Understanding the Impact of the Dark Web on Society: A Systematic Literature Review

[1]Sushil Kumar Pradhan; [1]B.K.N Satapathy, [2]Dayal Krushna Sahoo

[1]Assistant Professor, MBA, Gandhi Institute of Technology & Management, Bhubaneswar

[2]StudentGandhi Institute of Technology & Management, Bhubaneswar

Abstract

The dark web is considered an expansion of the deep web, intentionally hidden from the surface web. It can only be accessed with a particular group of browsers that allow the user to stay anonymous while navigating the dark web. With the untraceable hidden layer of the Internet and theanonymity of the users associated with the dark web, several impressive cybercrimes have been reported. This paper aims to examine the impact of the dark web on society. The article systematically reviews relevant academic literature and books to understand how the dark web works and its societal effects. The study has found that the dark web is an enabler of several cybercrimes. Moreover, while governments and regulatory authorities have introduced strategic detection techniques on the dark web, cybercriminals are adaptive towards the strategies and, giventime, will usually find ways to bypass such detection techniques. It is recommended that the regulatory authorities and cyber threat intelligence periodically review the detection techniques foreffective monitoring. Furthermore, security agencies or forensic analysts should ensure that they are updated with the latest scientific knowledge on the safe management of the dark web by undertakingmore training in cyber security. There is also a need for further research to focus on awareness campaigns about the dangers of the dark web.

Keywords: Cybercrime, Dark Web, Internet, Tor, Society.

Introduction

The Internet has three levels: the surface web, the deep web, and the dark web (Figure 1). The surface web is the most well-known portion of the Internet, indexed in standard web browsers and readily available to the general public (Gupta, Maynard & Ahmad, 2019; Odendaal, Hattingh & Eybers, 2019). The deep and dark web is the unindexed Internet portions inaccessible to a standard search engine (ibid). The deep and dark web holds approximately 96% of the Internet (Upulie & Prasanga, 2021). According to Hayes, Cappa and Cardon (2018),the dark web is a subset of the deep web that can only be accessed using a unique tool such as garlic, tunnel, or onion routing (Tor). Tor browser is the most widely used network, which is user-friendly and protects users' anonymity, especially for individuals seeking to overcome censorship (Aceto & Pescapé, 2015; Gupta et al., 2019). In addition, Tor ensures individual privacy, including for criminals who seek to obfuscate their identity (Broséus, Rhumorbarbe, Mireault, Ouellette, Crispino & Décary-Hétu, 2016; Jardine, 2018).

According to Hayes et al2018, p. 1), "Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security."Because of the effect of these crimes on individuals, governments, and business owners, efforts are taken by cyber threat intelligence to make cybersecurity a top priority to guide against malicious activities emanating from the dark web. However, while measures have been taken by cyber threat intelligence to monitor the hidden services on the dark web, the criminalactivities performed on this site are still on the increase. Scholz (2016) attributed the success ofthe dark web to its protection of users' privacy, which is essential to both privacy-conscious citizens and criminals. According to Nazah et al. (2020), security agencies are yet to find a wayto track cybercrimes on the dark web without infringing on people's rights to privacy. This makes the dark web powerful enough to harbor illegitimate malicious activities performed on this site, consequently increasing cybercrimes. Hence, it is essential to

investigate the effect ofthe dark web and its role in promoting cybercrime. With this investigation, the study will be able to provide recommendations on how to curb the security concerns associated with the dark web. Thus, the research study systematically reviewed relevant academic literature and books to understand the dark web.associated with the dark web be addressed?

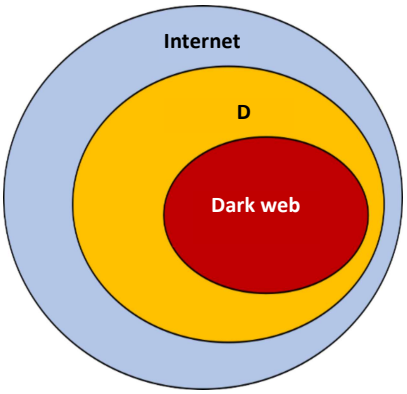


Figure 1: The Surface, Deep, and Dark Web (Odendaal et al., 2019)

The paper is structured as follows. Section 2 discusses the research methodology employedfor the study. Section 3 presents the findings of this study as it relates to the research questions.Section 4 provides an in-depth discussion of the results based on the evidence presented in Section 3, thus expanding the frontiers of knowledge on the impact of the dark web on society.

Materials and Methods

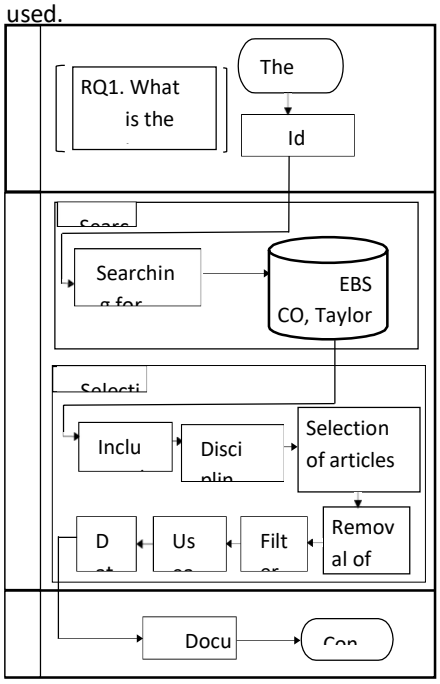
The researchers conducted a systematic desktop review of the effect of the dark web and its role in promoting cybercrime. A systematic review uses systematic methods to collect, analyze, and interpret secondary data accordingly (Eichler & Schwarz, 2019). Systematic reviews are characterized by a methodical and replicable analytical approach synthesizing data directly related to the systematic review question (Mallett, Hagen-Zanker, Slater & Duvendack, 2012). This process was preferred because it allowed the researchers to collect and summarize current evidence concerning the dark web. It was then analyzed and used to inform how securityagencies could further govern the dark web to secure society. According to Stapic, López, Cabot, de Marcos Ortega and Strahonja (2012), there are guidelines for a systematic literature review (SLR), which include planning, conducting, and reporting the review. These guidelines were followed in answering the study questions and developing the review procedure (Figure 2). In the first phase (i.e., planning), the research questions were identified, and the need for the study was established. In the second phase (i.e., conducting the review), as indicated in Figure2, the search strategy was done by accessing several search indices such as EBSCO, Google Scholar, and Scopus to identify relevant articles covering topics such as dark web, Tor and cybercrime, to name a few. The papers extracted were recent ones that were published before September 2022.

Inclusion and Exclusion Criteria

The selection process, which is also part of the second phase (conducting the review) as indicated in Figure 2, was based on the subject area of our search, and it was limited to disciplines such as computer science, information systems, ICT, and multidisciplinary.

Source: Authors' own

Those that did not meet the criteria were excluded. Likewise, articles such as editorials, abstracts, and comments that were not original research were excluded (refer to Figure 3), andthose not written in English. Proceedings, which yielded 314 papers. At stage 2, paperswere excluded based on title and keywords, which produced 144 papers. Also, at stage 3, paperswere excluded based on abstracts, prefaces, non-English comments, and editorials, which yielded 103 papers. In stage 4, each of the 103 papers was read entirely through, and 67 paperswere obtained and used.



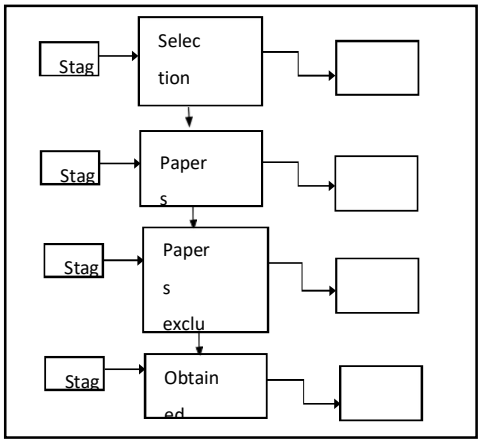


Figure 3: Stages of Selection

Figure 4 presents the distribution of the reviewed research papers by year. It shows the number of papers on the phenomenon of the dark web over the past few years. A significant number of articles (44 out of 67), representing 65.64%, were published between 2017 and 2022.A further 34.39% were published between 2016 and 2012. As shown in Figure 4, 2017 has thehighest report of the dark web, mainly devoted to cybercrime, ranging from human traffickingto terrorism. From the year 2018 to 2019, there was a slight decrease in reports. However, in 2020, there was a rise in reports, but it slightly declined in 2021. In 2022, there is a gradual increase in reports of the dark web. With this gradual increase, it is essential to investigate the dark web's effect on society and its role in promoting cybercrime.

Data Extraction and Synthesis

Two independent researchers were consulted to extract data from the selected research papers based on the criteria given, as follows:

- Does the paper address the dark web phenomenon and its impact on society?
- Does the paper discuss how the security concerns associated with the dark web can be addressed?

The data extracted by the two researchers were compared, and their mismatches were discussed and resolved through mutual consensus. Mallett et al. (2012) state that "disparities in studies such as this can be minimized by mutual agreement among the researchers involved inthe study who review their codes to ensure their consistency and relevance." The data were then synthesized using the core themes identified. Thematic synopsis was crucial in examining the dark web phenomenon and its impact on society.

Results

This section presents a detailed explanation of the data extracted from the reviewed research papers (the presentation of the findings represents the third phase of SLR methodology,as indicated in Figure 2). It synthesizes the literature by putting forward different situational contexts and discussing the impact of the dark web on society and how the security concerns associated with it can be addressed. Table 2 presents the mapping of each reviewed paper as itrelates to significant applications of the dark web. Table 3 presents the mapping of cybercrime activities conducted on the dark web, and Table 4 shows the mapping of techniques to addressthe security concerns associated with the dark web. Recommendations are provided on how security agencies could further govern the dark web to secure society.

Major Applications of the Dark Web

The anonymity features of the dark web open it up to legitimate and illegitimate uses. Communicating anonymously or using pseudonyms allows people to express themselves withlittle to no boundaries (Upulie & Prasanga, 2021). Gupta et al. (2019) have identified the significant applications of the dark web, including recruitment, anonymous marketplace (illegal content), cybercrime, illegal financial services, and cyber threat intelligence, as indicated below:

(i) Anonymous Marketplace: Anonymous online markets, which can also be described as "dark web marketplaces", have emerged, making it quite difficult for law enforcement to identify buyers and sellers (Christin, 2013; Vyas, Vyas, Chauhan, Rawat, Telang & Gottumukkala, 2022). These anonymous online markets, such as Silk Road, the Armory, BlackMarket Reloaded, or the General Store, often specialize in "black market" goods, which includeillicit drugs, pornography, stolen identities, stolen credit card details, or narcotics (Ablon, Libicki &

Golay, 2014; Christin, 2013; Gupta et al., 2019; Rhumorbarbe, Werner, Gilliéron, Staehli, Broséus & Rossy, 2018). According to Christin (2013), as cited by Gupta et al. (2019,

p. 5), "Silk Road was one of the first major anonymous online markets reaching sales of over USD 1.2 million per month.

(ii) Recruitment: The dark web allows for anonymous communication, including recruitment (Gupta et al., 2019; Weimann, 2016). Terrorists or Cybercriminals and OrganizedCrime Groups (OCG) can conduct recruitment and training, spread their ideology, fundraise, advertise, and form communities without concern for a local leader or geographical separation

(Brynielsson, Horndahl, Johansson, Kaati, Mårtenson & Svenson, 2013; Gupta et al., 2019; Scanlon & Gerber, 2014). People are recruited on the dark web to complete tasks that facilitateonline crimes. According to Gupta et al. (2019, p. 5), "Due to the extensive use of dark web forums for such purposes, they have been the target for various forms of monitoring ranging from manual observation to crawling combined with natural language processing techniques for automated threat intelligence and various other insights."

(iii) Cybercrime: Cybercriminals benefit from the dark web's anonymous features tocommit a malicious crime. For example, ransomware that requires the hacker's skill to implement can now be bought and deployed through the dark web (Ablon et al., 2014; Gupta et al., 2019; Topor, 2019). Likewise, DDoS attacks requiring several collaborators' input have been made simple by hiring a botnet to implement a DDoS as a Service (DDoSaaS) on a givennetwork (Chawki, 2022). The dark web motivates young hackers to get involved and earn money (Kaur & Randhawa, 2020; Topor, 2019). Other forms of cybercrimes carried out on the dark web include money laundering (Bryans, 2014), contract murder/kidnapping (Taleby Ahvanooey, Zhu, Mazurczyk, Kilger & Choo, 2022), drug trafficking (Bertola, 2020), and human trafficking (Kaur & Randhawa, 2020).

(iv) Cyberthreat Intelligence: Law enforcement agencies regularly monitor dark web activities, including cybercrime (Basheer & Alkhatib, 2021; Elmellas, 2016). This surveillance could include performing sting operations where a person is caught undercover or maintaining anonymous tip lines. Anti-virus and other security organizations protect their users from malware based on signatures derived from past attacks (Gupta et al., 2019; Samtani Chinn, R.,Chen, H. & Nunamaker, 2017). Likewise, some individuals protect their systems using an intrusion defense system/intrusion protection system (IDS/IPS). In addition, Information Security Risk Management (ISRM) has integrated a more proactive approach to security, and it includes Situation Awareness (SA) (Gupta et al., 2019; Webb, Ahmad, Maynard & Shanks, 2014). This SA enables data collection and processing, which can help manage security (Webbet al., 2014).

In summary, this section presented an insight into the five major applications of the dark web from the selected articles. More importantly, identifying these major applications enables

this study to quickly investigate the impact of the dark web on society and the possible solutions to address security concerns. The five significant applications have been summarized in Table2 as follows:

The Impact of the Dark Web on Society (RQ1)

There are different arguments about the societal impacts of the dark web (Jardine, 2018; Kaur & Randhawa, 2020). Some have argued that the dark web ensures individual privacy, which is essential to privacy-conscious citizens and could be considered a positive benefit (Odendaal et al., 2019; Samtani et al., 2017). Others believe the privacy and anonymity provided by the dark web is an avenue for illegal activities, which can be considered a negativeconsequence (Odendaal et al., 2019; Weimann, 2016). According to Mador (2021, p. 6), "muchof the dark web is devoted to cybercrime, from sharing techniques and tools to selling stolen data and credentials." Kaur and Randhawa (2020) state that the dark web is a marketplace for criminals as the dark web generates $500,000 per day. In addition, people hire hackers from the dark web to break into university systems and change grades (Kaur & Randhawa, 2020). This has impacted society negatively as most criminals rely on the dark web to perpetrate crimes, ranging from illegal drugs to stolen passwords and data (Odendaal et al., 2019). Dealing with malware is another prominent fraudulent activity on the dark web. It is used in large-scale data breaches to obtain unencrypted financial details (Weimann, 2016). This implies that the effect of the dark web on society is a rise in cybercrime activities. This study identified eight majocybercrime activities on the dark web, which helps to answer RQ1. These cybercrimes include drug trafficking, kidnapping/murder, human trafficking, firearms/weapons procurements, money laundering, contract hacking services, terrorism, and ransomware attacks

(i) Drug Trafficking: The dark web has offered opportunities for drug entrepreneurs to introduce a new paradigm on the link between vendors and buyers

of drugs (Bertola, 2020; Broséus et al., 2016). Furthermore, drug entrepreneurs create new business models and tap into a new consumer base while reducing many risks associated with offline markets (e.g., violence). The trade of illicit drugs is the stronghold of most dark web markets: most of the activities on the dark web are drug-related (Bertola, 2020; Me & Pesticcio, 2018). It is estimated that 57% of dark web market listings offer drugs (Bertola, 2020; Soska & Christin, 2015). Drug trade viacrypto markets on the dark web represents a new form of trafficking, providing a new channelfor drug flow across locales (Aldridge & Decary-Hétu, 2015; Bertola, 2020). Researchers increasingly believe decentralized networks offer the bulk of various drug markets (Bertola, 2020; Duxbury & Haynie, 2018).

(ii) Kidnapping/Murder: Many dark websites exist that allow individuals to pay in cryptocurrency, such as Bitcoin, as a form of payment in real-world kidnapping (Jin et al., 2022; Melsky, 2019; Taleby Ahvanooey et al., 2022). Likewise, the dark web allows a person to hirea hitman to murder another person (Besenyő & Gulyas, 2021; Zhou et al., 2020) . For example,in May 2016, a White-hat hacker named "bRpsd" reportedly helped the Federal Bureau oInvestigation (FBI) to arrest some hitmen by hacking into the "Besa Mafia" site on the dark web and revealing contract information, which included client messages, user accounts, and other information. According to Taleby Ahvanooey et al. (2022, p. 4), "this hidden website provided a link between hitmen and clients. The price of a murder service reportedly ranged between $5,000 and $200,000". In addition, a contractor could also be hired to mug instead ofmurder the victim (Lee et al., 2019).

(iii) Human Trafficking: Like other criminal activities, the dark web provides an anonymous marketplace for human trafficking services, including sex trafficking or organ trade (Burbano & Hernandez-Alvarez, 2017; Taleby Ahvanooey et al., 2022). According to Kaur and Randhawa (2020), most traffickers utilize tools such as encryption. They continually switch between sites and profiles on the dark web to avoid being monitored or tracked by law enforcement agencies. In 2019, the US State Department reported 118,932 victims of human trafficking (Taleby Ahvanooey et al., 2022). However, only 9,568 were successfully convicted out of 11,841 traffickers that were prosecuted (Taleby Ahvanooey et al., 2022).

(iv) Illegal Firearms/Weapons Procurement: The dark web has been abused to facilitate theprocurement of firearms/weapons (Taleby Ahvanooey et al., 2022). Illegal firearms can easily be bought on the dark web using cryptocurrencies as the payment method (Copeland et al., 2020; Revell, 2017). These firearms have been abused as terrorists use them to perpetrate crimesin society (Hayes et al., 2018). A study conducted on the international firearms trade by RANDEurope in 2017 reveals that dark web services have reportedly increased the accessibility of weapons for the same prices as on the black market on the street (Taleby Ahvanooey et al., 2022).

In summary, this section answered RQ1 by identifying eight significant cybercrime types of activities on the dark web. It has also been established that the dark web provides an untraceable functionality that enables these cybercriminals. According to Upulie and Prasanga (2021), these cyber criminals often use the dark web under cover of anonymity for discussion and illegal business transactions. He, He & Li (2019, p. 73) affirm that "providers of illegal services use the dark web to publish illegal content to evade network law enforcement becauseof the difficulty of locating their real IPs, which makes the abuse of the dark web more and more serious". It is important to note that these criminals might target vulnerable individuals or businesses without national borders to gain profit (Gupta et al., 2019).

Techniques to Address the Security Concerns Associated with the Dark Web (RQ2)

According to Nazah et al. (2020), tracking cybercrime on the dark web can be difficult dueto the decentralized nature of the platform. These challenges are further exacerbated because ofthe anonymity dark web services provide. This anonymity is one of the significant difficulties some cyber threat intelligence, law enforcement, or forensic analysts may face while investigating criminal activities, as they may infringe on individuals' privacy rights. However,this study has identified crime detection studies on the dark web to discover the criminals or the crimes. This section briefly discusses some detecting techniques and methods applied for this purpose. These techniques include law enforcement, cryptographic hash functions, memex tools, sock puppet detection, honeypot deployment, and classification of networks. This sectionanswers RQ2 as summarized in Table 4.

(i) Law Enforcement**:** Governments or regulatory organizations have some laws that regulate and monitor user activities on the dark web (Ghappour, 2017; Hayes et al., 2018). These laws, such as regulatory, civil, and criminal law, are related to criminal activities on thedark web (Dalins et al., 2018; Kavallieros et al., 2021; Nazah et al., 2020). Criminal law relatesto crimes at the government level of federal, state, and local (e.g., drug trafficking, murder, or money laundering). The type of penalty could be a fine, life imprisonment, or the death penalty, depending on the state in which the crime is

committed (Cole et al., 2021). Civil law relates toorganizations or individuals instructed to pay a fine or complete a service as part of the punishment. In regulatory law, the agency within a jurisdiction can issue penalties as punishment for illegal activities.

(ii) Cryptographic Hash Functions: Monitoring social sites on the dark web involves tracingcryptographic hash functions (Biswas et al., 2017; Singh et al., 2022). Hash functions producevalues representing the original message from which they have been computed (Kheshaifaty &Gutub, 2020). In investigations, the cryptographic hash functions are essential to prove that allevidence is genuine (Kheshaifaty & Gutub, 2020; Nazah et al., 2020). Some popular hash algorithms are SHA-512, SHA-256, and SHA-1, MD5 (Nazah et al., 2020). These cryptographic hash functions could help regulatory organizations gain governance over the darkweb more precisely.

(iii) Memex Tools: The Defense Advanced Research Projects Agency (DARPA) developeda suite of tools known as Memex for law enforcement agencies to help identify criminal operations on the dark web (Ehney & Shorter, 2016; Mattmann, 2015; Nazah et al., 2020). According to Nazah et al. (2020), US law enforcement uses Memex and the Metasploit Decloaking Engine tool to intelligently index deep websites to identify criminals on the dark web, especially human traffickers. These tools are primarily written in Python and were developed in collaboration with various universities (Hammonds, 2015; Heinl et al., 2019).

(iv) Sock Puppet Detection: Sock puppets are false online identities used for deception (Maity et al., 2017). Cybercriminals mainly use this method to steal identities, engage in terrorist activities, and sell fake products on the dark web (Maity et al., 2017). Thus, sock puppetdetection allows cyber intelligence operations to perform forensic accounting, extrapolate information about criminals, monitor communications, and scrutinize terrorist pursuits on the dark web (Nazah et al., 2020; Sönmez & Seçkin Codal, 2022). Several studies have used authorship identification to detect sock puppets on online social sites (Bu et al., 2013; Kumar, Cheng, Leskovec and Subrahmanian, 2017; Liu et al., 2016; Spitters et al., 2015).

Conclusion

As discussed in this study, the dark web is a part of the Internet used for many atrocious purposes, of which cybercrime is the topmost. People visit the dark web to perform some activity anonymously without leaving any traces. All transactions and payments are usually made in cryptocurrency (e.g., Bitcoin) because they are virtually untraceable. With the untraceable hidden layer of the Internet and the anonymity of the users associated with the dark web, several impressive cybercrimes, such as money laundering, drug trafficking, illegal firearm/gun procurement, and terrorism, have been reported. Cyberattacks can cause serious harm to thousands of people, including individuals and public and private entities. Hence, the study has provided some recommendations that will assist law enforcement agencies, security agencies, and IT security personnel in averting security threats from the dark web, thus protecting society. In addition, this study provides an empirical basis for future studies on the

dark web. This study was limited to a systematic review and therefore recommended future research to focus on collecting primary data to provide more insights into the impact of the darkweb. In addition, future research should focus on awareness campaigns about the dangers of the dark web.

References

[1] Ablon, L., Libicki, M. C. & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data:*

[2] *Hackers' bazaar*. Rand Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

[3] Aceto, G. & Pescapé, A. (2015). Internet censorship detection: A survey. *Computer Networks*, 83, 381-421. https://doi.org/10.1016/j.comnet.2015.03.008

[4] Albrecht, C., Duffin, K. M., Hawkins, S. & Rocha, V. M. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money LaunderingControl*, 22(2), 210-216. https://doi.org/10.1108/JMLC-12-2017-0074

[5] Aldridge, J., Decary-Hetu, D. & EMCDDA, U. (Ed.) (2015). Cryptomarkets and the future of illicit drug markets. In *The Internet and Drug markets* (pp. 23-32). (Insights; Vol. 21). Publications Office of the European Union. https://doi.org/10.2810/324608

[6] Basheer, R. & Alkhatib, B. (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications*. https://doi.org/10.1155/2021/1302999

[7] Bates, R. A. (2016). Tracking lone wolf terrorists. *The Journal of Public and Professional Sociology*, 8(1), 6.

[8] Bertola, F. (2020). Drug trafficking on Darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime. *American Journal of Qualitative Research*,4(2), 27-34. https://doi.org/10.29333/ajqr/8243

[9] Besenyő, J. & Gulyas, A. (2021). The effect of the dark web on the security. *Journal of Security &*

Sustainability Issues, 11(1), 103-121. https://doi.org/10.47459/jssi.2021.11.7
Bhakiyalakshmi, K., Vidhyalakshmi, G., Kumaresan, A. & Vijayakumar, K. (2017).

[10]Network traffic classification using correlation information. *Advances in Natural and Applied Sciences*, 11(6 SI), 76-82.

[11]Biswas, R., Fidalgo, E., & Alegre, E. (2017, December). Recognition of service domains on TOR dark net using perceptual hashing and image classification techniques. In *8th International Conference on Imaging for Crime Detection and Prevention (ICDP 2017)*(pp. 7-12). IET.

[12]Broadhurst, R., Woodford-Smith, H., Maxim, D., Sabol, B., Orlando, S., Chapman-Schmidt,

a. B. & Alazab, M. (2017). Cyber terrorism: research review: research report of the Australian national university cybercrime observatory for the Korean institute of criminology. https://doi.org/10.13140/RG.2.2.19282.96964

[13]Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F. & Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: structure and organizationfrom a Canadian perspective. *Forensic Science International*, 264, 7-14. https://doi.org/10.1016/j.forsciint.2016.02.045

[14]Bryans, D. (2014). Bitcoin and money laundering: mining for an effective solution. *Indian Legal Journals*, 89, 441. Retrieved from https://ssrn.com/abstract=2317990

[15]Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C. & Svenson, P. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics*, 2, 11. https://doi.org/10.1186/2190-8532-2-11

[16]Bu, Z., Xia, Z. & Wang, J. (2013). A sock puppet detection algorithm on virtual spaces. *Knowledge-Based Systems*, 37, 366-377. https://doi.org/10.1016/j.knosys.2012.08.016
Burbano, D. & Hernandez-Alvarez, M. (2017, October). Identifying human trafficking patterns online. In *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6).

a. IEEE.

[17]Eichler, G. M. & Schwarz, E. J. (2019). What sustainable development

[18]laundering: mixed results? An explorative study on money laundering of cybercrime proceeds usingbitcoin. *Journal of Financial Crime*, 25(2), 419-435. https://doi.org/10.1108/JFC-11- 2016-0067

[19]Volety, T., Saini, S., McGhin, T., Liu, C. Z. & Choo, K.-K. R. (2019). Cracking bitcoin wallets:I want what you have in the wallets. *Future Generation Computer Systems*, 91, 136- 143. https://doi.org/10.1016/j.future.2018.08.029

[20]Vyas, P., Vyas, G., Chauhan, A., Rawat, R., Telang, S. & Gottumukkala, M. (2022). Anonymous Trading on the Dark Online Marketplace: An Exploratory Study. In *Using Computational Intelligence for the Dark Web and Illicit Behavior Detection* (pp. 272- 289). IGI Global. https://doi.org/10.4018/978-1-6684-6444-1.ch015

[21]Webb, J., Ahmad, A., Maynard, S. B. & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, 44, 1-15. https://doi.org/10.1016/j.cose.2014.04.005

[22]Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, 39(3), 195-206. https://psycnet.apa.org/doi/10.1080/1057610X.2015.1119546

[23]Zhang, J., Xiang, Y., Wang, Y., Zhou, W., Xiang, Y. & Guan, Y. (2012). Network traffic classification using correlation information. *IEEE Transactions on Parallel and Distributed Systems*, 24(1), 104-117. https://doi.org/10.1109/TPDS.2012.98

[24]Zhang, X. & Chow, K. (2020). A framework for dark Web threat intelligence analysis. In *CyberWarfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 266- 276). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch017

[25]Zhou, G., Zhuge, J., Fan, Y., Du, K. & Lu, S. (2020). A market in dream: the rapid development of anonymous cybercrime. *Mobile Networks and Applications*, 25(1), 259-270. https://doi.org/10.1007/s11036-019-01440-2