Received Date: 08 May 2021; Accepted Date: 06 July 2021; Published Date: 11 July 2021

Review on Dark Web and Its Impact on Internet Governance

Diviya Shini Rajamanickam[1*], Mohamad Fadli Zolkipli[2]

[1]*School of Computing, University Utara Malaysia; diviya_shini_raja@soc.uum.edu.my*
[2]*School of Computing, University Utara Malaysia; m.fadli.zolkipli@uum.edu.my*

* *Corresponding author*

To cite this article (APA): Rajamanickam, D. S. & Zolkipli, M. F. (2021). Review on Dark Web and Its Impact on Internet Governance. *Journal of ICT in Education, 8*(2), 13-23. https://doi.org/10.37134/jictie.vol8.2.2.2021

To link to this article: https://doi.org/10.37134/jictie.vol8.2.2.2021

Abstract

Cyber attackers use the Dark Web, a collection of facilities that are not visible to search engines and normal users, to explore a variety of illegal products and services. In this paper, the Dark Web and its impact on internet governance were analysed. The findings of a review of the literature provide in-depth knowledge on the increasing number of crimes committed on the Dark Web, considering the economic, social, along with ethical consequences of cybercrime on the Dark Web, as well as analysing the consequences and methods for locating the criminals, as well as their drawbacks. Fraudsters, militants, and government-sponsored secret agents used the Dark Web where is among the most popular difficult together with unidentifiable channels to achieve their illicit goals. Crimes that were committed on the Dark Web are similar to criminal offenses committed in the real world. Nevertheless, the sheer size of the Dark Web, the unpredictability of the ecosystem, as well as the privacy and confidentiality afforded by Dark Web services, were also critical challenges in tracing criminals. Measuring the yachting Dark Web crime risks is a critical step in discovering alternative approaches to cybercrime. The study reveals that Dark Web services are available to arrest criminals, as well as digital facts and evidence, should be analysed and applied in a way that allows Internet Governance.

Keywords: Dark Web, Internet governance.

INTRODUCTION

There are lots of impacts of the Dark Web on Internet Governance. Besides criminal activities, illegal contents are also used on the Dark Web at a rate of 57%. Illegal drugs, fake currency child pornography, stolen financial details, weapon trafficking, illegal discussions, terrorist communication, and other crimes are common (Beshiri & Susuri, 2019). The secrecy proffered by Dark Web services is amongst the most difficult challenges that forensic examiners face while examining illegal behaviour on the

Dark Web (Chertaff, 2017; Alharbi et al., 2021). Tor, Freenet, I2P, together with JonDonym are unidentified services where it is frequently used the Dark Web's contents and services.

The impacts of the Dark Web on Internet Governance are very huge. This article is presented in this way; Section 2 examines the literature review on the Dark Web. Then Section 3 about cybercrime in the Dark Web. Section 4 the illegitimate activities on the Dark Web. Dark Web and criminal behavior is expressed in Section 5, which is accompanied by internet governance on Dark Web in Section 6. Finally, the conclusion is depicted in Section 7.

THE DARK WEB

The dark web is a network of websites that can only be accessed using a specialised web browser. It's used to keep online activity secret and anonymous, which may be useful in both legal and unlawful situations. The Dark Web is expanding within the Deep Web as new technologies make navigation simpler. Individuals may utilise the Dark Web for a range of legal and criminal activities since they may access it with little chance of being discovered (Nazah et al., 2020; East (2017). However, it is unknown how much of the Deep Web is occupied by Dark Web material and how much of the Dark Web is used for legitimate or criminal purposes. Dark Web sites work properly as a foundation for web clients who value obscurity because they not only protect against unlicensed individuals, but it does include encryption is used to eliminate supervision monitoring (Montieri et al., 2020). The Tor network is a fairly well-known source of Dark Web content. Tor is an unidentified network that can only be accessed by a select few via Tor browser is a highly specialised web browser (Nazah et al., 2020). I2P, another network, offers some of those same beneficial effects as Tor (Montieri et al., 2020). I2P, on the other hand, had been intended to become a platform linked to online. Tor does provide more unknown obtain to a public Internet, while I2P gives a significantly quite resilient and dependable “network within a network”.

Using the Dark Web and Getting Around It

The Dark Web may be accessed using a multitude of decentralised, anonymous nodes, such as Tor (short for The Onion Router) or I2P. Tor was designed by the U.S. Naval Research Laboratory as a tool for anonymously interacting online and was first published as The Onion Routing project in 2002 (Zhang & Chow, 2018).

Tor is a term that refers to both the software you install on your computer to run Tor and the network of machines that handle Tor connections. Users of Tor connect to websites “through a series of virtual tunnels rather than a direct connection, allowing both companies and individuals to communicate information across public networks without jeopardising their privacy.” Users route their web traffic through the computers of other users, making it impossible to trace the traffic back to the originating user (Zhang & Chow, 2018; Davies, 2020). To hide users' identities, Tor creates layers (similar to onion layers) and sends traffic via those layers. Tor has set up "relays" on computers all around the

Received Date: 08 May 2021; Accepted Date: 06 July 2021; Published Date: 11 July 2021

world that let information to flow from one layer to the next. The last relay is known as the "exit relay," and its IP address is used to identify the Tor traffic's origins. Users' IP addresses stay concealed when using Tor software. As a result, it seems that any given website's connection "comes from the IP address of a Tor exit relay, which can be located anywhere on the planet."

While there is no clear statistics on the size of the Deep Web and Dark Web, or how they relate to the Surface Web, there is data on Tor users. According to Tor Project data, the average number of daily Tor users in the United States was 353,753 in the first two months of 2017, accounting for 19.2% of all daily Tor users. The United States has the most average daily Tor users (11.9%), followed by Russia (11.9%), Germany (9.9%), and the United Arab Emirates (9.9%) (Davies, 2020; Omar & Ibrahim, 2020).

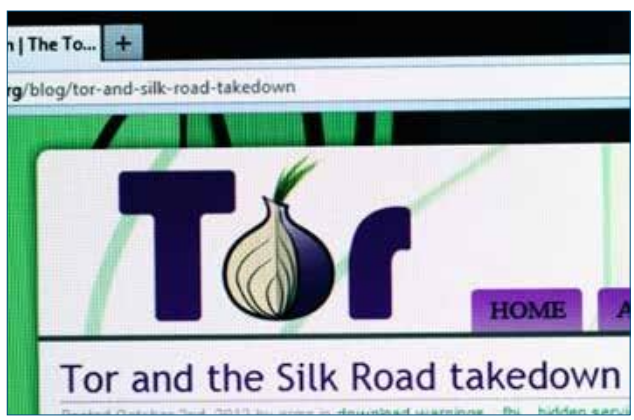

Figure 1: The blog page on the Tor Project website blog page deliberating the FBI's takedown of Silk Road (an online marketplace for contraband drugs, weapons, and narcotics) (Omar & Ibrahim, 2020)

The Dark Web's Main Functions

The dark web's promise of anonymity can be exploited in a variety of ways. Some legitimate reasons include civilians seeking protection from irresponsible corporations, censorship, and the ability to conduct sensitive research without fear; militaries hosting hidden command and control services; journalists conducting operations in countries with limited access to free media and speech; and militaries hosting hidden command and control services, activists and whistle-blowers denouncing injustices and speaking out against governments, as well as law enforcement conducting sting operations (Easttom, 2018). Because of the differences in the legal environment between countries, all of these applications need the usage of the dark web in some countries but not in others.

While not all situations that benefit from anonymity are unlawful by definition, the dark web phenomena do facilitate a significant number of illicit actions. One of these is offering an enabling

infrastructure to adversarial cyber-attacks. Botnet command-and-control endpoints, marketplaces for trading zero-day exploits, hired hackers, private communication, attack coordination, variable-sized botnets for rent to conduct DDoS assaults, and pawning of compromised data are all part of this architecture (Easttom, 2018; Robertson et al., 2017).

Individuals who desire to remain anonymous in the physical world can create a persona, or pseudonym, that they can use across numerous internet platforms. They can maintain a solid and continuous online presence while being physically mobile and always on the go, which may be a required extra step in evading legal prosecution in the real world, especially given industrialised countries' highly collaborative character (Easttom, 2018).

CYBERCRIME IN THE DARK WEB

Criminal activity on the internet will have evolved more accessible to others looking to interact in low-risk criminal activity. DDoS attacks on websites are as simple as having to rent a botnet that gives DDoS-as-a-Service (DDoSaaS) or deploying Ransomware able to infect unwitting perpetrators through phishing emails that involve security flaws links or attachments (Tapor, 2019a). These are the services that allow malicious actors– during this case, script kiddies – to focus on ‘low hanging fruit,' i.e. targets lacking adequate security measures or training. Furthermore, dark nets unknowingly function as a recruiting tool for these young 'hackers' amass knowledge, they will become future law enforcement personnel that a quite underground infrastructure that will eventually become beneficial for the position of a knowledge security specialist; companies are beginning to "hire hackers." (Tapor, 2019b). Tor's confidentiality or even, as a consequence, a complication in being turned off are ideal for C2 server-specific purposes, as indicated by botnet C2 services were among the most recognizable hidden services discovered on the Tor browser.

Nation-states have expressed concern about the necessity to start out preparing for digital warfare and which physical limits prevail pointless during such particular property. This is often especially concerning when this warfare affects Industrial Control Systems (ICS) and Critical Infrastructure (CI), which has the likelihood to have negative real-world consequences (Alkhatib & Basheer, 2019a). This simple entry into the planet of cybercrime is aided further by the asymmetry of the battlefield environment. Despite the very fact that cybercriminals seem to be not also funded or resourced because of the organizations they aim, they need a benefit on the digital battlefield because they will choose their tactic, timing, and site, in contrast to defence must keep an eye out in the least times (Easttom, 2018; Alkhatib & Basheer, 2019b). Deterrence and dissuasion have historically been effective military strategies in warfare for a spread of reasons, one among which is that the elevated barricade to the introduction of atomic warheads. Nevertheless, this doesn't use in virtual worlds because a serious offense is often formatted by humans on the Dark Web or definitely purchased from it (Alkhatib & Basheer, 2019a). Similarly, deterrence is not any longer solely the non-state actors can sometimes become willing members in cyber warfare toward prevalent adversaries, making it the domain of governments.

Received Date: 08 May 2021; Accepted Date: 06 July 2021; Published Date: 11 July 2021

Law enforcement agencies, as well as hacktivist organizations everywhere on the planet, have already been working hard to scale back terrorist groups' activity. This has resulted in their movement to the Dark Web as well as established their behaviour additionally immune to disruption (Alkhatib & Basheer, 2019b). Supporters can now freely express themselves anonymously; much less likely to occur targeted by hacktivists/vigilantes attempting to deactivate terrorism-related websites, and their activities can indeed be funded indefinitely using digital currencies.

ILLEGITIMATE ACTIVITIES ON THE DARK WEB

The Dark Web is the epicentre of criminal attacks because it provides anonymity and serves as a gateway to the criminal world (Godawatte, Raza, Murtaza, & Saeed, 2019). The following are some of the most well-known crimes that take place on the Dark Web:

a) Proxying

Users of Tor-like systems are vulnerable to assault because of their anonymity. The customary 'HTTPS' in the URL of this site does not appear, indicating that it is secure. They must bookmark the TOR page to ensure they are on the legitimate site. When a fraudster uses website proxying, the user is tricked into believing he is on the current source, and the fraudster then re-edits the link to send the user to his scam URL. When a user pays in bitcoin, the money is therefore sent to the fraudster.

b) Drug tracking

The dark web is an unlawful marketplace for the sale of illegal and hazardous substances in return for crypto currency. Bit currency, Ethereum, and ripple are just a few examples. The United States Police took down the dark web's largest dark net bazaar, which was founded by a Canadian. Silk Road was also a well-known marketplace for unlicensed medicines and illicit substances. The FBI took down this website in 2013. Agora is a website that was shut down last year as well. Alpha Bay is now the world's largest drug marketplace. Drug marketplaces include Dream Market, Valhalla, and Wall Street Market, among others.

c) Information leakage

Many anonymity-supporting systems, such as TOR, are important tools for whistle-blowers, activists, and law enforcement. Hackers use the Dark Web to spread sensitive information. On the black web, a hacking gang once uploaded the credit card details and logins of about 32 million Ashley Madison clients as a 9.7GB data dump. Likewise, in 2017, approximately 1.4 billion personal records were exposed on the dark web as plain text, which was accessible on the internet. Workers are paid to disclose business data via dark web hubs as well.

d) Human tracking

Human trafficking takes happen at Black Death, a dark web location. The British model Chloe Ayling is one of the human trafficking on the Dark Web. According to a 2017 research, the majority of human

trafficking victims were recruited for sex and labour trafficking. The Dark Web, according to some accounts, has aided in the concealment of this crime. Black Death is a dark web group that changes URLs regularly.

e) Child Pornography

Child pornography drives the highest traffic to TOR's hidden sites, according to the report. Finding such sites is difficult for the typical user. It occurs when children are used for sexual arousal and when minors are abused during sexual actions. It also contains kid pornographic sexual pictures. Lolita City, a site that had about 15,000 users and had over 100GB of child pornography images and videos, has officially been taken down. The FBI shut down PLAYPEN in 2015, which had over 200,000 users and may have been the largest child pornography site on the dark web.

f*) Frauds*

Theft and sale of a user's credit card details and confidential info are referred to as carding frauds. On the Dark Web, this is the most frequent form of criminal activity. There are many factors that contribute to the popularity of this scam on the Dark Web. Credit and debit cards are sold on dark net markets. The user is sent to the similar page by numerous URLs on these sites. Vendors from numerous forums publish classified advertisements describing their wares. A live chat feature is available on the various forums. Cards are sold at a cheaper cost by vendors. Carding fraud is also a possibility on several money transfer sites.

DARK WEB AND CRIMINAL BEHAVIOUR

On the Deep Web and Dark Web, malicious conduct is just as possible as it is on the Surface Web. From thieves to terrorists to state-sponsored espionage, cyberspace is used by a wide spectrum of bad actors. The internet may be used as a platform for discussion, cooperation, and action. They may rely on the Dark Web in particular to enable them carry out their operations with less danger of detection (Rafiuddin, Minhas & Dhubb, 2017). While the concerns discussed in this section are specific to cybercriminals, they are definitely applicable to other types of harmful actors.

Criminals in the twenty-first century increasingly rely on the Internet and modern technologies to carry out their illegal activities. Criminals, for example, may simply use the Internet to carry out classic crimes like drug distribution and sex trafficking. Furthermore, they use the digital realm to enable crimes that are frequently technological in nature, such as identity theft, credit card fraud, and intellectual property theft. High-tech crimes are among the most serious crimes facing the United States, according to the FBI.

The Dark Web has been blamed for supporting a wide range of criminal activities. Drugs, guns, exotic

Received Date: 08 May 2021; Accepted Date: 06 July 2021; Published Date: 11 July 2021

animals, stolen items, and data are all sold illegally for profit. Gambling sites, hired thieves and assassins, and troves of child pornography are all available. However, there is a scarcity of information about how common these Dark Web sites are (Rafiuddin, Minhas & Dhubb, 2017; [17, 18]. Only approximately 1.5 percent of Tor users, according to Tor, browse secret services or Dark Web pages. It's unknown what percentage of sites serve a specific illegal market at any one moment and even less so how much Tor traffic goes to any individual site.

- Tor traffic to secret services was investigated by a University of Portsmouth research. Researchers "ran 40 'relay' machines in the Tor network, allowing them to gather an unparalleled collection of data on the total number of Tor hidden services online approximately 45,000 at any given moment and how much traffic flowed to them," according to the study. While child abuse sites accounted for approximately 2% of the Tor hidden service domains discovered, they accounted for 83 percent of all visitors to hidden service sites. "Just a tiny handful of paedophilia sites account for the bulk of Dark Web http traffic," according to the researchers (Rafiuddin, Minhas & Dhubb, 2017). However, as previously said, the results might have been impacted by a number of factors.

- Another research from King's College London looked at the Tor network's hidden services. They utilised a web crawler to find 5,205 active websites, starting with two famous Dark Web search engines, Ahmia and Onion City. Researchers detected material on almost half of the 5,205 websites (2,723) and categorised them based on the type of information. Researchers discovered 1,547 websites with illegal content. This is a sampling of Tor hidden service websites; the crawler used by the researchers viewed over 300,000 websites (containing 205,000 distinct pages) on the Tor hidden service network (Rafiuddin, Minhas & Dhubb, 2017; Yang et al., 2019). Notably, Tor projected in 2015 that around 30,000 hidden services "announce themselves to the Tor network every day." Tor also estimates that "hidden service traffic accounts for around 3.4 percent of overall Tor traffic." According to more current statistics from March 2016 to March 2017, daily hidden services, or unique.onion addresses, averaged between 50,000 and 60,000.

The Dark Web may be used for a variety of nefarious purposes. As previously stated, it may be used as a platform for organising and coordinating crimes via chat rooms and communication services. For example, there have been claims that some tax-refund fraudsters shared their methods on the Dark Web (Yang et al., 2019).

- On the Dark Web, malware used in large-scale data breaches to acquire unencrypted credit and debit card information was purchased. RAM scrapers, for example, are a type of malware that can be purchased and remotely placed on point-of-sale systems, as was done in the 2013 Target hack and others.

- On the Dark Web, thieves may make money by selling stolen data. For example, within weeks of the Target data breach, underground black markets were reportedly "flooded" with stolen credit and debit card account information, which was "sold in batches of one million cards and

going for anything from $20 to more than $100 per card." The specialised marketplaces on the Dark Web include places like these "card stores."

- Data can not only be stolen and sold on the Dark Web, but it can also be done rapidly. Researchers from security firm BitGlass generated a treasure mine of false "stolen" data in one experiment, including over 1,500 names, social security numbers, credit card information, and more. They then uploaded the information to DropBox and seven well-known black market websites. The data has been accessed roughly 1,100 times in 22 countries in only 12 days.

Cybercriminals may target both persons and businesses, and they do it without regard for national borders. Law enforcement faces a constant problem in determining how criminals exploit borders, especially since the idea of borders and limits has developed [29, 20].

a) Physical Limits

Jurisdictional boundaries have been created between nations, states, and other localities for law enforcement purposes. Various law enforcement authorities have been given jurisdiction to administer justice inside certain regions. When crimes transcend jurisdictional lines, a single organisation may no longer be solely responsible for criminal enforcement, and laws may not be uniform across jurisdictions. These phenomena have long been known and exploited by criminals.

b) Physical Cyber Borders

The physical world's relatively obvious bounds are not always reproduced in the virtual world. High-speed Internet connection has aided criminals' skills to operate in an atmosphere where they may widen their pool of prospective targets and quickly exploit their victims. Frauds and scams that were formerly carried out in person can now be carried out remotely from across the nation or even the globe. Botnets, for example, allow thieves to target victims all over the world without ever having to cross a single border.

c) Cyber Borders

While cyberspace has no physical borders, it does have jurisdictional and technological limits. Some web addresses, for example, are country-specific, and their administration is under the jurisdiction of individual countries. The boundaries between the Surface Web and the Deep Web are another cyberspace barrier. Subscriptions or paid access to certain website content may be required to cross these limits. Some business news sites, magazines, file-sharing platforms, and other resources may charge for access. Other sites require an invitation to access.

Is the Dark Web required or beneficial for bad actors to carry out their activities? Researchers have identified the benefits and drawbacks of depending on the Dark Web's anonymity. Criminals selling illegal items may profit from the Dark Web's enhanced anonymity in order to better elude law

Received Date: 08 May 2021; Accepted Date: 06 July 2021; Published Date: 11 July 2021

enforcement (Schäfer et al., 2019; Kadoguchi et al., 2019). They may, however, have more difficulty obtaining business. According to Trend Micro's Dark Web report, "sellers suffer from a loss of reputation induced by greater anonymity." Being untraceable has disadvantages for a vendor who can't readily build a trust connection with consumers unless the marketplace enables it." In other words, if you're attempting to sell anything online and haven't been verified, anonymity might be a hurdle (Kadoguchi et al., 2019).

INTERNET GOVERNANCE ON DARK WEB

The government's strategies for controlling the Dark Web must be defined. These should be defined in such a manner that illegal behaviour on the Dark Web is prohibited and the anonymity of legitimate users is preserved to the fullest extent possible. Different government agencies' skills can be included along to implement Dark Web regulations (Zhang, Ebrahimi, Li, & Chen, 2020). The FBI uses the Computer and Internet Protocol Address Verifier (CIPAV) to track down suspects who used anonymity services or proxy servers to hide their location. It distinguishes between ordinary Internet traffic and TOR traffic. It aids the FBI in narrowing down the scope of any inquiry. The Department of Defense's Defense Advanced Research Projects Agency (DARPA) has created a programme called "Memex" that discovers patterns to identify unlawful behavior. Rather of revealing all types of individuals, it simply exposes suspicions based on certain characteristics (Ferry et al., 2019). The FBI also utilised a hacking tool to track down the IP addresses of those who were using Playpen, a secret Tor child abuse site.

As a result, legislative structures that assist illegal researches are necessary. A variety of instances have been reported in the literature, spanning the range from ineffective to effective enforcement. There will be a need to put in place a solid legal framework that government entities at both the national and international levels can use to undertake effective inspections. For the proper governance of the Dark Web, the following aspects must be supervised (Zhang, Ebrahimi, Li, & Chen, 2020; Ferry et al., 2019):

1. *Customer Data Monitoring.* Because there is no method for user tracking, top-level domains are tracked using destination queries. Because the endpoints of web requests must be watched, this may be done without invading users' privacy. The FBI, for example, has specific capabilities for investigating Carnivore (software that monitors email and electronic communication) from 1997 and earlier.
2. *Semantic Analysis.* A record of concealed site activity and records must exist.
3. *Monitoring of Social Sites.* This involves tracking down cryptographic functions about some of the most prominent social media platforms.
4. *Hidden Services Surveillance*. The agencies must record ("snap-shot") the new services or sites for subsequent study before they vanish or reappear under a different name.

5. *Marketplace Profiling*. There ought to be a system in place to trace vendors, purchasers, and middle brokers that engage in unlawful activity. So that one may figure out what actions a specific customer has already been participating in.
6. *Mapping the hidden services directory*. In TOR, the database is hidden via the distributed hash table method. The deployed nodes might keep track of the nodes and map them.

CONCLUSION

The dark web is a section of the Internet where people go to perform things in secret and leave no evidence. It has now become a center for illegal operations such as child pornography, weapons trafficking, drug smuggling, and onion cloning, among others. The anonymity afforded by this site is the major driving force behind these operations. The ransom payment is obtained in the form of bit currency through the Dark Net in a number of assaults performed on this site. For the sake of confidentiality, it is also utilised by governments of many nations. A summary of the various Dark Web assaults, exploits, browsers, and crimes. It may be argued that the benefits and drawbacks of the Dark Web are determined by the user's objectives.

The deep Web and particularly Dark Web networks like Tor present a viable means for unscrupulous people to facilitate trade in an anonymous manner whether legally or illegally. The absence of observable activity in unconventional Dark Web networks doesn't necessarily imply their absence. In fact, the operations are simply harder to spot and observe, in accordance along with guiding that underpins the Dark Web.

ACKNOWLEDGEMENT

The authors would like to thank all School of Computing members who involved in this study. This study was conducted for the purpose of the System and Network Security Research Project. This work was supported by the Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

REFERENCES

Alharbi, A., Faizan, M., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2021). Exploring the topological properties of the Tor Dark Web. *IEEE Access, 9*, 21746-21758. https://doi.org/10.1109/ACCESS.2021.3055532

Alkhatib, B, & Basheer, R. (2019a). Mining the Dark Web: A novel approach for placing a Dark Website under investigation. *International Journal of Modern Education and Computer Science*, *11*(10), 1-13. https://doi.org/10.5815/ijmecs.2019.10.01

Alkhatib, B., & Basheer, R. (2019b). Crawling the Dark Web: A conceptual perspective, challenges and implementation. *Journal of Digital Information Management, 17*(2), 51-60. https://doi.org/10.6025/jdim/2019/17/2/51-60

Beshiri, A., & Susuri, A. (2019). Dark Web and its impact in online anonymity and privacy: A critical analysis and review. *Journal of Computer and Communications. 7*. 30-43. https://doi.org/10.4236/jcc.2019.73004

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy. 2*. 1-13. https://doi.org/10.1080/23738871.2017.1298643

Davies, G. (2020). Shining a light on policing of the Dark Web: An analysis of UK investigatory powers. *The Journal of Criminal Law*, *84*(5), 407–426. https://doi.org/10.1177/0022018320952557

East, C. S. (2017). Demystifying the Dark Web. *ITNOW*, *59*(1), 16-17. https://doi.org/10.1093/itnow/bwx007

Easttom, C. (2018). Conducting investigations on the Dark Web. *Journal of Information Warfare*, *17*(4), 26-37. https://doi.org/doi:10.2307/26783825

Ferry, N., Hackenheimer, T., Herrmann, F., & Tourette, A. (2019, June 27-29). Methodology of dark web monitoring, ECAI 2019: Pitesti, Romania. https://doi.org/10.1109/ECAI46879.2019.9042072

Godawatte, K., Raza, M., Murtaza, M., & Saeed, A. (2019, Dec 5-7). *Dark Web along with The Dark Web marketing and surveillance* [Paper presentation]. PDCAT 2019: Gold Coast, Australia.

Kadoguchi, M., Hayashi, S., Hashimoto, M., & Otsuka, A. (2019, 1-3 July). Exploring the Dark Web for cyber threat intelligence using machine leaning. ISI 2019: Shenzhen, China. https://doi.org/10.1109/ISI.2019.8823360

Montieri, A., Ciuonzo, D., Bovenzi, G., Persico, V., & Pescapé, A. (2020). A dive into the Dark Web: Hierarchical traffic classification of anonymity tools. *IEEE Transactions on Network Science and Engineering*, *7*(3), 1043-1054. https://doi.org/10.1109/TNSE.2019.2901994

Nazah, S., Huda, S., Abawajy, J, & Hassan, M. M. (2020). Evolution of Dark Web threat analysis and detection: A systematic approach. *IEEE Access*, *8*, 171796-171819. https://doi.org/10.1109/ACCESS.2020.3024198

Omar, Z. M., & Ibrahim, J. (2020). An overview of Darknet, rise and challenges and its assumptions. *International Journal of Computer Science and Information Technology*, *8*(3), 110-116.

Rafiuddin, M. F., Minhas, H., & Dhubb, P. S. (2017, Sept 21-22). A Dark Web story in-depth research and study conducted on the dark web based on forensic computing and security in Malaysia. IEEE ICPCSI 2017: Chennai, India. https://doi.org/10.1109/ICPCSI.2017.8392286.

Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Darkweb cyber threat intelligence mining. *Journal of Computer Science and Information Technology*, *15*(2), 28-43. https://doi.org/10.1017/9781316888513

Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019, 28-31 May). BlackWidow: Monitoring the Dark Web for cyber security information. CyCon 2019: Tallinn, Estonia. https://doi.org/10.23919/CYCON.2019.8756845

Topor, L. (2019a). Dark Hatred: Antisemitism on the Dark Web. *Journal of Contemporary Antisemitism*, *2*, 25-42. https://doi.org/10.26613/jca/2.2.31.

Topor, Lev. (2019b). Dark and Deep Webs-Liberty or Abuse. *International Journal of Cyber Warfare and Terrorism*, *9*, 1-14. https://doi.org/10.4018/IJCWT.2019040101.

Yang, Y., Yang, L., Yang, M., Yu, H., Zhu, G., Chen, Z., & Chen, L. (2019, May 24-26). Dark Web forum correlation analysis research. ITAIC 2019: Chongqing, China. https://doi.org/10.1109/ITAIC.2019.8785760

Zhang, N., Ebrahimi, M., Li, W., & Chen, H. (2020, Nov 9-10). A generative adversarial learning framework for breaking text-based CAPTCHA in the Dark Web. ISI 2020: Arlington, VA, USA. https://doi.org/10.1109/ISI49825.2020.9280537

Zhang, X., & Chow, K. (2018). A framework for Dark Web threat intelligence analysis. *International Journal of Digital Crime and Forensics (IJDCF)*, *10*(4), 108-117. http://doi.org/10.4018/IJDCF.2018100108