Тања МИЛОШЕВСКА

УДК: 007:004.056
Прегледен труд

ДАРК ВЕБ – НОВА ТРАНСНАЦИОНАЛНА БЕЗБЕДНОСНА ЗАКАНА

Кратка содржина

Во последните години, Дарк веб се претвори во една од најдискутираните теми во круговите за кибербезбедност. Неодамнешните академски анализи и написи за медиуми имаат тенденција да се фокусираат како се користи анонимната природа на Дарк веб со цел да се овозможат криминални активности. Оваа статија ги анализира и ги потенцира главните улоги што ги има Дарк веб како маркет; како комуникациска платформа; како овозможувач на киберкриминал; како овозможувач на анонимни финансиски трансакции и како полномошник на површинската мрежа. Поточно, привлекува внимание „црниот пазар" на интернет-темната мрежа бидејќи претставува скриен простор станувајќи најголема аплицирана анонимна мрежа. Овој успех е поддржан од бројни одлики, карактеристики што се вградени во високотехнолошката структура на темната мрежа, на пример, тајност, анонимност и употреба на криптовалути. Различното опкружување на пазарот Дарк веб кое е крајно анонимно, таинствено, како и сигурно, го етаблира како случај за тестирање за неограничен интернет кој може да се добие на маркетот.

Клучни зборови: *ДАРК ВЕБ, КИБЕРБЕЗБЕДНОСТ, БЕЗБЕДНОСНА ЗАКАНА, ИЛЕГАЛНИ АКТИВНОСТИ, НЕЗАКОНСКИ УСЛУГИ*

Вовед

Дигиталниот универзум е огромен, а интернетот и глобалната мрежа се многу поголеми од она што го перципираме преку редовното прелистување. Интернетот и неговите корисници рапидно растат како резултат на новите апликации на информатичката технологија (ИТ) и се очекува трендот да продолжи. Сепак, брзиот раст на интернетот го остави подложен истиот на неправилно користење и злоупотреба, што станува значајна закана и предизвик во киберпросторот низ целиот свет (Ozkaya, Islam, 2019).

Интернет и мрежните технологии се развиле драматично во последните две децении, со зголемувањето на барањата на корисниците да ги зачуваат своите идентитети и приватноста. Истражувачите развија пристапи за да ги постигнат барањата на корисниците, каде што се формира најголемиот дел од Длабоката мрежа. Како и да е, со оглед на тоа што Длабокиот веб обезбедува „одморалиште" за многу бенигни корисници кои сакаат да ја зачуваат својата приватност, тој исто така стана совршено

место за хостирање на недозволени активности, кои ги создава Дарк веб (мрачниот веб) (AlKhatib, Randa Basheer, 2018).

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 порнографски слики и видеа и имаше повеќе од 215.000 корисници (Koch, 2019).

Како дел од подготовките за терористичките напади во Париз во ноември 2015 година, комуникацијата беше анонимна со користење на софтверот TOP; додека оружјето користено во нападот во Минхен во јули 2016 година, исто така било набавено преку Темната мрежа. Покрај дрога, оружје и детска порнографија, 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 (Koch, 2019).

Терминологија

Мошне често, термините Дарк нет (Darknet), Длабок веб (Deep Web) и Дарк веб (Dark Web) неправилно се мешаат или се користат наизменично. Поради недоволното раздвојување и злоупотребата на термините, податоците и евалуациите можат да бидат неправилно распоредени и да ја прикријат фактичката состојба (Koch, 2019).

Длабок веб. Длабокиот веб „се однесува на сите интернет-информации или податоци што се недостапни од пребарувачот и ги вклучуваат сите веб-страници, интранет, мрежи и мрежни заедници кои се намерно и/или ненамерно скриени, невидливи или недостапни за роботите на пребарувачот" (Janssen 2018). Терминот Длабок веб, „има асоцијација на длабоки морски/океански опкружувања, кои се практично невидливи и недостапни" (Janssen 2018). Овие скриени делови на интернет се познати како Длабок веб. Длабоката мрежа е приближно 400 - 500 пати помасовна од површинската мрежа. (Wilson Center, 2015). 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" (Janssen 2018).

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 содр-

жина 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“ (Biddle 2002). 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 (Zhang 2003). Софтверот Тор 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 (Koch, 2019).

Најдлабоките слоеви на Длабокиот веб, сегмент познат како „Темна мрежа“, содржат содржини кои се намерно 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 Тор). Една неодамнешна студија 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 (Moore, Rid, 2016).

Незаконски активности и услуги

Темниот веб е цитиран како олеснување на широк спектар на злосторства/криминални активности. Нелегалната стока како што се дрога, оружје, егзотични животни и украдени производи и информации се продаваат како профит. Постојат сајтови за коцкање, крадци и атентатори за изнајмување и содржини со сексуална злоупотреба на деца (Chertoff, Simon, 2015). Податоците за застапеноста на овие веб-страници, сепак, недостасуваат. Тор софтверот проценува дека само околу 1,5 % од корисниците на Тор посетуваат скриени услуги/темни веб-страници (Tor Project Blog, 2015).

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 (EUROPOL, 2018).

Интернет-криминалците можат да ги злоупотребуваат поединците и организациите, и тие можат да го сторат тоа без оглед на границите. Како криминалците ги искористуваат границите е повеќегодишен предизвик за спроведување на законот, особено што се развиваше концептот на границите (Finklea, 2017).

Активностите како што се трговија со дрога, трговија со оружје, злоупотреба на деца, трговија со чувствителни информации, малициозен софтвер и шпионски производи, споделување на софтвер, искористуваат информации што хактивистите ги откриваат во компјутерски системи или изнајмување на Ботнет, што е целосно опремена мрежа поврзана на интернет каде 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 може да се идентификуваат. Исто така, вклучува финансиска измама, рекламирање на криминални идеологии, дури и врбување на напаѓачи и многу повеќе. Темниот вебскриен сервис, исто така, се наоѓа во „Темниот веб“, каде специјални служби што се домаќини на безбедносните активности работат како околина за хостирање (Hawkins, 2016).

Улога во поширок контекст	**Специфични случаи**	**Опис**
As a Market	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 (Tzanetakis, 2018).
	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 (Armin et al., 2015).
	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 (Denic, 2017)
	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. (Kirkpatrick, 2017).
	Трговија со оружје	Продажба на оружје особено во земји каде е забрането (Rhumorbarbe et al., 2018).

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 (Sapienza et al., 2018).
	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 (Maddox et al., 2016).

Улога во поширок контекст	Специфични случаи	Опис
Овозможувач на киберкриминал	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 (Huang et al., 2017).
	Сервери за команда и контрола (C2) распоредени како скриени услуги	Ботнет се контролираат од C2 услугите хостирани како Tor скриени услуги (Owen and Savage, 2016).
	Терористички операции спроведени во врска со други улоги	Врбување, обука, радикализација, планирање, собирање средства за познати терористички организации, на пр. Исламската држава ИСИС (Broadhurst, 2017).

Улога во поширок контекст	Специфични случаи	Опис
Како извор на разузнавање за закани	Форуми за скенирање и места за разузнавање закани	Проценка за вид на напади кои може да бидат иманентни, засновани на информации кои се продаваат или разменуваат на форумите. (Robertson et al., 2017).

Улога во поширок контекст	Специфични случаи	Опис
Овозможување анонимни финансиски трансакции	Употреба на биткоин преку Tor за анонимност	Додадено ниво на анонимност и претпазливост (DiPiero, 2017).
	Перење пари на криптовалути преку Tumbling услуги	Специфични услуги за перење пари, на пр., преку конвертирање во биткоини (Dalins et al., 2017).

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 (Chertoff and Simon, 2015).
	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 (Moore and Rid, 2016).

Според Европскиот центар за мониторинг на наркотици и зависности од дрога (EMCDDA, 2018) и Европол (2018), Германија, Холандија и Велика Британија биле најважните земји во однос на снабдувањето со дрога преку Дарк веб 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 Дарк нет се „локални трговци на мало" кои функционираат како „последна милја" на рутите за трговија со дрога (Dittus, at al, 2018). Ова е поткрепено со други истражувања дека пазарите во Дарк веб најмногу се користат за продажба на пазарот со среден или низок обем или продажба директно на потрошувачите. Голем обем на продажба на пазарите во Дарк нет е релативно невообичаен (Europol, 2018).

Но, бидејќи трговијата со недозволена стока е една од најзначајните активности што се одвива на Длабокиот веб, 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. Како таква, технологијата ќе се користи за спроведување на полни размери на пазарот без ниту една точка на неуспех и кои се потпираат на одредени аспекти на теоријата на игри, за да се гарантираат безбедни трансакции, механизми за зачувување и доверба меѓу актерите кои можат да бидат во сенка (Ciancaglini at all, 2015).

Терористичка употреба на онлајн платформи

Терористите се активни на разни мрежни платформи уште од крајот на 90-тите години (Weimann, 2016). 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" (Berton, 2015).

Ова доведе до нивна миграција кон темната мрежа и го направија нивното однесување уште поотпорно за да бидат нарушени (Denic, 2017). 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". Вториот се припишува на значителна количина на терористичка активност низ целиот свет и нивната идентификација на темните веб-форуми преку обработка на мајчиниот јазик е постојан напор кој се вложува (Brynielsson et al., 2013).

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 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 (Weimann, 2017).

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 (Malik, 2018). 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.

4. Терористите користат виртуелни валути за да избегнат откривање и прибирање финансиски средства: Терористите, како криминалци, користат криптовалути, бидејќи тоа обезбедува иста форма на анонимност во финансискиот амбиент како што е криптирањето за комуникациските системи (Weimann, 2016).

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 се јавуваат со зголемени стапки во иднина (Rivera and Archy, 2019).

Заклучок

Темниот веб претставува сериозен безбедносен ризик и тајните мрежи од една страна стануваат начин за постигнување слобода преку интернет; додека од друга гледна точка овие мрежи не се повеќе од нови канали за изразување одредени криминогени желби.

Наодите од овој труд би помогнале во унапредувањето на безбедносните технологии и практики за подобро управување со некои од поу-

никатните карактеристики на Дарк веб кои се идентификувани. Темната мрежа не е општество каде криминалот е модел или шема. Всушност претставува технолошка платформа која ја користат различни индивидуи за најразлични намени.

Литература:

ALKHATIB, B. BASHEER, R. (2018). Crawling the Dark Web: A Conceptual Perspective, Challenges and Implementation. *Journal of Digital Information Management*. Syrian Virtual University. Syria.

ARMIN, J. AT AL. (2015). 0-day vulnerabilities and cybercrime, in: Availability, Reliability and Security (ARES), 10th *International Conference On.*

BERTON, B. (2015). "The dark side of the web: ISIL's one-stop shop?". Report of the European Union Insti-tute for Security Studies, June 2015. Available at: http://www.iss.europa.eu/uploads/media/Alert_30_The_-Dark_Web.pdf.[Accessed 17 February 2020].

BIDDLE, P. AT AL. (2002). The Darknet and the Future of Content Protection. In ACM Workshop on Digital Rights Management, Springer-Verlag Berlin Heidelberg.

BROADHURST, R. (2017). *Cyber Terrorism Research Review Cyber Terrorism*: Research Review Research Report of the Australian National University. Available at: https://doi.org/10.13140/RG.2.2.19282.96964. [Accessed 17 February 2020].

BRYNIELSSON, J. AT AL. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Secur. Inform*. 2, 11.

CHERTOFF, M., SIMON, T. (2015). *The Impact of the Dark Web on Internet Governance and Cyber Security,* Global Commission on Internet Governance, The Royal Institute od International Affairs, Centre for International Governance Innovation and Chatham House, No. 6. Available at: https://www.cigionline.org/sites/default/files/gcig_paper_-no6.pdf. [Accessed 17 February 2020].

CIANCANGLINI VINCENZO AT AL. (2015). *Below the Surface: Exploring the Deep Web* Trend Micro.

DALINS, J. AT AL. (2017). *Criminal motivation on the dark web: A categorisation model for law enforcement.* Digit. Investig.

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.

DIPIERO, C. (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. *Ill. L. Rev.*1267.

DITTUS, M. AT AL. (2018). Platform Criminalism: The 'last-mile' geography of the darknet market supply chain, in WWW 2018, Lyon: France. European Monitoring Centre for Drugs and Drug Addiction (2018). Available at: http://www.emcdda.europa.eu/drugs-library/emcdda-europol-working-arrangement-2018_en. [Accessed 16 February 2020].

EUROPOL. (2018). *Internet Organized Crime Threat Assessment*, European Union Agency for Law Enforcement Cooperation 2018. Available at: www.europol.europa.eu. [Accessed 12 March 2020].

FINKLEA, K. (2017). *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, CRS Report R41927.

HAWKINS, B. (2016). Under The Ocean of the Internet - The Deep Web. Available at: https:/ /www.sans.org/reading-room/whitepapers /covert/ oceaninternet-deepweb-37012. [Accessed 22 February 2020].

HUANG, K. AT AL. (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt*.

JANSSEN, D. (2018). Deep Web. Techopedia 2018.

KIRKPATRICK, K. (2017). Financing the Dark Web. *Commun*. ACM 60, 21–22.

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

KREBS, B. (2015). "Tax Fraud Advice, Straight From the Scammers," *Krebs on Security*.

MADDOX, A. AT AL. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde.' *Inf. Commun. Soc*. 19, 111–126. Available at: https://doi.org/10.1080/1369118X.2015.1093531 [Accessed 17 February 2020].

MALIK, N. (2018). "Terror in the Dark", a report by the the Henry Jackson Society, London. Available at: http://henryjackson-society.org/wpcontent/uploads/2018/-04/Terror-in-the- Dark.pdf. [Accessed 17 February 2020].

MOORE, D., RID, T. (2016). Cryptopolitik and the Darknet. *Survival* (Lond). 58, 7–38.

OWEN, G. SAVAGE, N. (2016). Empirical analysis of Tor hidden services. IET *Inf. Secur.* 10, 113–118.

OZKAYA E, RAFIKUL, I. (2019*). Inside the Dark Web*, CRC Press, Taylor and Francis Group: USA.

RHUMORBARBE, D. AT ALL., (2018). Characterising the online weapons trafficking on cryptomarkets. *Forensic Sci. Int*. 283, 16–20.

RIVERA, J. ARCHY, W. (2019). The Role of the Dark Web in Future Cyber Wars to Come, *Small War Journal*. Available at: https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-com. [Accessed 1 February 2020].

ROBERTSON, J. AT AL. (2017). *Darkweb Cyber Threat Intelligence Mining*. Cambridge: University Press.

SAPIENZA, A. AT AL. (2018). Early Warnings of Cyber Threats in Online Discussions.arXiv Prepr. arXiv1801.09781.

TOR PROJECT BLOG. (December 30, 2014) *Tor: 80 Percent of ??? Percent of 1-2 Percent Abusive*.

TZANETAKIS, M. (2018). Comparing cryptomarkets for drugs. A characterization of sellers and buyers over time. *Int. J. Drug Policy*.

WEIMANN, G. (2016). "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism* 39, 195-206.
Available at: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546. [Accessed 12 February 2020].

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

WILSON CENTER REPORT. (2015). "The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box".
Available at: https://www.wilsoncenter.org/sites/default/files/deepweb-report_october_2015.pdf. [Accessed 12 April 2020].

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