International Journal of Information Science and Management
Vol. 21, No. 4, 2023, 1-21
DOI: https://doi.org/10.22034/ijism.2023.1978002.0 / DOR: https://dorl.net/dor/20.1001.1.20088302.2023.21.4.1.7

Original Research

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

Lizzy Oluwatoyin Ofusori
Research Fellow/ Lecturer, School of Management, IT and Governance, University of KwaZulu-Natal, Durban, South Africa.
ofusoril@ukzn.ac.za
ORCID iD: https://orcid.org/0000-0002-6036-619X

Rimuljo Hendradi
Lecturer, Information Systems Department, Faculty of Science and Technology, Universitas Airlangga, Surabaya, Indonesia.
Corresponding Author:
rimuljohendradi@fst.unair.ac.id
ORCID iD: https://orcid.org/0000-0002-8679-0220

Received: 28 November 2022
Accepted: 31 December 2022

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 the anonymity 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, given time, 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 for effective 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 undertaking more 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 al.

(2018, 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."

With the untraceable hidden layer of the Internet and the anonymity of the users associated with the dark web, several impressive cybercrimes have been reported, such as WannaCry ransomware, Distributed Denial-of-Service (DDoS) attacks, illegal harm procurements, illicit fraud transactions, and illegal recruitment (Nazah, Huda, Abawajy & Hassan, 2020). Such cyberattacks can cause serious harm to thousands of people in society (i.e., individuals, public, and private entities). For example, weapons can be bought easily from the dark web to perpetrate crimes in society. Likewise, cybercriminals can now recruit people on the dark web to execute ransomware and DDoS attacks (Upulie & Prasanga, 2021). According to Ehrenfeld (2017), "WannaCry ransomware" automatically encrypts every file on the computer's hard drive, making them impossible for users to access, and demands ransom payment (usually using cryptocurrency) to decrypt them.

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 criminal activities performed on this site are still on the increase. Scholz (2016) attributed the success of the 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 way to 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 of the 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.

Accordingly, two research questions (RQ) were raised:

RQ1. What is the impact of the dark web on society?

RQ2. How can the security concerns associated with the dark web be addressed?

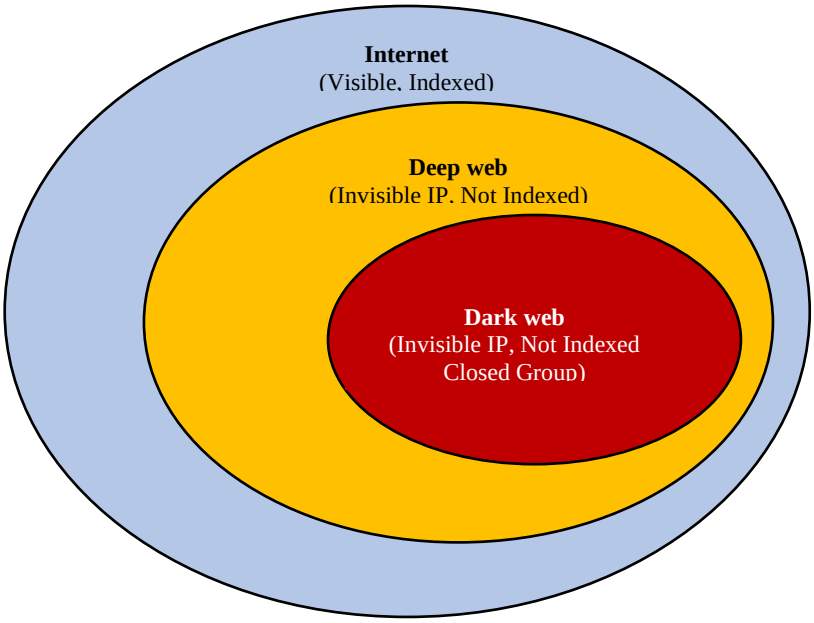


Figure 1: The Surface, Deep, and Dark Web (Odendaal et al., 2019)

The paper is structured as follows. Section 2 discusses the research methodology employed for 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 security agencies 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 Figure 2, 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.

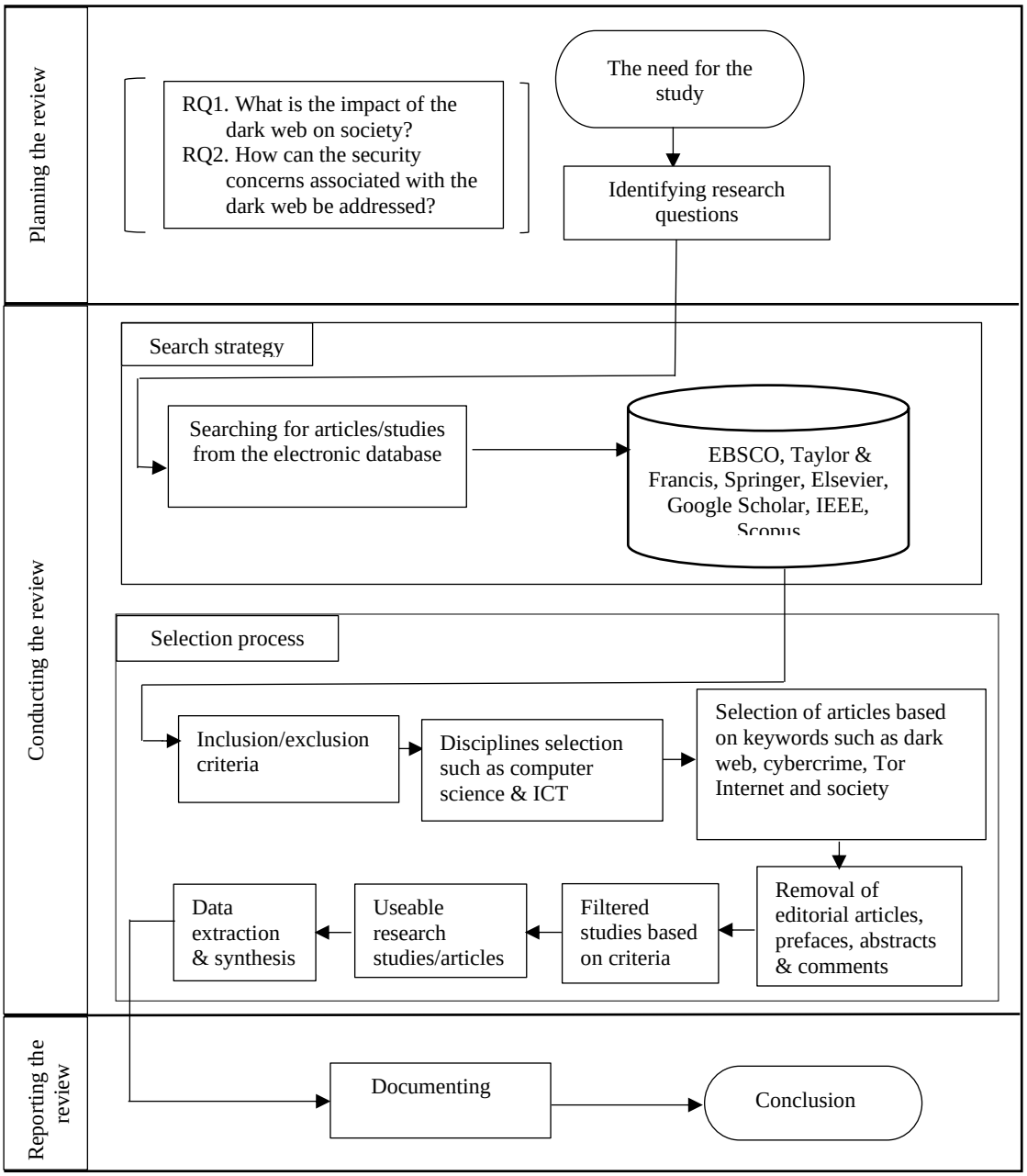


Figure 2: Overview of SLR Procedure (Authors' own)

Data extraction involved using keywords in titles and abstracts such as "dark web," "Tor," "cybercrime," "Internet," and "society" (Table 1). Articles were assessed and screened for eligibility using the pre-specified eligibility search criteria (i.e., "dark web," "Tor," "cybercrime," "Internet," and "society").

Table 1
Search Items

Search terms	***Phrases used in the search terms***
Dark web	Dangers associated with the dark web The perspective of the dark web The deep and dark web Crypto market Darknet Hidden marketplace
Tor	Traveling the silk road An anonymous browser Tor black markets Onion routing
Cybercrime	A web of crimes Market of cybercrime Terrorism on the dark web Techniques to detect terrorists Anonymous cybercrime
Internet	Internet freedom Online weapons trafficking Dark web and internet governance Internet censorship detection
Society	Darkweb impact on society Perspective of public policy on the dark web Dark web and society Law enforcement and dark web

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), and those not written in English. The search led to extracting 314 research papers, of which 67 were usable for analysis (Figure 3). As shown in Figure 3, stage 1 involved selecting papers from electronic databases and conference proceedings, which yielded 314 papers. At stage 2, papers were excluded based on title and keywords, which produced 144 papers. Also, at stage 3, papers were 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 papers were obtained and used.

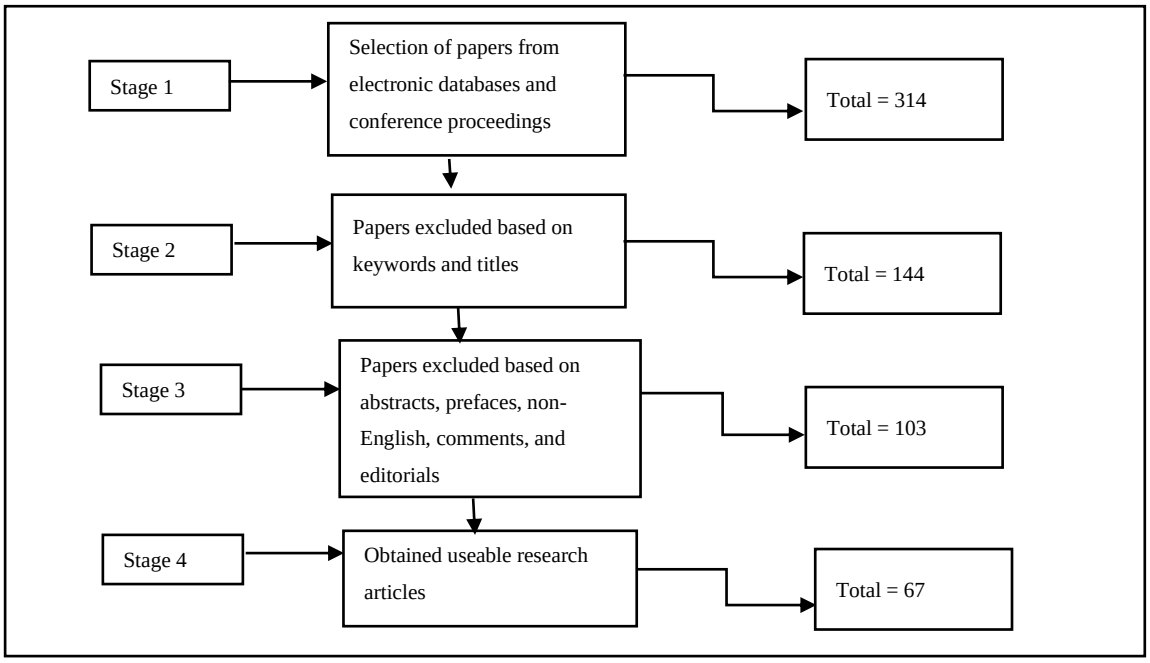
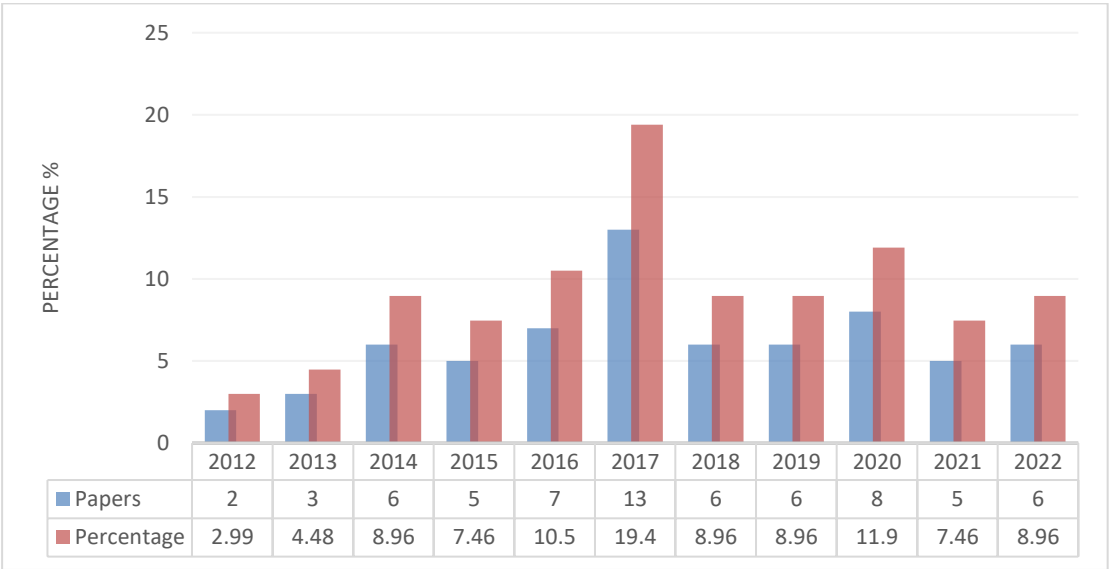


Figure 3: Stages of Selection

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 the highest report of the dark web, mainly devoted to cybercrime, ranging from human trafficking to 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.



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Papers	2	3	6	5	7	13	6	6	8	5	6
Percentage	2.99	4.48	8.96	7.46	10.5	19.4	8.96	8.96	11.9	7.46	8.96

Figure 4: Distribution of Research Papers per Year

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 in the 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 it relates 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 address the 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 with little 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, Black Market Reloaded, or the General Store, often specialize in "black market" goods, which include illicit 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 Organized Crime 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 facilitate online 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 to commit 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 given network (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) Illegal Financial Services: Illegal financial services are one of the major unlawful acts of financial fraud on the dark web (DiPiero, 2017). While most real-life financial transactions can be traceable to entities or individuals, the emergence of cryptocurrencies like Bitcoin allows for near-anonymous money exchange (Gupta et al., 2019). The decentralized Bitcoin system offers pseudonymity and is not regulated by any centralized authority or tracked by a formal institution (Broadhurst et al., 2017). This decentralized system complements the dark web's nature to make funds available for operations without revealing the source. Cryptocurrencies facilitate activity on the dark web for marketplace payments and to fund crime (Chawki, 2022; Gupta et al., 2019). According to Upulie and Prasanga (2021), the two noticeable dark websites that enable the user to perform untraceable financial transactions are InstaCard, and Banker & Co. Upulie and Prasanga (2021, p. 6) affirm that "the main two methods in which these illegal transactions are performed include; (1) disguising the actual source of the transaction to launder cryptocurrency and (2) issuing an anonymous debit card issued to a financial institution". In addition, the dark web allows trusted traders to create and issue virtual credit cards on the site. For example, a website named "Atlantic Carding" permits its users to purchase virtual credit cards.

(v) 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 (Webb et 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 Table 2 as follows:

Table 2
Mapping of Reviewed Papers on Major Applications of the Dark Web

Study	Anonymous marketplace	Recruitment	Cybercrime	Illegal financial transaction	Cyberthreat intelligence
Ablon et al. (2014)	✓			✓	
Basheer and Alkhatib (2021)					✓
Bertola (2020)				✓	
Broadhurst et al. (2017)					
Bryans (2014)				✓	
Brynielsson et al. (2013)				✓	
Chawki (2022)		✓			
Christin (2013)	✓			✓	✓
DiPiero (2017)				✓	
Elmellas (2016)			✓		
Gupta et al. (2019)	✓	✓		✓	✓ ✓
Kaur and Randhawa (2020)				✓	
Rhumorbarbe et al. (2018)					✓
Samtani et al. (2017)		✓			
Scanlon and Gerber (2014)				✓	
Taleby Ahvanooey et al. (2022)					
Topor (2019)				✓	✓
Vyas et al. (2022)	✓				
Webb et al. (2014)					✓
Weimann (2016)		✓			

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 negative consequence (Odendaal et al., 2019; Weimann, 2016). According to Mador (2021, p. 6), "much of 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 major

cybercrime 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 (Table 3).

Table 3
Mapping of Reviewed Papers on Cybercrime Activities Conducted on the Dark Web.

Cybercrimes	**Study**
Drug trafficking	Bertola (2020), Broséus et al. (2016), Me and Pesticcio (2018), Soska and Christin (2015), Aldridge and Decary-Hétu (2015), Duxbury and Haynie (2018)
Kidnapping/murder	Jin, Jang, Lee, Shin & Chung (2022), Lee et al. (2019), Melsky (2019), Taleby Ahvanooey et al. (2022), Zhou, Zhuge, Fan, Du & Lu (2020), Besenyő and Gulyas (2021)
Human trafficking	Burbano and Hernandez-Alvarez (2017), Taleby Ahvanooey et al. (2022), Kaur and Randhawa (2020)
Firearms/weapons procurement	Copeland, Wallin & Holt (2020), Taleby Ahvanooey et al. (2022), Revell (2017), Hayes et al. (2018)
Money laundering	Taleby Ahvanooey et al. (2022), Van Wegberg, Oerlemans and van Deventer (2018), Albrecht, Duffin, Hawkins & Rocha (2019), Bryans (2014), Volety, Saini, McGhin, Liu & Choo (2019)
Contract hacking services	Gupta et al. (2019), Taleby Ahvanooey et al. (2022), Odendaal et al. (2019), Samtani et al. (2017)
Terrorism	Chawki (2022), Chertoff and Simon (2015), Bates (2016), Nazah et al. (2020), Weimann (2016)
Ransomware attack	Chawki (2022), Ehrenfeld (2017), Gokhale and Olugbara (2020), Zhang and Chow (2020)

(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 via crypto markets on the dark web represents a new form of trafficking, providing a new channel for 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 hire a 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 of

Investigation (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 of murder 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 the procurement 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 crimes in society (Hayes et al., 2018). A study conducted on the international firearms trade by RAND Europe 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).

(v) Money Laundering: Money Laundering is one of the most common crimes conducted on the dark web (Taleby Ahvanooey et al., 2022). Criminals rely on the dark web to transfer illicit funds (e.g., proceeds of crime), usually through a complex sequence of transactions (including those involving cryptocurrency) to anonymous accounts (Albrecht et al., 2019; Taleby Ahvanooey et al., 2022). According to Van Wegberg et al. (2018), money is easily laundered on the dark web in the form of Bitcoin because it is hard to trace due to its anonymous nature. Bitcoin is the virtual currency of interest because it is presumably the preferred cryptocurrency among cybercriminals (Bryans, 2014; Volety et al., 2019).

(vi) Contract Hacking Services: According to Gupta et al. (2019), the dark web has buzzed with hacking services. "There exist several hacking forums or communities throughout the dark web that provide underground marketplaces for trading different tools or services, as well as stolen/leaked information" (Taleby Ahvanooey et al., 2022, p. 3). There are several ways to buy hacking services, but the most attractive place where it is possible to meet members of the principal hacking communities is the dark web (Odendaal et al., 2019; Samtani et al., 2017).

(vii) Terrorism: The dark web and terrorists complement each other because the latter needs an anonymous network that is readily available yet generally inaccessible (Chertoff & Simon, 2015). Terrorist organizations such as the Islamic State in Iraq and Syria (ISIS) and Al-Qaeda use the features of the dark web to spread propaganda and solicit funds to carry out their negative motives (Bates, 2016; Chawki, 2022; Nazah et al., 2020). According to Weimann (2016), terrorism on the dark web is a dangerous threat to national security. Nazah et al. (2020) claim complex data on the dark web supports ISIS in indoctrination and ambition.

(viii) Ransomware Attack: Ransomware, also referred to as malware, is one type of malicious software where the attacker automatically encrypts every file on the computer's hard drive, making them impossible for users to access, and demands ransom payment (typically using cryptocurrency) to decrypt them (Chawki, 2022; Ehrenfeld, 2017). A typical example is Wannacry ransomware, which automatically encrypts files when downloaded and has caused severe damage estimated at 4 billion dollars (Gokhale & Olugbara, 2020). Dark web websites are mostly encrypted, which helps maintain the confidentiality of user identities and makes activities untraceable (Zhang & Chow, 2020).

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 because of 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 due to the decentralized nature of the platform. These challenges are further exacerbated because of the 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 section answers RQ2 as summarized in Table 4.

Table 4
Mapping of Reviewed Papers on Techniques to Address Security Concerns

Dark web security techniques	Study
Law Enforcement	Dalins, Wilson & Carman (2018), Ghappour (2017), Hayes et al. (2018), Nazah et al. (2020), Kavallieros, Myttas, Kermitsis, Lissaris, Giataganas & Darra (2021), Cole, Latif & Chowdhury (2021)
Cryptographic hash functions	Kheshaifaty and Gutub (2020), Nazah et al. (2020), Biswas, Fidalgo & Alegre (2017), Singh, Amritha and Sethumadhavan (2022)
MEMEX tools	Hammonds (2015), Nazah et al. (2020), Ehney and Shorter (2016), Mattmann (2015), Heinl, Yu and Wijesekera (2019).
Sock puppet detection	Bu, Xia and Wang, (2013), Maity, Chakraborty, Goyal and Mukherjee (2017), Kaur and Randhawa (2020), Liu, Wu, Han

Dark web security techniques	Study
	and Zhou (2016), Nazah et al. (2020), Sönmez and Seçkin Codal (2022), Spitters, Klaver, Koot and Van Staalduinen (2015)
Honeypot deployment	Fan Du, Fernández and Villagra (2017), Koniaris, Papadimitriou, Nicopolitidis and Obaidat (2014), Mishra, Pilli, Varadharajan and Tupakula (2017), Moore (2016), Nazah et al. (2020)
Classification of networks	Chaudhari and Patil (2017), Ling, Luo, Yu, Fu, Xuan and Jia (2012), Nazah et al. (2020), Bhakiyalakshmi, Vidhyalakshmi, Kumaresan and Vijayakumar (2017), Zhang, Xiang, Wang, Zhou, Xiang and Guan (2012)

(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 the dark web (Dalins et al., 2018; Kavallieros et al., 2021; Nazah et al., 2020). Criminal law relates to 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 to organizations 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 tracing cryptographic hash functions (Biswas et al., 2017; Singh et al., 2022). Hash functions produce values representing the original message from which they have been computed (Kheshaifaty & Gutub, 2020). In investigations, the cryptographic hash functions are essential to prove that all evidence 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 dark web more precisely.

(iii) Memex Tools: The Defense Advanced Research Projects Agency (DARPA) developed a 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 puppet detection 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).

(v) Honeypot Deployment: Cybercriminals often target network servers to spread malicious software over the network or compromise systems (Nazah et al., 2020). Hence, using honeypots to detect cyber-attacks in the network traffic is another effective way to curb illegal activities in the dark web Tor network (Fan et al., 2017; Koniaris et al., 2014; Mishra et al., 2017). According to Nazah et al. (2020), the honeypot technique is used as a ransomware detection method. This technique can detect unauthorized access because the honeypot tricks the attacker into acting as a decoy computer (Moore, 2016; Nazah et al., 2020).

(vi) Classification of Networks: Classifying network traffic using correlation helps detect illegal activities on the dark web (Nazah et al., 2020). This technique allows for safe inferences about the network as it automates the detection of darknet traffic to block criminal activities (Chaudhari & Patil, 2017). Classifying traffic flows plays a vital role in network security and management, such as lawful interception, quality of service (QoS) control, and intrusion detection (Bhakiyalakshmi et al., 2017; Zhang et al., 2012). In addition, it locates entry and exit nodes to identify attacks by analyzing the users' communication and the Tor network's routing behavior (Ling et al., 2012).

In summary, this section has answered RQ2 by showing the various detection techniques used to address security concerns associated with the dark web. However, the main issue in analyzing the dark web for cyber security intelligence is that a considerable amount of unstructured and inaccessible information must first be found and processed (Schäfer, Fuchs, Strohmeier, Engel, Liechti & Lenders, 2019). “This processing also needs to be done in a scalable way that enables humans to collect useful intelligence quickly and reliably” (Schäfer et al., 2019, p. 6).

Discussion

The advent of the dark web is fundamentally changing how crime is conducted. The findings indicate that the dark web is used for many atrocious purposes. Likewise, the results reveal the impact of dark web activities on society. It shows that the dark web is an enabler of cybercrime due to its decentralized and anonymous features. It is important to note that much of the dark web is devoted to cybercrime, from sharing techniques and tools to selling stolen data and credentials. A cyber-attack, on an individual level, can lead to various consequences, ranging from extortion of money to theft of personal information (Kaur & Randhawa, 2020). When cybercriminals steal an individual’s identity, they can take out loans, incur credit, amass debt, and then flee without a trace (Cole et al., 2021; Gupta et al., 2019). Cybercriminals are making money but causing more damage (Odendaal et al., 2019). The overall monetary impact on society and government is estimated to be billions of dollars annually (Zhang & Chow, 2020). According to the United Nations, “annual proceeds from transnationally organized crime activities amount to more than 870 billion dollars, with drug trafficking producing the largest individual segment of that total amount” (Holland, 2020, p. 108).

While governments and regulatory authorities have introduced strategic governance of the activities on the dark web, cybercriminals are becoming adaptive towards the enforced strategies to detect them on the dark web (Nazah et al., 2020).

The majority of past research on the dark web has concentrated on the dark web phenomenon and threat analysis, but just a few studies have looked at the impact of the dark web on society. This represents a gap in the literature and is one that this study addresses. Hence, this study provides insight into the cybersecurity threats the community is exposed to

due to illegal activities on the dark web. Also, the study has established that the dark web is an enabler of several cybercrimes in society. Thus, the following recommendations are made based on the research findings.

Firstly, this study recommends a periodic review of the detection techniques for effective monitoring because cybercriminals are adaptive and, given time, will usually find ways to bypass such detective techniques. Secondly, the study recommends that regulatory authorities, security agencies, or forensic analysts ensure that they are updated with the latest scientific knowledge on the safe management of the dark web by undertaking more training in cyber security. Thirdly, this study recommends some areas that security agencies can monitor to successfully govern and avert the adverse effects of the dark web on society. These areas include:

(i) Hidden Services Directory: Monitoring crime via its hidden service is one of the few ways a crime could be traced back to its origin. However, Kaur and Randhawa (2020) argue that most hidden services are highly volatile, with constant URL changes to dodge charges. Hence, it is suggested that the new sites/services should be captured (i.e., snapshot) by the regulatory agencies as soon as they pop up and are studied for analysis before they vanish or reappear under a different domain name.

(ii) Social Sites: The dark web holds several social media sites like Pastebin, which are often used to exchange new addresses for new hidden services (Nazah et al., 2020; Upulie & Prasanga, 2021). Cybercriminals rely heavily on such sites to communicate and sell stolen identities, credit card numbers, and other information (Kaur & Randhawa, 2020). However, these sites can be monitored to identify criminals by using cryptographic functions (Surette, 2015). Therefore, keeping social sites under constant watch is essential to eliminate new illegal dark web domains.

(iii) Customer Data: Top-level domains can be monitored using destination requests. The monitoring process can be done without intruding on the users' privacy since only the endpoint of the request is monitored without tracing the request back to the user (Kaur & Randhawa, 2020).

(iv) Marketplace Profiling: The profiling utilizes gathered customer data, such as online marketplace behavior, subscriber information, usage, and the like to determine what activities a particular buyer or seller has been involved in (Kaur & Randhawa, 2020; Koh, 2011). This will enable law enforcement agencies to identify illegal acts on the dark web quickly.

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 dark web. In addition, future research should focus on awareness campaigns about the dangers of the dark web.

References

Ablon, L., Libicki, M. C. & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Rand Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

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

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

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

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

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

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

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

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.

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

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

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

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

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). IEEE.

Chaudhari, R. R. & Patil, S. P. (2017). Intrusion detection system: classification, techniques and datasets to implement. *International Research Journal of Engineering and Technology (IRJET)*, 4(2), 1860-1866. Retrieved from https://www.irjet.net/archives/V4/i2/IRJET-V4I2366.pdf

Chawki, M. (2022). The Dark Web and the future of illicit drug markets. *Journal of Transportation Security*, 15, 173-191. https://doi.org/doi.org/10.1007/s12198-022-00252-y

Chertoff, M. & Simon, T. (2015). *The impact of the dark web on internet goverannce and cyber security*. the Centre for International Governance Innovation and Chatham House. Retrieved from https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224).

Cole, R., Latif, S. & Chowdhury, M. M. (2021, October). Dark web: A facilitator of crime. In *2021 international conference on electrical, computer, communications and mechatronics engineering (iceccme)* (pp. 1-6). IEEE.

Copeland, C., Wallin, M. & Holt, T. J. (2020). Assessing the practices and products of Darkweb Firearm vendors. *Deviant Behavior*, 41(8), 949-968. https://doi.org/10.1080/01639625.2019.1596465

Dalins, J., Wilson, C. & Carman, M. (2018). Criminal motivation on the dark web: A categorization model for law enforcement. *Digital Investigation*, 24, 62-71. https://doi.org/10.1016/j.diin.2017.12.003

DiPiero, C. (2017). Deciphering cryptocurrency: Shining a light on the deep dark web. *University of Illinois Law Review*, 3, 1267-1299.

Duxbury, S. W. & Haynie, D. L. (2018). Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks*, 52, 238-250. https://doi.org/10.1016/j.socnet.2017.09.002

Ehney, R. & Shorter, J. D. (2016). Deep web, dark web, invisible web and the post ISIS world. *Issues in Information Systems*, 17(4), 36-41.

Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems*, 41(7), 104. https://doi.org/10.1007/s10916-017-0752-1

Eichler, G. M. & Schwarz, E. J. (2019). What sustainable development goals do social innovations address? A systematic review and content analysis of social innovation literature. *Sustainability*, 11(2), 522. https://doi.org/10.3390/su11020522

Elmellas, J. (2016). Knowledge is power: the evolution of threat intelligence. *Computer Fraud & Security*, 7, 5-9. http://dx.doi.org/10.1016/S1361-3723(16)30051-3

Fan, W., Du, Z., Fernández, D. & Villagra, V. A. (2017). Enabling an anatomic view to investigate honeypot systems: A survey. *IEEE Systems Journal*, 12(4), 3906-3919.

Ghappour, A. (2017). Searching places unknown: Law enforcement jurisdiction on the dark web. *Stanford Law Review.*, *69*, 1075-1136. Retrieved from https://scholarship.law.bu.edu/faculty_scholarship/204

Gokhale, C. & Olugbara, O. O. (2020). Dark web traffic analysis of cybersecurity threats through South African Internet protocol address space. *SN Computer Science*, 1, 273. https://doi.org/10.1007/s42979-020-00292-y

Gupta, A., Maynard, S. B. & Ahmad, A. (2019). The dark web phenomenon: A review and research agenda. In *Australasian Conference on Information Systems*. Perth, WA. Retrieved from https://arxiv.org/ftp/arxiv/papers/2104/2104.07138.pdf

Hammonds, J. (2015). An inquiry into privacy concerns: Memex the deep Web and sex trafficking. Retrieved from http://www.infosecwriters.com/Papers/JHammonds_Privacy.pdf

Hayes, D. R., Cappa, F. & Cardon, J. (2018). A framework for more effective dark web marketplace investigations. *Information*, 9(8), 186. https://doi.org/10.3390/info9080186

He, S., He, Y. & Li, M. (2019, March). Classification of illegal activities on the dark web. In *Proceedings of the 2nd International Conference on Information Science and Systems* (pp. 73-78). https://doi.org/10.1145/3322645.3322691

Heinl, M. P., Yu, B. & Wijesekera, D. (2019). A Framework to Reveal Clandestine Organ Trafficking in the Dark Web and Beyond. *Journal of Digital Forensics, Security and Law*, *14*(1), 2.

Holland, B. J. (2020). Transnational cybercrime: The dark web. *Encyclopedia of Criminal Activities and the Deep Web*, 108-128. https://doi.org/10.4018/978-1-5225-9715-5.ch007

Jardine, E. (2018). Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media & Society*, 20(8), 2824-2843. https://doi.org/10.1177/1461444817733134

Jin, Y.W., Jang, E., Lee, Y., Shin, S. & Chung, J. (2022). Shedding New Light on the Language of the Dark Web. *North American Chapter of the Association for Computational Linguistics*. Retrieved from https://arxiv.org/pdf/2204.06885.pdf

Kaur, S. & Randhawa, S. (2020). Dark web: A web of crimes. *Wireless Personal Communications*, 112, 2131-2158. https://doi.org/10.1007/s11277-020-07143-2

Kavallieros, D., Myttas, D., Kermitsis, E., Lissaris, E., Giataganas, G. & Darra, E. (2021). Understanding the dark web. In *Dark Web Investigation* (pp. 3-26). Springer.

Kheshaifaty, N. & Gutub, A. (2020). Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions. *IJCSNS International Journal of Computer Science and Network Security*, 20(9), 16-28. Retrieved from http://paper.ijcsns.org/07_book/202009/20200903.pdf

Koh, B. (2011). *User profiling in online marketplaces and security*. The University of Texas at Dallas.

Koniaris, I., Papadimitriou, G., Nicopolitidis, P. & Obaidat, M. (2014, June). Honeypots deployment for the analysis and visualization of malware activity and malicious connections. In *2014 IEEE international conference on communications (ICC)* (pp. 1819-1824). IEEE.

Kumar, S., Cheng, J., Leskovec, J. & Subrahmanian, V. S. (2017, April). An army of me: Sockpuppets in online discussion communities. In Proceedings of the 26th International Conference on World Wide Web (pp. 857-866).

Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., Son, S. & Shin, S. (2019, February). Cybercriminal minds: an investigative study of cryptocurrency abuses in the dark web. In *26TH Annual Network and Distributed System Security Symposium (NDSS 2019)* (pp. 1-15). Internet Society.

Ling, Z., Luo, J., Yu, W., Fu, X., Xuan, D. & Jia, W. (2012). A new cell-counting-based attack against Tor. *IEEE/ACM Transactions On Networking*, 20(4), 1245-1261.

Liu, D., Wu, Q., Han, W. & Zhou, B. (2016). Sockpuppet gang detection on social media sites. *Frontiers of Computer Science*, 10, 124-135. https://doi.org/10.1007/s11704-015-4287-7

Mador, Z. (2021). Keep the dark web close and your cyber security tighter. *Computer Fraud & Security*, 1, 6-8.

Maity, S. K., Chakraborty, A., Goyal, P. & Mukherjee, A. (2017, February). Detection of sockpuppets in social media. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 243-246).

Mallett, R., Hagen-Zanker, J., Slater, R. & Duvendack, M. (2012). The benefits and challenges of using systematic reviews in international development research. *Journal of Development Effectiveness*, 4(3), 445-455. https://doi.org/10.1080/19439342.2012.711342

Mattmann, C. A. (2015, December). Search of the deep and dark web via darpa memex. In *AGU Fall Meeting Abstracts* (Vol. 2015, pp. IN33A-1795).

Me, G. & Pesticcio, L. (2018). Tor black markets: economics, characterization and investigation technique. In *Cyber Criminology* (pp. 119-140). Springer.

Melsky, M. (2018). *The Dark Corners of the Lindbergh Kidnapping*. Vol. 2. iUniverse.

Mishra, P., Pilli, E. S., Varadharajan, V. & Tupakula, U. (2017). Intrusion detection techniques in cloud environment: A survey. *Journal of Network and Computer Applications*, 77, 18-47. https://doi.org/10.1016/j.jnca.2016.10.015

Moore, C. (2016, August). Detecting ransomware with honeypot techniques. In 2016 Cybersecurity and Cyberforensics Conference (CCC) (pp. 77-81). IEEE.

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

Odendaal, R., Hattingh, M. & Eybers, S. (2019, September). The good, the bad and the ugly of the dark web: Perceptions of South African students and parents. In *Proceedings of the South African Institute of Computer Scientists and Information Technologists* (pp. 1-9). https://doi.org/10.1145/3351108.3351117

Revell, T. (2017). US guns sold in Europe via dark web. *New Scientist*, 3136.

Rhumorbarbe, D., Werner, D., Gilliéron, Q., Staehli, L., Broséus, J. & Rossy, Q. (2018). Characterizing the online weapons trafficking on cryptomarkets. *Forensic Science International*, 283, 16-20. https://doi.org/10.1016/j.forsciint.2017.12.008

Samtani, S., Chinn, R., Chen, H. & Nunamaker Jr, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, 34(4), 1023-1053. http://dx.doi.org/10.1080/07421222.2017.1394049

Scanlon, J. R. & Gerber, M. S. (2014). Automatic detection of cyber-recruitment by violent extremists. *Security Informatics*, 3, 5. https://doi.org/10.1186/s13388-014-0005-5

Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M. & Lenders, V. (2019, May). BlackWidow: Monitoring the dark web for cyber security information. In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-21). IEEE.

Scholz, R. W. (2016). Sustainable digital environments: What major challenges is humankind facing? *Sustainability*, 8(8), 726. https://doi.org/10.3390/su8080726

Singh, R., Amritha, P. P. & Sethumadhavan, M. (2022, April). Scoring Scheme to Determine the Sensitive Information Level in Surface Web and Dark Web. In *International Conference on Advances in Computing and Data Sciences* (pp. 157-167). Cham: Springer International Publishing.

Sönmez, E. & Seçkin Codal, K. (2022). Terrorism in cyberspace: A critical review of dark web studies under the terrorism landscape. *Sakarya University Journal of Computer and Information Sciences*, 5(1), 1-21. https://doi.org/0.35377/ saucis.05.01. 950746

Soska, K. & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *24th USENIX security symposium (USENIX security 15)* (pp. 33-48). Retrieved from https://www.usenix.org/system/files/sec15-paper-soska-updated_v2.pdf

Spitters, M., Klaver, F., Koot, G. & Van Staalduinen, M. (2015, September). Authorship analysis on dark marketplace forums. In *2015 European Intelligence and Security Informatics Conference* (pp. 1-8). IEEE.

Stapic, Z., López, E. G., Cabot, A. G., de Marcos Ortega, L. & Strahonja, V. (2012). Performing systematic literature review in software engineering. In *Central European Conference on Information and Intelligent Systems* (p. 441-447). Faculty of Organization and Informatics Varazdin.

Surette, R. (2015). Performance crime and justice. *Current Issues in Criminal Justice*, 27(2), 195-216. https://doi.org/10.1080/10345329.2015.12036041

Taleby Ahvanooey, M., Zhu, M. X., Mazurczyk, W., Kilger, M. & Choo, K. K. R. (2021, December). Do dark web and cryptocurrencies empower cybercriminals?. In *International Conference on Digital Forensics and Cyber Crime* (pp. 277-293). Cham: Springer International Publishing.

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

Upulie, H. & Prasanga, P. (2021). *Dark Web, Its Impact on the Internet and the Society: A Review*. http://dx.doi.org/10.13140/RG.2.2.11964.36484

Van Wegberg, R., Oerlemans, J.-J. & van Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419-435. https://doi.org/10.1108/JFC-11-2016-0067

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

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

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

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

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

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

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