LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 1 | Issue 4

2024

DARK WEB : UNVEILING THE PATHWAYS TO CRIMINALITY IN THE CYBER UNDERGROUND

Gnanavel.L[1]

I. ABSTRACT:

This research paper delves into the intricacies of the Dark Web and its impact on internet users, focusing on privacy, security, and the perpetration of cybercrimes. The advent of the Internet in the 20th century paved the way for the World Wide Web, transforming communication and information exchange globally. However, the ease of quick communication also raised concerns about privacy and security, particularly with the emergence of the Dark Web. The Dark Web constitutes a small but significant part of the Deep Web, requiring specialized software like the Tor browser for access. This hidden online environment facilitates both positive, secure communication and nefarious activities, creating a dichotomy. The research objectives include evaluating cybersecurity threats, analyzing societal impacts, and examining measures to regulate the Dark Web and reduce crime rates. The overview on the Dark Web explores its origins, structure, and access methods. Tor, developed by the U.S. Naval Research Laboratory, plays a crucial role in accessing the Dark Web by employing onion routing for anonymity. Also, this paper highlights the three layers of the internet – Surface Web, Deep Web, and Dark Web – each serving different purposes. The criminal activities associated with the Dark Web are discussed, ranging from cyber terrorism and illegal markets to hitman hiring and information leakage. The paper sheds light on the challenges law enforcement faces in combating crimes on the Dark Web due to its encrypted and anonymous nature. The importance of legislative frameworks and law enforcement efforts is emphasized to curb cybercrimes and protect individuals' security and privacy. In conclusion, the research underscores the significance of understanding the Dark Web's dynamics to combat cybercrime effectively.

[1] Student – IV th year B.Com. LL.B (Hons),School of Excellence in Law [SOEL], The Tamil Nadu Dr Ambedkar Law University, Chennai, TAMILNADU. Email: Gnanavell2002@gmail.com

 (ISSN: 2583-7753)

II. KEYWORDS:

Dark web, Security, Privacy, Illegal activities, Crime.

III. INTRODUCTION:

The World Wide Web, an information system that allows people all over the world to exchange information, has been rendered possible by the Internet. With the advent and introduction of Internet during the 20th century the technological developments also started to bloom slowly around the world. Since the majority of people visit websites to fully satisfy their demands, internet safety has become a critical topic of worry in today's technologically advanced society. The mid-1990s saw the Internet continue to flourish and change a great deal of things. The primary shift is the ease of quick communication. You can instantaneously communicate with anyone if you're connected to an Internet connection. However, the biggest worry is that privacy, security, and anonymity were not considered while designing the Internet. Thus, everything can be monitored, tracked or traced etc. The Growth of Internet technology though can be seen as great deal on one side, but on the other side it can be seen as a dangerous threat to privacy of every Internet User.

Scientists, programmers, and engineers of the next generation built the internet, commonly referred to as the "information superhighway." The surface, deep, and dark webs are the three main layers that make up the internet. The websites that are accessible to the general public using common search engines like Google, Yahoo, and Bing are collectively referred to as the surface web, sometimes known as the open or transparent web. Websites that are inaccessible through conventional engines like Google since the search engines are unable to index them are part of the deep web, also known as the invisible web. These websites need to be accessed through login or payment methods because they are password- or paywall-protected. A portion of the deep internet that needs special software to access is called the dark web, or darknets. This is sometimes mistaken for the phrase "deep web," which refers to any website that a standard web browser cannot visit directly. Around 90% of the internet is made up of the deep web, however less than 5% of the internet is made up of the dark web, which is a very minor portion of the deep web. Thus, this paper delves into the

understanding the dark web and how it is in recent times used as a tool to exploit the internet users also affecting the privacy and data. This research paper also focusses on how the cyber crimes happens under the blanket of Dark web and various measures to curb the crime.

IV. RESEARCH OBJECTIVES:

- To evaluate the Cyber security threats.
- To analyze the Impact on the Society.
- To Examine and anlayse the various measures available to completely curb and regulate the dark web and reduce crime rates.

V. RESEARCH METHODOLOGY:

The research has embraced the doctrinal method of research relying mostly on the available secondary sources. The Sources include Government reports, Journals, Websites, Books, Articles, and other mass media sources on Dark web. Therefore, the pertinent information on the dark web and crime has only been evaluated and interpreted from the sources and used in accordance with the requirements of the research.

VI. AN OVERVIEW ON DARK WEB:

The internet was invented in the late 1960s by the Advanced Research Project Agency Network, also known as ARPANET. ARPANET was created with funding from the US Department of Defence to facilitate information sharing among government researchers by allowing several computers to connect to a single network. The Transmission Control Protocol and the Internet Protocol, or TCP/IP, is a communication model that was developed in the 1970s by Vinton Cerf and Robert Kahn. The standards for data transmission between several networks, as opposed to just one, are established by TCP/IP. The "dark web" is a secret online environment where both good and evil can be found. Positively, the dark web offers extremely secure, anonymous communication channels to cover up government activity that is

secret and to shelter reformers like journalists and human rights advocates from repressive foreign regimes.

Unfortunately, the dark web has become a major center for illicit trade; it is a fully operational marketplace where covert buyers and sellers can transact with relative confidence, frequently displaying customer reviews similar to those found on open websites. The Onion Router (TOR) is one such piece of software that is utilized to access a large portion of the dark web. This free program is powered by the TOR and makes use of "onion routing." . The dark web is an online community that is a portion of the worldwide web platform that search engines do not index and to which access requires authentication. In order to access the dark web pages, one may need to use specialized software, like proxy software, in accordance with this authorization. The drug trade, the sale of firearms, and human trafficking are a few instances of the dark web.[2] There are several justifications for avoiding the dark web. It is, nevertheless, a location that is as worthwhile to visit. Not everyone should use the dark web, although there are some worthwhile resources there. A few instances of dark web websites are Ahmia, ProPublica, Secure Drop, Tor, and Duck Duck Go. To hide its commerce in a variety of illicit goods, including opioids and various other drugs, bomb parts, small and large weapons, pornography involving children, social security information, body parts, and even criminal activity for hire, the unlawful component of the dark web depends on anonymizing technologies and cryptocurrencies.[3] The anonymity of the dark web not only promotes illicit activity but also puts many law enforcement organizations mostly in the dark about its existence, despite the fact that online transactional crimes are occurring within their territories.

VII. THE INTERNET'S STRUCTURE:

The Internet is a big part of our daily lives these days. It is become a necessary component of everyday living. The Dark Web is essentially an undetectable hidden

[2] Henderson, L, *"The Tor and the dark art of anonymity",* (Volume. 1) *2022.*
[3] Diodati, J., & Winterdyk, J., *"Dark Web: The Digital World of Fraud and Rouge Activities. In Handbook of Research on Theory and Practice of Financial Crimes"* (pp. 477-505), (2021). IGI Global.

component of the Internet that is used to access and store private and sensitive data. The World Wide Web is made up of three sections. They are:

1. ***Surface Web:***

   Anything that appears on the internet as a whole is referred to as the surface web, which is additionally referred to as the publicly accessible web, indexable web, or Clearnet. The surface web consists of what consumers often browse during their daily routines. The general public can access it through common search engines and normal web browsers that don't need any extra setup, like Google Chrome, Mozilla Firefox, and Internet Explorer from Microsoft or Edge [4]. The surface web includes sites like Google or Yahoo, Facebook, YouTube, Wikipedia, blogs on a regular basis, and pretty much whatever we can see on the results page of any search engine.

2. ***Deep Web:***

   The following component is the deep web, sometimes referred to as the invisible or hidden web because it is separate from the outermost web. People can freely share their opinions and protect their anonymity thanks to the deep web. For countless innocent people who are harassed by criminals and other criminals, privacy is crucial. It is used to maintain the privacy and anonymity of online activities, which has uses in both legitimate and illicit contexts. It has been known to be used for extremely unlawful activities, even though some people use it to get around government censorship[5].Emails, conversation chats, secret content on social media platforms, electronic bank statements, and more are examples of the Deep Web.

3. ***Dark Web:***

   The latter section is known as the "Dark Web." The University of Edinburgh researcher Ian Clarke's 2000 thesis project, Free Net, which sought to create a "Decentralized Distributed Data Storage and Access System," has been

[4] Jamie Bartlett, *The Dark Net: Inside the Digital Underworld,* 2014.
[5] Lightfoot, S., & Pospisil, F. "*Surveillanceon the deep Web.*" ResearchGate, Tech. Rep. (2017).

connected to the start of the dark web. Clarke aimed to provide a novel approach to data sharing and anonymous online communication.[6] The dark web is an area that is a portion of the worldwide web platform that search engines do not index and to which access requires authentication. In order to access the dark web pages, one may need to use specialized software, like proxy software, in accordance with this authorization. To mention a few, the drug trade, the sale of firearms, and human trafficking are some instances of the dark web.

VIII. GETTING ON THE DARK WEB – WAY OF ACCESSING IT:

The dark web is one of the most popular concepts on the internet. It is impossible to estimate the size of the dark web, but one thing is certain: the deep and clear webs fade in comparison. A website is made up of one HyperText Markup Language, or HTML, document on each page. A web browser may display text, graphics, and other multimedia on a page by using the markup language. A browser for the internet is a piece of software for browsing websites. Web browsers that are commonly used include Internet Explorer, Firefox, Chrome, and Safari. A web server is an electronic software that stores and sends data to other computers over a network. Whenever an internet user accesses a web page from a specific website, the browser gets its files from the web server and shows the page on the user's computer screen. There is a great difference between the Web browser and the search engine. Also in addition the web browsers serves the user with additional dynamic features than the search engine.

Standard search engines do not provide access to the content on the dark web. Internet users need specialist software, like the Tor browser, in order to access the black web. The U.S. Naval Research Laboratory created Tor, also known as The Onion Router, in the middle of the 1990s to safeguard American intelligence communications transmitted over the internet. It uses a technique called "*onion routing,*" which hides the origin and destination of data transferred over a network by using several

[6] Senker C, "*Cybercrime & the Dark Net: Revealing the hidden underworld of the internet*", Arcturus Publishing. (2016).

encryption layers and randomly selected relay servers, or nodes. More specifically, each of the three levels of internet nodes that comprise the Tor circuit are used by Tor to anonymously send encrypted data. Users' data is transferred into the Tor circuit in the very first layer when the Tor browser connects at random to an entrance node that is known to the public. The data is completely secured and routed via several nodes in the second layer. Moreover, each node only has knowledge of the identities of the nodes that come before and after it in order to maintain anonymity. After passing through an exit node on the Tor circuit and arriving at the ultimate server destination, data are decrypted at the last and third layer. It is entirely lawful to use and free to download the Tor browser. However, Tor is either prohibited by national authorities or illegal in nations including Saudi Arabia, China, Russia, and Iran .The fact that the browser used by Tor is not perfect is noteworthy. For instance, even though a user's location and browsing behaviour are hidden when using the Tor browser, the individual's Internet Service Provider (ISP) continues to know that the user is using Tor. Furthermore, as the owners/operators of such nodes will be able to determine the users' true IP addresses, Tor is unable to block monitoring at both entry and exit node of its network. [7]

IX. CRUCIAL ACTIVITIES ASSOCIATED WITH THE DARK WEB: THE CRIME SIDE:

The criminal underside of the dark web covers its trade in a wide range of illicit goods, including body parts, explosives, tiny and large weapons, child pornography, financial information, and even unlawful activities for hire. They do this by using anonymizing technologies and cryptocurrencies. The anonymity of the dark web not only promotes illicit activity but also maintains many law enforcement organizations mostly in the dark about its existence, despite the fact that online transactional crimes are occurring within their territories. The criminal underside of the dark web covers its trade in a wide range of illicit goods, including body parts, explosives, tiny and large weapons, child pornography, financial information, and even unlawful activities

[7] Ngo, F. T., Marcum, C., & Belshaw, S. (2023). *"The Dark Web: What Is It, How to Access It, and Why We Need to Study It."* Journal of Contemporary Criminal Justice, 39(2), 160-166. https://doi.org/10.1177/10439862231159774

for hire. They do this by using anonymizing technologies and cryptocurrencies. The anonymity of the dark web not only promotes illicit activity but also maintains many law enforcement organizations mostly in the dark about its existence, despite the fact that online transactional crimes are occurring within their territories. Let's discuss about the various ways in which the Darknet in used as an tool or pathway to commit illegal and criminal activities:

- **Cyber Terrorism and Cybercrime** - On the dark web, both individuals and well-organized groups are capable of committing cybercrime or acts of terrorism. Cybercrime is becoming more and more accessible to anyone looking to commit low-risk crimes and still make a difference.[8] The Cyber terrorism has now became an increasing act where the cyber terrorist group tries to target a particular area or country and threatens the government and the citizens. It is so hard to find out those criminals as there is problem of many technological obstacles.

- **Illegal Markets and Products** - Over the years, online marketplaces such as Silk Road, Hansa, and AlphaBay have gained popularity by facilitating the exchange of illegal commodities such as illegal substances, firearms, credit card details stolen, stolen identities, and child pornography, among other things. One of the very first significant online markets of this kind, Silk Road had monthly sales of about USD 1.2 million, mostly of drugs and restricted substances.[9] The route promoted trade in a variety of goods in addition to silk, including animal skins, metal and wood products, precious stones, grains, fruits, vegetables, and other textiles. Although guns are also a common item on these markets, the sale of illegal substances takes precedence.

- **Cloning onions** - Cloning onions is an alternative technique. when the fraudster copies the actual webpage and modifies it to direct users to their fictitious websites. This is a fraud intended to defraud users of their money.

[8] Chesney, B., & Citron, D. (2019), "*Deep fakes: A looming challenge for privacy, democracy, and national security.*", Calif. L. Rev., 107, 1753.
[9] Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). "*Drug sales on darkweb cryptocurrency markets: distinct routes, dangers, and benefits*", The British Journal of Criminology, 60(3), 559-578.

Example in recent times the popular e-commerce websites like Amazon, Flipkart are being onion cloned and selling the original products at very low cost using these websites.

- **Red Room** - A popular fable or myth is said to surround a red room. The rumour states that on "Red Room" dark web sites, people pay thousands of dollars to watch murders and rapes occur in real time. On the "dark web," there is a secret website or platform where users can watch or take part in interactive murder or torture. A concealed network of websites that can only be accessed using a specialized web browser is known as the "dark web."[10] It serves to maintain the privacy and anonymity of online activities, which has uses in both legitimate and illicit contexts. It has been known to be used for extremely unlawful acts, even though some people utilize it to get around government censorship. To access the black web, you must use the Tor anonymous browser.
- **Hitman Hiring** - The underground internet platform offers the ability to hire a skilled assassin. Among the organizations involved in murder-for-hire are Hitman Network, Unfriendly Solution, and others. The only form of payment accepted for the unfriendly group solution is bitcoin.
- **Gateway to the Surface Web** - The surface web is also accessed by a large number of non-military users through the Tor darknet infrastructure, or through hidden service versions of well-known surface websites like Facebook (e.g. media), ProPublica (news), DuckDuckGo (search engines), and other services that might be restricted locally or raise privacy/ad tracking concerns. The Dark web is also used to view the blocked pornographic websites to view porn videos and also to watch the child pornographic contents which is strictly restricted in many countries.
- **Information Leakage**: TOR is one of the most effective methods available to activists, law enforcement, and whistleblowers. There are numerous of unidentified or ignorant support systems available. The dark web is used by

[10] Beckstrom, M., & Lund, B. (2019) "*Casting light on the Dark*" Rowan & Littlefield.

hackers to reveal important information. Employees are compensated by dark web hubs for disclosing company secrets, as evidenced by the 1.4 billion personal data exposed in text form on the dark web in 2017.

X. SUGGESTIONS:

Dark Web networks like TOR have made it possible for criminals to exchange both legal and illegal "goods" in a variety of anonymous methods. The Dark Web is becoming more and more popular, particularly when it comes to illicit goods and activities. Proactive problem-solving and removal strategies should be implemented by protection processes. The Government should also keep an active eye on the functioning of the cyber world and should formulate rules and regulations to regulate. Its an alarming time in need for special legislature and a framework for the Cybercrime. The Government should also enact laws and special statues to govern and regulate the cyber areas. Finding and accessing the "hidden" websites and content on this portion of the internet is a substantial difficulty for academics and researchers interested in researching the dark web. As stated already, the dark web is made up of anonymous websites that are not indexed by regular search engines. The Law enforcement agencies must be promoting knowledge concerning the dark web between local and state governments. Also forming alliances between agencies which cover jurisdictions. In addition, expanding and improving training to give police the tools they need to recognize behaviour and evidence from the dark web. It is essential to take measures and address the problem of the hidden nature of the dark web in order to safeguard people's security and privacy.

XI. CONCLUSION:

The research examines the impact of the Dark Web, its secrecy and confidentiality, and the amount of anonymous people that access globally, as well as the influence of websites with hidden resources on the Dark Web. Technology is playing a bigger role in the privacy vs. security issue than it did in the past because it is now not only a question of legality but also of technical capacity to monitor and spy individuals. This discussion may not be necessary in the future if technology develops to the point where people and private companies control privacy instead of governments. After

that, the conversation on this subject moves outside of the realm of technology and requires consideration by professionals in the fields of law, sociology, psychology, and other fields. Therefore, understanding the dark web and its effects on society is essential to fighting cybercrime and safeguarding civilians from cyberattacks. I'm hoping that these prevalent problems will spur more investigation into the dark web in the future, along with increased efforts to combat online crime and victimization. Incognito as a mask for illicit activity and anonymity for privacy's sake are two very different things. Since the dark net is encrypted, governments have significant challenges. As such, every nation should prioritize developing new systems for monitoring and stopping illicit and destructive activity on the hidden web.

XII. REFERENCES:

1. Srinjoy Saha," *Dark Web: The Hub of Crime*" International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue IX Sep 2022.
2. Davenport, D., "*Anonymity on the Internet: why the price may be too high. Communications of the ACM*", 45(4), 33-35 (2002).
3. Gupta, Maynard & Ahmad , "*The Dark Web Phenomenon*", Australasian Conference on Information Systems 2019, Perth, WA.
4. Ngo, F. T., Marcum, C., & Belshaw, S. (2023). "*The Dark Web: What Is It, How to Access It, and Why We Need to Study It. Journal of Criminal Justice,*" 39(2), 160-166.
5. Hong, N. "*Silk road creator found guilty of cybercrimes.*" *Wall St J* 4 (2015): 2015.
6. Diodati, J., & Winterdyk, J. (2021). "*Dark Web: The Online Fraud and Rogue Activity Universe. In the Handbook of Research on Financial Criminology Theory and Practice*" (pp. 477-505). IGI Global.