-Verlag Berlin Heidelberg.
14. Broadhurst, R. (2017). *Cyber Terrorism Research Review Cyber Terrorism*: Research Review Research Report of the Australian National University, достапно на: https://doi.org/10.13140/RG.2.2.19282.96964.
15. Brynielsson, J. at al. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists, Security Informatics, no.11.
16. C. Aliens. (2018). "More Details Revealed in The Dublin Explosives Case", *Deep Dot Web*, достапно на: https://www.deepdotweb.com/2018/08/05/more-details-revealed-in-the-dublin-explosives-case/.
17. Callahan, Michael (2014) "Hackonomics: A First-of-Its-Kind Economic Analysis of the Cyber Black Markets," *Juniper Networks*, достапно на: https://forums.juniper.net/t5/Security/Hackonomics-A-First-of-Its-Kind-Economic-Analysis-of-the-Cyber/ba-p/234262.
18. Carl von Clausewitz, On War, trans. J.J. Graham (London, UK: Nicholas Trubner, 1873), Book I, Chapter 1, para 2, http://www.gutenberg.org/files/1946/1946-h/1946-h.htm#link2HCH0001
19. Casadei B. (2019) Terorist Use of Cryptocurrencies- A Blockchain Compliance White Paper, Blockchain Consultus, London, United Kingdom
20. Center for Strategic and International Strudies (2022), *Significant Cyber Incidents*, достапно на: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
21. Charles Arthur (2013). "Lulzsec: What They Did, Who They Were And How They Were Caught", *The Guardian*, достапно на:

https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail.

22. Chen, H. (2012). *Dark web: Exploring and data mining the dark side of the web*. New York, NY, достапно на: https://www.springer.com/gp/book/9781461415565
23. Chertoff M., A (2017). Public policy perspective of the Dark Web, *Journal Cyber Policy*, p.28.
24. "Cybersecurity Incidents", U.S. Office Of Personnel Management, достапно на: https://www.opm.gov/cybersecurity/cybersecurity-incidents
25. Clarke, Richard A. & Knake, Robert K. (2010) *Cyber War. The Next Threat to National Security and What to Do About It*, Harper Collins e books.
26. Clearing Up Confusion - Deep Web Vs. Dark Web - Brightplanet", (2014), *Brightplanet*, достапно на: https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.
27. Cognyte CTI Research Group (2021), *2021 Linkendin Breach: Cyber criminals are the new heradhunters,* достапно на: https://www.cognyte.com/blog/2021-linkedin-breach-cybercriminals-are-the-new-headhunters/#
28. Conversation between Dark Web vendor and an individual potentially affiliated with terrorism"(2018), Complaints Board, достапно на: https://www.complaintsboard.com/complaints/fake-id-passports-fake-id-passports-c735014.html?page=2#comments/.
29. Cox, Joseph (2018). "After Arrest In Serbia, Netflix Hackers 'The Dark Overlord' Say They're Still Going", *Motherboard,* достапно на: https://motherboard.vice.com/en_us/article/mbkex8/dark-overlord-arrest-serbia-netflix-hackers.)
30. "Crypto Crowdfunding Terrorists: Marketplace for Jihadist Crowdfunding Found on Dark Web" (2018), *CCN*, достапно на: https://www.ccn.com/crypto-crowdfunding-terrorists-marketplace-for-jihadist-crowdfunding-found-on-dark-web/.
31. Dalins, J. at al. (2017). Criminal motivation on the dark web: A categorisation mode for law enforcement. Digital Investigation.

32. Dalins, J.at. al. (2017) Criminal motivation on the dark web: A categorization model for law enforcement. *Digital Investigitation*.
33. Danny Bradbury *(*2014). Unveiling the dark web. *Network Security* 4(4)*: 14-17*
34. Denic, N. V. (2017). *Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web,* thesis presented to the Faculty of the U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.
35. Derek Jinks (2003) „State Responsibility for the Acts of Private Armed Groups ", *Chicago Journal of International Law*, Vol. 4, достапно на: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=391641
36. DiPiero, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep DarkWeb. *University of Illionois Law Review*.
37. Drakulic, Mirjana (1996). "*Osnovi kompjuterskog prava*." Drustvo operacionih istrazivača Jugoslovije, DOPIS, Belgrade.
38. Enternmann, E, Willem van derBerg (2018). *Terorist Financing and Virtual Cirrencies: Different Sides of the Same Bitcoin?* International Centre for Countering Terrorism, Hague.
39. EUROPOL. (2018). *Internet Organized Crime Threat Assessment*, European Union Agency for Law Enforcement Cooperation, достапно на: www.europol.europa.eu.
40. Everette J. (2017) *Public-Private Analytic Exchange Program: Risks and Vulnerability of Virtual Currency*, Washington, Director of National Intelligence.
41. Finklea, K. (2015). *The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement*, CRS Report R41927 p.35
42. Geers, Kenneth. (2013). Sun Tzu and Cyber War (NATO Cooperative Cyber Defence Centre of Excellence; Libicki, Cyber War as a Confidence Game; Schmidt, Eric & Cohen, Jared. *The New Digital Age: Reshaping the Future of People, Nations and Business*, John Murray Publishers.
43. Geneva Sands (2016). "What To Know About The Worldwide Hacker Group 'Anonymous'", *ABC News*, достапно на: https://abcnews.go.com/US/worldwide-hacker-group-anonymous/ story?id=37761302.)

44. Gupta, Maynard & Ahmad (2019). *The Dark Web Phenomenon*, Australasian Conference on Information Systems.
45. Gupta, Maynard & Ahmad, Perth, (2019) *WA The Dark Web Phenomenon*, Australasian Conference on Information Systems.
46. H. Chen (2010). *Dark Web: Exploring and Data Mining the Dark Side of the Web*, Springer, p.66
47. Hacktivist | Definition of Hacktivist in English by Oxford Dictionaries", Oxford Dictionaries, достапно на: https://en.oxforddictionaries.com/definition/hacktivist.
48. http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/
49. http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf
50. https://ccdcoe.org/tallinn-manual.html
51. https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev.)
52. https://www.newamerica.org/cyber-global/compilation-of-existingcybersecurity-and-information-security-related-definitions/
53. Huang, K. at al. (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*.
54. Iasiello Emilio (2015). Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs*. Vol.7.
55. "International arms trade on the dark web" (2017), RAND Corporation, достапно на: https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html.
56. III Хашка конвенција о започињању непријатељстава из 1907. године, http://www.icrc.org/ihl.nsf/FULL/190
57. James Risen, Mark Mazeti (2009). Blackwater Guards Tied to Secret C.I.A. Raids, *The New York Times*.
58. Janseen, D. (2018). Deep Web. *Techopedia*.

59. Jason Rivera and Wanda Archy (2019). The Role of the Dark Web in Future Cyber Wars to Come, *Small Wars Journal,* достапно на: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-come
60. Jona, Sam, (2018) "Cybercrime Revenue Estimated to Be $1.5 Trillion", *Deep Dot Web*, достапно на: ttps://www.deepdotweb.com/2018/05/05/cybercrime-revenue-estimated-to-be-1-5-trillion/.
61. Kirkpatrick, K. (2017). Financing the Dark Web. *Communication*. ACM 60, 21–22.
62. Koch, R. (2019). *Hidden in the Shadow: The Dark Web – A Growing Risk for Military Operations?* NATO CCD COE Publications, Tallinn.
63. "Kafr Qasem Resident Indicted for Financing and Purchasing Weapons for Terrorist on Dark Web"(2018), *Deep Dot Web*, достапно на: https://www.deepdotweb.com/2018/12/01/kafr-qasem-resident-indicted-for-financing-and-purchasing-weapons-for-terrorist-on-dark-web
64. Lau, Lynette. (2018) "Cybercrime 'pandemic' may have cost the world $600 billion last year", *CNBC*, достапно на: https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html.
65. Libicki, Martin (2011). C. Cyber War as a Confidence Game, *Strategic Studies Quarterly* no. 5
66. Maddox, A. at al. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde.' *Information, Communication and Society*. 19, 111–126, достапно на: https://doi.org/10.1080/1369118X.2015.1093531
67. Malik, N. (2018). How Criminals and Terrorists Use Cryptocurrency: And How To Stop It, Forbes, 31 August, достапно на: http://www.forbes.com/sites/nikitamalik/2018/08/31 how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it//
68. Maurer Tim (2018). *Cyber mercenaries*, Cambridge University Press.
69. Martijn Spitters, Stefan Verbruggen, Mark van Staalduinen (2014). *Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services*, IEEE Joint Intelligence and Security Informatics Conference.

70. Mazzetti, Mark; et al. (2017) "Killing C.I.A. Informants, China Crippled U.S. Spying Operations", *The New York Time*, достапно на: https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html.
71. Michael N. Schmitt, (2007) 21st Century Conflict: Can the Law Survive? ", 8(2) Melbourn Journal of International Law 24, достапно на: http://www.austlii.edu.au/au/journals/MelbJIL/2007/24.html
72. Mirjana Drakulić, Ratimir Drakulić, (2010) Evropska perspektiva regulisanja Internet usluga: izazov tradicionalnom evropskom pravu ", *Telekomunikacije*, no. 6.
73. Moore, D., Rid, T. (2016). Cryptopolitik and the Darknet. *Survival,* London, 58, 7–38.
74. NATO. (2008). Bucharest Summit Declaration para. 47 (Apr. 3).
75. NATO. (2010). Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, достапно на: http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng. p.
76. North Korea's APT 38 hacking group behind bank heists of over $100 million", (2018) ZD-Net, достапно на: https://www.zdnet.com/article/north-korea-s-apt38-hacking-group-behind-bank-heists-of-over-100-million/.
77. Nye, Joseph S. Jr, (2010), Nuclear Lessons for Cybersecurity. *Strategic Studies Quarterly* 5 no.4, 21.
78. Oftedal, E. (2015). *The financing of Jihadi Terorist Cells in Europe*, Norway: Forsvarets Forskningsinstitutt.
79. Owen, G. Savage, N. (2016). Empirical analysis of Tor hidden services. IET *Information Security* 10, 113–118.
80. Ozkaya E, Rafikul, I. (2019*). Inside the Dark Web*, CRC Press, Taylor and Francis Group, USA.
81. Peter W. Singer, Allan Friedman. (2014)

82. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Document A/70/174, 22 July 2015, paragraph 13h
83. Rhumorbarbe, D. at all., (2018). Characterising the online weapons trafficking on cryptomarkets. *Forensic Science Int*ernational 283, 16–20.
84. Rivera, J. Archy, W. (2019). The Role of the Dark Web in Future Cyber Wars toCome, *Small War Journal*, достапно на: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-com.
85. Robert W. Gehl (2016), Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network, *New Media and Society*, достапно на: https://journals.sagepub.com/doi/full/10.1177/1461444814554900
86. Robertson, J. at al. (2017). *Dark web Cyber Threat Intelligence Mining*. Cambridge: University Press.
87. Sapienza, A. at al. (2018). *Early Warnings of Cyber Threats in Online Discussions*. ar Xiv Prepr. arXiv1801.09781
88. Adam Segal Adam (2017). *The hacked world order. How nations fight, trade, maneuver, and manipulate in the digital age,* Public Affairs.
89. Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for A Growing Problem".
90. Shapiro, J.N. (2012). Terrorist Decision-Making Insight from Economics and Political Science, *Perspectives on Terrorism*, Vol.6 No.4-5.
91. Michael N. Schmitt (2015) 'In defense of due diligence in cyberspace', *Yale Law Journal Forum*, Vol. 125, pp. 68-81.
92. Sico Van Der Meer (2020). *How states could respond to non-state cyber-attackers*, Clingendael Institute, Netherlands Institute of International Relations.
93. Stolen Drone Files Sold on Dark Web"(2018). *BBC News*, достапно на: https://www.bbc.com/news/technology-44807091
94. Stone, Jeff (2015), "The Dark Net Is Selling Hacked OPM Information, And It Could Be Worth $140M: Report", *International Business Times*, достапно на: https://www.ibtimes.com/dark-net-selling-hacked-opm-information-it-could-be-worth-140m-report-1989911.

95. Taking Stock of the Online Drugs Trade", (2016), RAND Corporation, достапно на: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.
96. Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). Cambridge University Press.
97. The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) (2018), достапно на: https://www.emcdda.europa.eu/emcdda-home-page_en
98. "Taking Stock of the Online Drugs Trade" (2016), RAND Corporation, достапно на: https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.
99. The Tor Project, Inc, *Torproject.Org*, достапно на: https://www.torproject.org/
100. The United States Department of Justice (2020), Office of Public Affairs, Global Disruption of Three Terror Finance Cyber –Enabled Campaigns, 13 August.
101. Tisma, M. (2020). Hibridno ratovanje i bojno polje, Odbrana i bezbednost, Analiza sa distance, достапно на: https://odbranaibezbednost.rs/2020/02/11/hibridno-ratovanje-i-bojno-polje/
102. Tunggal A. T. (2021). What is Cyber Threat? достапно на: https://www.upguard.com/blog/cyber-threat
103. Tzanetakis, (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time, *International journal on drug policy*, p.176-186.
104. V. Ciancaglini, M. Balduzzi, R. McArdle, M. Rosler (2019), "Below the Surface: Exploring the Deep Web", *Trend Micro*, pp. 1-48.
105. Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, 8 I.L.M.
106. Ward, A. (2018) *Bitcoin and the Dark Web: The New Terorist Threat*? RAND Corporation, January, достапно на: http://www.rand.org/blog/2018/01bitcoin-and -the-dark-web-new-terrorist-threat.html
107. Warrick, Joby. (2011). "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack", *Washington Post*, достапно на:

http://www.washingtonpost.com/wpdyn/content/article/2011/02/15/AR2011021505395.html?noredirect=on.

108. Weimann, G. (2016). "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism* 39, 195-206, достапно на: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546

109. Weimann, G. (2016). "Terrorist Migration to the Dark Web," *Perspectives on terrorism*, Vol. 10, no. 3.

110. Weimann, G. (2017). *Going Darker-The challenge of Dark Net Terrorism*, Wilson Center, Washington DC, USA.

111. Weise, Elizabeth (2017). "Terrorists use the Dark Web to hide," *USA Today,* 2017, достапно на: https://www.usatoday.com/story/tech/news/2017/03/27/terrorists-use-dark-web-hide-london-whatsapp-encryption/99698672/.

112. What Is an Insider Threat? An Insider Threat Definition"(2018), *Digital Guardian*, достапно на: https://digitalguardian.com/blog/what-insider-threat-insider-threat-definition.

113. William Turton, Michael Riley, Jennifer Jacobs. (2021). "Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom", *Bloomberg*.

114. Williams, David. (2018)"Americans Will Soon Be Able to Legally Download 3-D Printed Guns", *CNN* https://www.cnn.com/2018/07/19/us/3d-printed-gun-settlement-trnd/index.html.

115. Wilson Center Report. (2015). "*The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box"*, достапно на: https://www.wilsoncenter.org/sites/default/files/deepweb-report_october_2015.pdf.

116. Zetter, Kim. "An Unprecedented Look at Stuxnet (2014), The World's First Digital Weapon", *WIRED*, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

117. Zhang, X. (2003). *System/Application Designs, Optimization and Implementations on Overlay Networks*. High Performance Computing and Software Lab. Ohio State University.

118. Декларација о принципима у међународном праву из 1970. године, (http://daccessdds.un.org/doc/RESOLUTION/GEN/NR0/348/90/IMG/NR034890.pdf?OpenElement

119. Длабока интернет мрежа. Невидлив интернет, достапно на интернет страницата: https://bitserv.ru/mk/deep-internet-network-invisible-internet/

120. Милошевска, Т. (2020), Дарк веб- Нова транснационална безбедносна закана, *Годишен зборник*, вол.73, Филозофски факултет, Скопје.

121. Поповска Весна (2016). Правни аспекти на сајбер безбедноста, год. 6, бр.6, *Годишен зборник*, Универзитет Гоце Делчев, Штип.