JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Exploring the Dark Web: Unveiling its Depths and Examining the Ethical Impact on Society

Ms. Sanju Xavier
Assistant Professor, Jain (Deemed to be University)
Dr. Bhargavi D Hemmige
Professor, Jain (Deemed to be University)

ABSTRACT

The Dark Web, a mysterious part of the internet has captured people's attention. Raised concerns. In this research paper titled "Exploring the Dark Web; Revealing its Depths and Examining its Impact, on Society " we delve into the network of encrypted platforms and services that make up this online world. The study offers an overview of the Dark Webs structure, including its marketplaces, forums and the technologies that enable anonymity and privacy. Additionally, it explores the reasons behind using the Dark Web, which range from protecting privacy to engaging in activities such as cybercrime, drug trafficking and contraband exchange. Moving beyond the aspects our paper delves into the implications presented by the Dark Web in society. It examines issues related to cybersecurity, law enforcement efforts, privacy concerns and freedom of expression. This analysis also addresses how the Dark Web serves both as a sanctuary for those seeking protection from surveillance while also being a haven for criminals and malicious individuals. Furthermore, the research considers the challenges faced by society when trying to strike a balance, between maintaining personal privacy needs and ensuring security in an era characterized by increasing interconnectivity. The ethical responsibility surrounding the regulation and control of the Dark Web brings up inquiries regarding individuals, corporations and governments.

Keywords: ***cybercrime, cyber security, Dark web, privacy, web***

INTRODUCTION

The internet is a vast and ever-expanding network of information and connectivity. However, there is a hidden corner of the web that is not accessible to conventional search engines and requires specialized software and encrypted networks to access. This clandestine realm is known as the Dark Web.

The Dark Web has gained a reputation for harboring illicit activities, such as black markets, illegal trade, and anonymous communication. However, it also has legitimate uses, such as providing a platform for whistleblowing and political dissent.

This research paper explores the Dark Web, its structural framework, ethical implications, and multifaceted impact on society. In simpler terms: The Dark Web is a hidden part of the internet that can only be accessed with special software. It is often used for illegal activities, but it also has legitimate uses.

Scope of the study

The focus of this study is to analyze criminal activities on the web, which encompass various online actions involving trading, buying, or stealing personal information like bank details and digital security credentials. It aims to explore the internet's extensive networks and infrastructure, which link millions of computers, allowing them to communicate. The primary goal is to examine how these activities impact the general population in detail.

Significance of the study

The significance of this study lies in its attempt to fill gaps in the existing knowledge about the Dark Web. Most research on the Dark Web primarily focuses on its use in threat intelligence. This is intriguing because it reflects how people seek private spaces for their online activities. Understanding this perspective can help us make better predictions about the Dark Web's growth and inform decisions made by stakeholders. We argue that as regulations have become stricter and personal freedoms have diminished, the Dark Web has expanded. Cybercriminals use the Dark Web for their activities, and law enforcement efforts to combat them can stimulate innovation and development in the Dark Web. This is especially true when the financial gains from such activities support these developments. In essence, the crackdown on unlawful behaviour drives technological advancements aligned with it.

The Dark Web is evolving into a space where dedicated individuals aim to create a network that shields people from any intrusion by companies, governments, or spy agencies. For those living under oppressive regimes that limit internet access or punish political dissent, the Dark Web is a vital lifeline that provides information access and protection from persecution. In more open societies, it can serve as an essential tool for whistleblowers and secure communication, safeguarding individuals from potential repercussions in their workplaces or communities.

Alternatively, it can offer privacy and anonymity to those concerned about how their data is tracked, used, and possibly monetized by corporations and governments. Some common illegal activities on the Dark Web include arms trading, drug dealing, and the sharing of exploitative content, often involving minors, such as pornography and violent images. To address cybersecurity threats posed by hackers, it's crucial to understand how hackers and exploiters operate, and the Dark Web provides a platform for cyber security experts to engage with hackers.

Objectives

The analysis of the impact of the dark web on various aspects of society involves a comprehensive exploration of its influence on different facets of social, economic, and technological domains. Understanding the correlation between the rise in criminal activities and the presence of the dark web is crucial in deciphering the intricate relationship between the hidden online realm and the surge in illicit behaviors. Additionally, examining how the pandemic has affected criminal activities on the dark web provides insights into the adaptability and resilience of illicit networks in response to global events. This research allows the understanding of the dark web's role in shaping and responding to societal dynamics, shedding light on both its challenges and potential mitigations.

REVIEW OF LITERATURE

1. Dark Web: the economics of online drug markets, Stephen Machin, 2017

The author points out how the dark web has emerged as a visible dimension of cybercrime. Specifically, three questions were carefully studied by analyzing data online. Silk Road was one of the famous platforms for drugs in 2011 until its founder was arrested. The study talks in detail about the rise and fall of online drug platforms throughout the years. As part of their findings, they came up with different reasons for why sites get closed down or exit from the market. 1.5 million drug sales were analyzed. Although they receive negative comments due to the low quality of drugs sold, the increase in the selling of drugs online is on a continuous rise. The market responds flexibly to the demand and the exit of major players only makes it easier for newer players to join. Fall of the Silk Road and market condition post the scenario are thoroughly examined. Aftermath - total number of drugs listings being higher a month later, as Agora became the new market leader and Nucleus grew very rapidly. The ability of the platform to maintain anonymity has also largely contributed to the success of drug markets. (Vieira, 2017)

2. The dark web, Kristin Finklea

The author starts by describing how the contents of the Dark web are intentionally hidden to conceal criminal activities. An important observation made in this study is Just as criminals can rely upon the anonymity of the Dark Web, so too can law enforcement, military, and intelligence communities. The study also found out that one of the first places a user looking to access the dark web would turn to is Reddit. The further Anonymity factor is discussed in detail. How many software offer anonymity but are not foolproof. Software Tor is analyzed and how it ensures free speech. This area of research has gained massive attention. The author also gives a clear demarcation between the dark web and the deep web. How coordination, conversation, and action for illegal activities that occur without detection are also discussed in this paper. Individuals or organizations are targeted by cybercriminals. Ends the paper with suggestions on how and what can be done going forward regarding the dark web. For example, how in an anonymous environment we can effectively combat those who exploit the dark web. (Finklea, 2015)

3. The influence of black market activities through dark web on the economy, Hilary Mazi, Foka Ngniteyo Arsene, Akalanka Mailewa Dissanayaka

In the research paper titled “the influence of black market activities through dark web on the economy” published by Hilary Mazi (Department of Information Assurance - USA), Foka Ngniteyo Arsene (Department of Information Assurance - USA), Akalanka Mailewa Dissanayaka (Department of Computer Science and IT - USA). The authors of this paper have studied all the aspects that are required for an economy to run and in which black market and dark web takes place depending on the geographical areas. The paper traces down on how the black market which was limited to one specific geographical area moved on to various geographical areas with help of various improvements in the IT sector. Dark web plays a major role in helping black market businesses to be widespread among the geographical areas. The paper concentrates on the influence of black market activities on the dark web and also looks into effects which are caused by both black market and dark web on the development of specific countries' economies as well as world economy as a whole. Towards the end of the paper the authors have concluded that most of the major money making IT sector companies must thrive on the basis of protecting the privacy of the people and taking care especially of their financial aids. (Hilary Mazi, 2020)

4 . Uncovering the dark web - a case study of jihad on the web, Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, Gabriel Weimann

In the case study titled "Uncovering the dark web - a case study of jihad on the web" published by Hsinchun Chen, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, Gabriel Weimann on 7 April 2008. The study focuses on how communication have been used by various terrorist groups. In order to complete the study the authors have used various methodologies such as information collection, analysis, visualization techniques and exploits various web information sources. Through the help of these methodologies the authors could obtain some good results in which they were able to prove their hypothesis. In which the result helped the policymakers and intelligence research. (Chen, 2008)

5. The internet and drug markets, Jane Mounteney, Alessandra Bo, Alberto Oteo

In this research the authors explains how new internet technologies have emerged over the past ten years, and they have significantly facilitated the growth of online drug markets. In the past, illicit drug retail markets have been physically present, with all of the restrictions and boundaries that entails. Low-level drug transactions have often been linked to real people, real places, and real geographic regions, whether they occur in an open drug scene in the middle of the city or in a dealer's apartment on a suburban housing estate. The expansion of internet commerce in virtual markets with a worldwide reach has been made possible by recent advances. It may widen the scope of the drug supply and increase the options available to people looking to purchase drugs. Additionally, online drug marketplaces give participants the option to sell and buy from the comfort of their homes, avoiding the in-person interactions common to offline markets. Participants claim that this can offer a level of physical safety and anonymity that would be otherwise challenging to achieve. (Jane Mounteney, 2016)

6. Cocaine retail markets: multiple indicators suggest continued growth and diversification

Drug affordability is a measurement that takes into account drug purity and different national economic conditions as measured by price level indices (PLI) (for more information and restrictions, see Groshkova et al., 2018). In other words, the affordability of a medicine is determined by how much 1 gramme of a pure, "uncut" drug costs purchasers in relation to their national standard of living. A more thorough comparison of retail medication markets between nations and throughout time is made possible by affordability. Based on retail pricing and purity data from the EMCDDA for 16 European nations that provided sufficient information, which together account for about 60% of the EU's population, it was determined that between 2015 and 2020, the price of 1 gramme of cocaine decreased by an average of 38%. Although adulteration still occurs, the purity of cocaine sold at retail in Europe has been rising since 2010 and reached its highest level in the past ten years in 2019. (See Box Recent trends in cocaine adulteration). Between 2010 and 2020, the drug's retail price was largely unchanged. This seems to support the pattern noted in the earlier version of this study, which states that there is now more cocaine available on European retail markets than there was previously (EMCDDA and Europol, 2019). Even while a minor price increase and a stabilisation of purity can be seen in 2020, the COVID-19 pandemic does not appear to have significantly affected retail prices or the increase in purity documented since 2010. (Addiction, 2022)

7. Terrorism on the Dark Web, Weimann Gabriel

The material on the World Wide Web that is not indexed by standard search engines is referred to as the Deep Web, Deep Net, Invisible Web, or Dark Web. The Surface Web, or the "top" layer of the Internet, may be reached with ease by doing standard searches. However, conventional search engines like Google have not indexed "deeper" levels, or the material of the Deep Web. Internet searching is like dragging a net across the surface of the ocean; while much information may be collected in the net, much deeper information is ignored, according to Michael K. Bergman, the author of the fundamental study on the Deep Web. In reality, the majority of the information is buried far down on sites, and standard search engines are unable to access it. (Weimann, 2016)

8. Dark Web: A Web of Crimes, Kaur Shubhdeep

Our daily lives are significantly impacted by the internet. It now forms a crucial component of every everyday activity or way of life. The dark web, or untraceable hidden layer of the internet, is often used to store and access private information. However, there have been some recorded instances when this platform has been used to covertly carry out illicit and unlawful acts. This document provides an overview of the dark web as well as a list of popular dark web browsers. An understanding of the characteristics, benefits, drawbacks, and browsers of the Dark Web is provided. A summary of the various attack, exploit, and malware kinds is also provided. There are several kinds of The discussion of criminal activities and events that occur on the Dark Web aims to make readers aware of these sorts of activities and enable them to take the necessary preventive action. (Shubhdeep Kaur, 2020)

RESEARCH METHODOLOGY

The research methodology employed in this study revolves around a qualitative approach, focusing on analyzing a range of case studies associated with the dark web. These case studies are aligned with the objectives outlined in the research. Additionally, an interview was conducted to gain insights into the behavioral patterns and usage of the dark web.

The qualitative method permits an in-depth exploration and understanding of the phenomena related to the dark web through detailed case analyses. These case studies offer a comprehensive view of the diverse aspects and implications of dark web activities, enabling a thorough investigation in line with the study's objectives.

Furthermore, the interview serves as an invaluable tool to gather firsthand information and insights directly from individuals involved or knowledgeable about dark web usage. The intention behind this approach is to gain a more comprehensive understanding of the behavioral patterns, motivations, and practices of individuals engaging with the dark web, adding depth and context to the research findings.

Case study 1- Data breach in Kashmir University

On August 11, 2022, Kashmir University in Srinagar encountered a reported case of data breach and sale. Responding promptly, the university established a specialized information technology team to investigate the alleged breach. The breached data, allegedly available for sale at $250 for undergraduate student details, prompted immediate action. While personal credentials were identified as potentially compromised, they were reportedly not tampered with. To prevent future breaches, the university is enhancing its security measures. The potential breach was brought to the institution's attention through an email notification.

NordVPN, a cybersecurity firm, conducted research into the valuation of data on the dark web. The dark web serves as a hub for various personal information, including IDs, passports, emails, and financial data. This exploitation takes advantage of the extensive digital footprint left by individuals, much of which is accessible to large corporations. NordVPN's analysis revealed that around 720,000 items were sold for an estimated total of $17.3 million. They noted that the dark web encompasses over 30,000 websites, constituting only 4 percent of the internet, which is accessible to online users.

The cost of items on the dark web varies based on multiple factors, such as their difficulty to replicate, demand, and the level of security implemented by the respective countries. For instance, the average price for Slovakian or Lithuanian passports was around Rs 294,813, while Indian passports were priced at approximately Rs 776, reflecting the complexity involved in hacking them. Accounts like Uber, Netflix, and Twitter ranged in prices, with hacked Uber accounts costing around Rs 930.9, Netflix at Rs 751, and Twitter at Rs 155. Cryptocurrency and investment accounts were valued higher than payment processing or bank accounts, with the most expensive being Binance at Rs 30,567. Hacked email accounts were also listed, valued at approximately Rs 1,241 globally, while Indian email accounts cost around Rs 776.

Users are advised to be vigilant regarding the data they share on sites and how it relates to the activities being carried out, emphasizing the importance of protecting personal information online. (Correspondent, 2022)

Case study 2 - Government Portal Hacking

Living in the IT world and everything being computerized, hacking of portals has been a concern. There are multiple instances of government portals being hacked. Government portals hold a lot of data and hacking of it can be a serious issue and it's an offense. This offence once proven can lead to rigorous punishment and imprisonment. With the UK and the US being ahead of several developing countries such as India. Hacking the portals has been a simple task.

Government portals are well maintained but badly established. The encryption is very basic and hacking is simple. Several state portals of states like Orissa and Assam were hacked multiple times in under 20 days in 2018. The ministry of Defense and Home Affairs, Law, Labor and over 100 websites were hacked. The supreme court website of India has been hacked right after the judgment of Justice Loyala's death was given out. The website was hacked by a server based in Brazil and the Supreme court website had a marijuana leaf as its logo and the phase hacked by Brazil hitech team in its bio. Ankush Johar, director of infosys ventures which is the leading software solutions told that this cyber crime is increasing and UK and US are majorly responsible for it due to their accessibility. Russia on the other had is threatening us for a cyber war and with our portals being hacked regularly this could lead to a serious issue if neglected.

The ministry of Electronics and I.T confirmed that the website was hacked and efforts were made instantly to get back the website under control and to restore data and look deeper into the incident. Keeping this in mind is Indian infrastructure ready to go against highest ranking technical counties like UK, US and Russia on a cyber war? When people give out their information about the card and account of a individual the details are sold online in the dark web. The sold details can be used by the hacker to drain all the money in the account and this is an offense. Government portals have a lot of chaos in their homepage. The website of the supreme court of India had a lot of unnecessary information and and posts that were running in their homepage. This is mainly because of the number of languages that our country has and managing all the sites as a priority is a task, failing in this task leads to hacking. Citizens of India give out all information to an official government website on a trust that their data will be safe. But due to increased hacking of government portals, people are now thinking twice before logging in to a official government website and the best example for that is the hacking of the Supreme Court India's website.

Case study 3- Usage of the Dark Web to hire Hitman

A hitman, commonly associated with organized crime, is a hired individual tasked with killing someone, while a female undertaking the same is referred to as a "hitwoman." Despite the romanticized portrayal of contract killings in movies, the reality of such transactions is grim and illegal.

Websites like Azerbaijani Eagles and Slayers Hitmen operate on the dark web, offering murder-for-hire services. For example, Azerbaijani Eagles claims to perform a murder for $5,000, while Slayers Hitmen provides options ranging from a beating for $2,000 to death by torture for $50,000. However, experts and law enforcement assert that these sites are primarily scams, and there is no known murder attributed to their services. (Popper, 2020)

Yet, these websites serve as hubs for individuals genuinely seeking to pay for someone's murder. Some individuals have been apprehended by law enforcement after attempting to engage these services. For instance, an Italian faced charges for hiring a "dark web hitman" to kill his ex-girlfriend, paying around €10,000 in Bitcoins for the job.

The investigation primarily centered on the suspect's process of acquiring the Bitcoins used for the payment, rather than on tracing the hitman's Tor network connections or linking the bitcoins to the alleged assassin. Fortunately, many so-called dark web hitmen are revealed as scammers, providing a layer of protection for those attempting such transactions. Consequently, those who engage in secret online dealings to arrange murders are unlikely to report to authorities if the individual on the other end absconds with their cryptocurrency.

Case study 4 -Dark web for counter terrorism

The analysis of the dark web plays a crucial role in counterterrorism efforts. Currently, terrorist attacks pose one of the most significant challenges to humanity, with the world consistently threatened by these meticulously planned, technologically advanced, and well-coordinated operations. Terrorists create various websites on the public internet where they exchange ideologies, spread propaganda, and recruit new members anonymously. The dark web serves as a platform for terrorists to communicate and propagate their messages. Nations worldwide are prioritizing counterterrorism measures.

Utilizing dark web analysis can serve as a proactive approach to counterterrorism, effectively detecting and preventing terrorist threats and attacks. This study proposes a model for dark web analysis focused on examining forums within the dark web for counterterrorism purposes. The aim is to protect nations from potential terrorist threats and attacks. (Sachan, 2012)

The study references the "International Terrorism: Attributes of Terrorist Events" data file from the Office of Political Research of the Central Intelligence Agency (ITERATE file), examining both overt and covert threats posed by international terrorism. Independent expert analyses conducted on threats and other factors extrapolated from the ITERATE file demonstrated limited correlations.

Interview: Youth accessing the dark web

In an interview with one of the active user of this web, when he was asked certain questions starting with- How and when did you start accessing the dark web ? He responded saying, he was introduced to this platform by one of his friend’s back in 2016 to fetch information on Political blogs, dark hat chats platforms buying illegal stuff and watching things that are only available on the dark web. He also claimed that one of the few things that dark web doesn’t posses are ethics of any sort anyone can access this web page and can do anything adding to it, first things first it’s not at all safe as someone might be looking into our system or just mirroring through our web camera and things can really get a lot worse if one don’t take the basic precautions rest if they presently minds their stuff then there’s nothing to stop one from purchasing what they desire. The things that aren’t ethical on dark web varies from things like rape pornography to online torture houses and wherever our wildest imaginations takes its all somewhere there on dark web. The person also added precautions to buff up before taking a dive in the dark web are as follows.

1: Always use something to cover your webcam.

2: The VPN should be certified enough that it’s firewalls aren’t that easy to bulldoze.

3: Never share anything personal, even the name.

ANALYSIS

The data breach at Kashmir University on August 11, 2022, underscores the growing threat to individuals' privacy and the lucrative market for stolen personal information on the dark web. The university's swift response and establishment of a dedicated IT team demonstrate a commitment to addressing the issue. The alarming valuation of data, estimated at $17.3 million by NordVPN, highlights the extensive reach and profitability of the dark web. The varied pricing based on the type of information reflects the diverse demands of cybercriminals. This incident underscores the critical need for heightened online security measures and user vigilance in safeguarding personal data against potential breaches.

The second case study highlights the vulnerability of government portals to hacking, particularly in countries like India where cybersecurity measures are deemed inadequate. The instances of hacking in various ministries and state portals underscore the potential risks associated with poorly established and minimally encrypted government websites. The mention of cyber threats from countries like the UK, US, and Russia raises concerns about the readiness of Indian infrastructure for a cyber war. The aftermath of such breaches, including the sale of individuals' information on the dark web, not only poses financial risks but also erodes public trust in government websites, as seen in the hesitancy of citizens to share sensitive data online.

The usage of the dark web to hire hitmen represents a disturbing intersection of criminal intent and digital anonymity. While platforms like Azerbaijani Eagles and Slayers Hitmen claim to offer murder-for-hire services, experts emphasize that such sites are often scams. Law enforcement focuses on tracing financial transactions rather than Tor network connections, as seen in a case where an Italian attempted to hire a hitman for his ex-girlfriend. The prevalence of scams within this illicit market may inadvertently protect potential victims, but the dangerous allure of these online transactions underscores the need for robust cybersecurity measures and international cooperation to combat such criminal activities effectively.

The proposal to employ dark web analysis as a proactive counterterrorism measure is commendable, given the escalating threat of technologically sophisticated terrorist activities. The emphasis on scrutinizing dark web forums aligns with the clandestine nature of terrorist communication. However, the study's reliance on the ITERATE file reveals limited correlations between dark web activities and identified threats. A critical examination of these independent analyses is essential to refine the proposed model. While the dark web is undoubtedly a breeding ground for extremist ideologies, refining the approach by integrating diverse data sources and addressing the identified limitations will enhance the effectiveness of the counterterrorism strategy.

The interviewee's admission of accessing the dark web since 2016 for political blogs, illicit transactions, and disturbing content highlights the platform's diverse and often nefarious offerings. Their acknowledgment of the dark web's lack of ethical boundaries and potential risks, including privacy invasion and cyber threats, underscores the inherently hazardous nature of this hidden online realm. The casual attitude towards purchasing desired items, coupled with the mention of unethical content ranging from rape pornography to online torture houses, serves as a stark reminder of the darker aspects of the internet that elude conventional scrutiny. The interviewee's cautionary tone emphasizes the importance of taking basic precautions when navigating the treacherous terrain of the dark web.

FINDINGS

Data breaches are prevalent on the dark web, where a vast range of personal data, from passports to credit card details, is readily available for sale at alarming prices. The digital era has made our information vulnerable to hacking and sale on various illicit websites. The lack of ethics on the dark web means that anything, no matter how sensitive, can be sold and accessed by hackers. This has been evident through numerous news articles reporting data breaches.

The use of cryptocurrencies like Bitcoin and Ether has facilitated a new wave of criminal activity. The global reach of these currencies allows buyers from any part of the world to make payments anonymously and swiftly, enabling transactions without direct communication between the parties. While cryptocurrency hasn't entirely transformed the criminal landscape, it has certainly streamlined illegal transactions.

The case of government portal hacking highlights the minimal security and functioning of these portals. Citizens often provide personal information on these portals, assuming it's secure. However, the ease of hacking raises concerns about the government's lack of robust coding and system improvements. Despite claims of reforms, the situation remains unchanged. Some portals collect monetary data, which, if hacked, can lead to substantial financial losses, with poor tracking capabilities.

Regarding murder-for-hire schemes on the dark web, despite many being scams, there are persistent attempts to hire contract killers. An intriguing finding was that the pricing structure of these sites mirrored real-world prices for such illicit services. Those seeking such services often believe they are connecting with individuals having criminal or military backgrounds, and investigations often start from email or contact information provided by scammers.

The concept of cyber terrorism, despite persisting for over two decades, lacks a precise definition or comprehensive case studies that validate its existence. Scholars have debated whether it's a tangible threat, examining potential perpetrators and their motives. High-profile terrorist events like the 1993 World Trade Center bombing led to discussions on cyber terrorism, prompting the US Department of Defense to conduct cybersecurity tests in 1997 and address the growing cyber threat scenario brought forth by the Marsh Commission report.

This reiterates the importance of tackling data breaches, understanding the implications of cryptocurrencies in criminal activities, and clarifying the concept and potential risks of cyber terrorism in today's digital landscape.

CONCLUSION

The study highlights that the dark web has evolved into a complete online platform supporting unlawful activities. This has directly or indirectly fostered illegitimate actions worldwide, connecting multiple countries through the internet and enabling unethical use of the website. The platform not only facilitates the sale of illegal substances but also serves as a hub for coordinating terrorist operations, connecting with hitmen, and conducting various criminal activities under its shelter. Cybersecurity threats are significantly elevated as the dark web presents a substantial risk of divulging personal information, including names and locations through IP addresses.

Countries and major international organizations are consistently working to safeguard the cybersecurity landscape. Despite its association with nefarious activities, the dark web is also utilized by governments to counter terrorism. Ultimately, the impact of the dark web is contingent upon the end users. As a recommendation, this study underscores the necessity for more stringent regulations and guidelines to serve as a gatekeeper against illicit activities in this realm.

REFERANCES

- Aulakh, G. S. (2023, August 2). NordVPN data on the dark web valued, reveals research study. Indian Express. https://indianexpress.com/article/technology/tech-news-technology/nordvpn-data-dark-web-value-research-study-7962906/
- The Hindu. (2023, August 4). Kashmir University starts probe after alert on students' data sale on dark web.https://www.thehindu.com/news/national/other-states/kashmir-university-starts-probe-after-alert-on-students-data-sale-on-dark-web/article65754560.ece
- Vieira, H. (2017, November 6). Dark web: The economics of online drugs markets. The Magazine of LSE’s Centre for Economic Performance. https://blogs.lse.ac.uk/businessreview/2017/11/06/dark-web-the-economics-of-online-drugs-markets/
- Mazi, H., Arsene, F. N., & Dissanayaka, A. M. (2020). The Influence of Black Market Activities Through Dark Web on the Economy: A Survey. In Midwest Instruction and Computing Symposium https://www.micsymposium.org/mics_2020_Proceedings/MICS2020_paper_2.pdf

- United Nations Office on Drugs and Crime. (n.d.). Darknet and cryptocurrency: A comprehensive analysis. https://www.unodc.org/documents/Focus/WDR20_Booklet_4_Darknet_web.pdf
- Finklea, K. (2015, July 7). Dark Web. Specialist in Domestic Security. https://digital.library.unt.edu/ark:/67531/metadc700882/m1/1/high_res_d/R44101_2015Jul07.pdf
- Christin, N. (2020). Darknet markets. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598902
- Subramanian, A., & Raj, R. G. (2019). Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. ResearchGate. https://www.researchgate.net/publication/331867659_Dark_Web_and_Its_Impact_in_Online_Anonymity_and_Privacy_A_Critical_Analysis_and_Review
- Westerlund, M. (2021). Cybersecurity in the Dark Web: A study of online anonymity services. Uppsala University. https://uu.diva-portal.org/smash/get/diva2:1792762/FULLTEXT01.pdf
- Choudhary, M., Singh, M., & Singh, P. K. (2021). Dark web and its challenges: A comprehensive review. IEEE Xplore. https://ieeexplore.ieee.org/document/9740785
- Yoran, A. (2007). What is the dark web, how to access it, and what you'll find. CSO Online. https://www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
- Kumar, A., & Chouhan, S. (2019). Dark Web: An in-depth exploration. Journal of Emerging Technologies and Innovative Research. https://www.jetir.org/papers/JETIREQ06074.pdf
- Perlroth, N. (2020, March 4). Can you hire a hitman online? The New York Times. https://www.nytimes.com/2020/03/04/technology/can-you-hire-a-hit-man-online.html
- Vincent, J. (2019, October 21). What is the dark web and how does it work? BBC News. https://www.bbc.com/news/technology-50150981
- Jones, H. (2023, June 9). Russian-linked hackers taunt HWL Ebsworth over data breach. ABC News. https://www.abc.net.au/news/2023-06-09/russian-linked-hackers-taunt-hwl-ebsworth-over-data-breach/102461608
- News.com.au. (n.d.). NSW man, 55, arrested for allegedly dealing drugs on the dark web. https://www.news.com.au/technology/online/internet/nsw-man-55-arrested-for-allegedly-dealing-drugs-on-the-dark-web/news-story/61a406987b46f51b445e3de96c262455