Amity Journal of Computational Sciences (AJCS)
ISSN: 2456-6616 (Online)
Volume 6 issue 1 July-Dec 2022

Modern World Dark Web: *A Theoretical Perspective*

Ranjana Rajnish
Amity University
Uttar Pradesh. Lucknow
rrajnish@lko.amity.edu

***Abstract*—21st century is the era of digital technology where most of the information is online. People can share information and connect with any part of the world with just a click. The web visible to an ordinary user seems like a vast knowledge resource, but it is just the surface of the web. In reality, there is a lot more to the Internet. The websites we are able to access are approximately 4% of the whole web. The other 96% of the web is hidden and invisible. This invisible, deeply hidden, non-indexed web is generally known as the deep web. Every technology has pros and cons of it, and the same is the case with the Web. A very small portion of the web, known as the dark web, has gained a lot of attention over the last few years. Dark Web is the portion of the world wide web which is not indexed by the conventional search engines and thus does not appear in the result of such search engines. Specific browsers, such as Tor browser are used to access the contents of the dark web and due to its nature of design the search through the browser is anonymous. Anonymous search was designed for certain benefits, but it has some drawbacks also, which make us think about putting some regulations in place. In this paper we are discussing about the regulation for the use of dark web with respect to Indian Perspective.**
This paper explores the concept of Open Web, Deep Web and Dark Web. It then explores the activities that are operated under the dark web, benefits and drawbacks of the dark web, legality of dark web. Paper then concludes with the need of regulations of the dark web with Indian perspective.

***Keywords*— Open Web, Deep Web, Dark Web, Legal aspects, Regulations.**

I. INTRODUCTION

The web as whole is a collection of web pages that are stored on multiple computer networks. These web pages are accessible through various search engines such as Google, Firefox, Yahoo etc. Web pages that are indexed on these search engines and can easily be accessed through such search engines are collectively termed as open web. Another important segment of the web is the part of web the portion that can be accessed through the username and password, or maybe by knowing the exact link, come under the category of deep web. The third category or segment of the internet consists of the web pages that are not indexed on traditional search engines and cannot be accessed through them are part of the web that is known as Dark Web. To access the contents of the dark web, specialized browsers like Tor (The Onion) have been developed. Such browsers were developed for providing privacy during the session and thus provide anonymous access to the dark web content. This feature of anonymity is being used by the criminals for various illegal activities like hacking, drug trafficking, child trafficking, arms trafficking, selling of all such products that are not legal in market otherwise.

As discussed, the dark web is mainly used for illegal purposes. We can better understand the magnitude of this problem by examining statistics. According to the literature, 57% of activities on the dark web are illegal, including data breaches, illegitimate drugs, pornography, human trafficking, and more [8]. A study conducted by the University of Surrey found the total revenue generated from cybercrimes in 2018 was approximately $ 1.5 trillion [9], and cybercrimes will become more frequent and aggressive over time.

This paper explores different aspects related to the dark web and then why it is important to have government regulations to regulate such activities.

II. OPEN WEB, DEEP WEB AND DARK WEB

Search engines like Google, Bing, and Yahoo can search and index websites because of links. They use links to rank search results according to things like relevancy, inbound links, and regular keywords. Regular browsers search the surface web but that's where the search stops. To explore more, let us understand that the web content is available for search in three models:

1. Free content that can be searched by popular search engines
2. Content that is accessible on a payment basis
3. Content that is accessible by logging in to the website

Based on access (using popular search engines like Bing, Google, or Yahoo) we categorize the web into three categories:

A. *Open/ Surface Web*- Open web is a small part of the web that be easily accessed using popular search engines.

B. *Deep Web– The password-protected web, or paid services, subscription services like Netflix, databases (academic databases) or, web pages that can only be accessed through an online form (email services) forms the deep web.*

C. This may directly not be accessible through popular search engines but is accessible if the link is known.

D. *Dark Web*- Dark web is the part of the web that has hidden IP addresses and cannot be directly accessed through popular search engines. Accessing such sites requires specific tools and is hidden for the popular search engines. It is said that most of the dark web is engaged in illegal activities like Credit Card details data, Weapon selling websites, Drug selling websites, Selling of stolen products, etc.

In this section, we will focus on the Dark Web. The dark web originated in the mid-1990s by the United States Naval Research laboratory employees to protect US intelligence communications. Though developed with a bonafide intention, it, in the latter part, became a place for criminals to shoot their ill-minded activities.

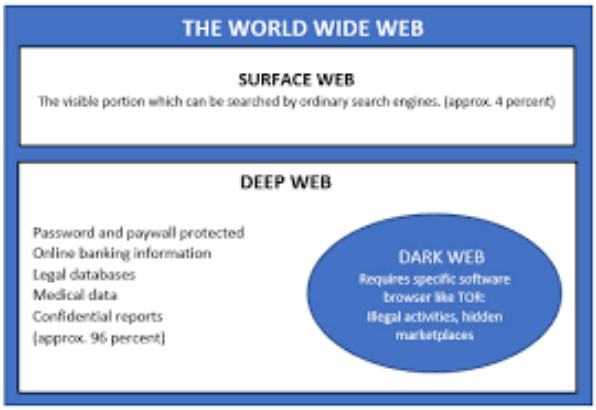

Figure 1: Types of Webs

Open web is just like the tip of iceberg, and majority of web pages are either, part of Deep web, or of the Dark Web. Dark Web is very small as compared to Open Web or the Deep web and accounts for less than 0.01% of the sites on the internet [1]. As mentioned, dark web cannot be accessed by regular search engines and is accessible through search engines designed for this specific purpose. One such commonly used browser is The Onion Router – "Tor". Tor allows to access the web anonymously and makes it nearly impossible to trace the user or the sites a user has accessed. Because of this nature of anonymity, it has become synonymous to criminal activities.

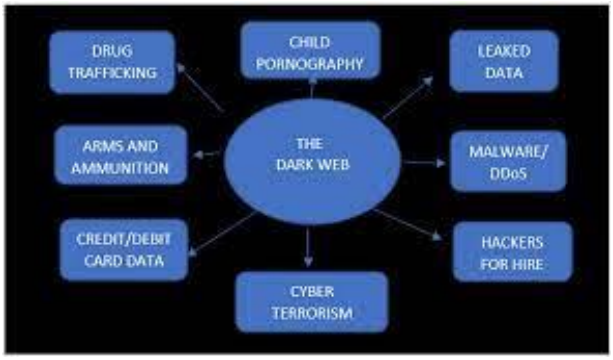

Figure 2: Types of activities in a Dark Web

Dark web has been existing from a long time but it has become very popular after 2013, when Ross William Ulbricht, operator of Silk Road was arrested (Sui, Caverlee, and Rudesill 2015). Silk Roads was a marketplace for illegal goods and services accessed through Tor.

India has the biggest marketplace for dark web, and it makes up 26% of all the countries users using the dark web. According to the Arxiv, if we take the category-wise statistics, we can summaries it as below from the table.

TABLE 1: TABLE DEPICTING PERCENTAGE OF USERS USING THE DARK WEB.

Category Group	Percentage of users using the dark web
18-25	35.9%
26-35	34.8%
36-45	16.8%
46-55	8.8%
56-65	3.1%
Above 65's	0.6%

We can also breakup of type of activities on dark web.

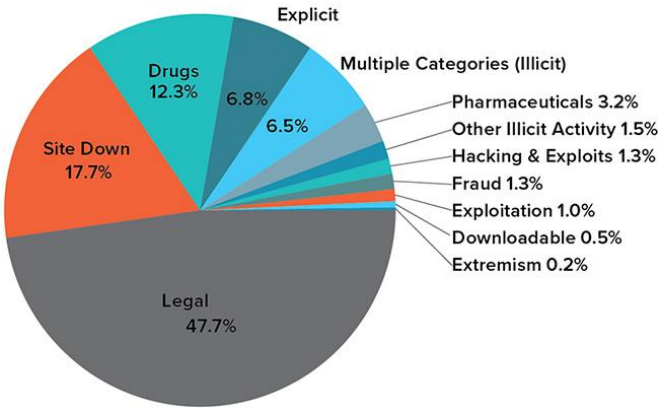

Figure 3: Only 47% of the dark web is used for Legal activities.

III. Benefits and drawbacks of Dark Web Before

Though we have learned that dark web is repository of many illegal things, it is important to understand that most of the dark web users do not access it for illegal purposes. The user may be using it for different purposes like to understand how dark web works (knowledge perspective), to do research and development related to dark web (research perspective), to maintain privacy, or may be that open web is not available in those regions. So, we can see that dark web has both pros and cons. We will now explore both sides of the dark web.

A. *Benefits*

While developing Tor, the developers had a very positive thought and they had developed it for some important benefits. Since Tor and Dark web have become synonymous in their properties, the following benefits of Tor have become the benefits of Dark Web as well.

a. ***Block Trackers:*** Tor has been designed in such a way that the browser isolates each website you visit so third-party trackers and ads can't follow you. The browsers automatically clear cookies and browsing history when you are done browsing.
b. ***Defend against surveillance:*** The browser is designed to prevent someone watching your connection from knowing which websites you visit.
c. ***Resist Fingerprinting:*** To protect the user, the browser aims to make all users look same, making it difficult for you to be fingerprinted based on your browser history and device information.
d. ***Multi-layered encryption:*** The network traffic is secured by three layered encryptions when it passes through the Tor network.
e. ***Browse Freely:*** Tor browser allows you to access all the sites you want to visit, even if they have been blocked by the home network.

B. *Drawbacks*

Though, the purpose of designing dark web was a genuine effort for maintaining privacy, but now it has become a place illegal activity. It has become virtually impossible to separate Dark Web and Tor, and the design of Tor makes it impossible to track people using the dark web for illegal activity. Majority of the traffic to dark web is using Tor for hiding behind and are involved in various crimes like drug trafficking, child pornography, selling arms and ammunitions and various cyber-crimes. The online markets not only sell drugs but can sell anything that a seller wants to put online. Stolen Credit cards and other objects also find place in such markets.

IV. Is it illegal to go on the dark web?

No, it is not illegal to go on dark web in India. our Indian Constitution gives us the Right to access the Internet under Article 21. Due to the benefits of dark web as seen in the above section, dark web has attracted many parties who do not wish to reveal their identity due to security purposes. Legality to use dark web is based on the way you access the web. Those who are using it for security purposes are using it in a legal way, others may indulge in illegal activities in dark web, then it becomes illegal. On the network, though the dark web is a bit grey area, and the real benefits of anonymity may be used by criminals to hide their identities, or to carry illegal activities. In all such cases, accessing the dark web becomes illegal. Anonymity comes with a dark side also as the malicious hackers and other such people would prefer to operate in the shadows and they would use dark web to hide themselves. A very good analogy can be understood by the example as "If you keep a licensed gun with you at your home, that's not illegal. But if you, with the same weapon, shoot someone, that is illegal. You will be charged under either Section 307 or Section 324 of the Indian Penal Code, 1860". So, we can understand that going to dark web is not illegal, with what objective you are going there and what are you doing there makes it legal or illegal.

V. Regulations related to Dark Web

Due to its volatile nature of dark web, it is important to have policies related to dark net in place. Looking at the benefits of the dark web, it will not be correct to legislation that would encroach civil liberties, and thus become very difficult to enforce. But, looking at the drawbacks of it, it is not wise to leave it unaddressed. Formulation of policies related to dark web needs through understanding of open web and dark web, their potential, and their drawbacks. This section explores the policies related to the dark web.

As of now, India lacks stringent laws against dark web, some policies are existing, but it is difficult to enforce them. A comprehensive set of legislative policies needs to be formulated and adopted to keep track of illegal use of the dark web.

Presently, India does not have any law specifically dedicated to maintaining the use of VPNs. Here is what other countries have done.

- While countries such as the U.S. and Germany have supported Tor, going as far as to fund it, other countries are vehemently opposed to it (Tor: Sponsors, n.d.). This poses a major challenge to international policy development.

- China has some of the strictest and best-enforced policies regarding internet regulation. They heavily censor online conversation and quickly silence those who

speak out for collective action or otherwise threaten the regime (King, Pan, and Roberts 2013). China has made efforts to block access to Tor, Russia has made efforts to deanonymize Tor for political purposes, and Austria has made efforts to eliminate Tor traffic within its borders.

- Countries like Iraq, Turkmenistan, and Belarus have entirely banned the use of VPN services.

- UAE, Russia, and China have restricted access to VPN services. In the UAE, only banks and similar organizations have access, but it is highly bound to be used in personal capacity. In China and Russia, the services can be used only for those approved by the government.

Similarly, it is suggested that India should implement such a system where these freely available VPNs are banned. CyberBlogIndia, in its blog, indicates that the government should create an authority under Chapter-VI of the Information Technology Act, 2000 where the government may create a mandatory charge for VPN registration.

In an article by Indian Express, we got to know the opinions of two cyber law experts:

- Karnika Seth, a Supreme Court Advocate and a cyber law expert believes it becomes difficult to prove a particular charge due to the availability of self-destructive mailboxes and proxy servers that help people in creating fake IDs. Since the real identities of people are not disclosed, it becomes difficult to trace them. Hence, there is a need to amend the Information Technology Act, 2000, and the Indian Evidence Act, 1872.
- However, cyber law expert Vicky Shah believes that instead of running behind the need for newer laws, we need to have specialized police trained who know the changing cyber trends.
- This recommendation remains at the core-heart of every problem, i.e., raising awareness of the dark web. We should try to equip more trained officers who can mainly work in unclear web evidence and activity.

VI. Conclusion

Dark Web by its nature is anonymous that makes it difficult discriminate between regular users or criminals. This makes it very difficult for enforcement agencies to track the criminals. If the government orders to shut down all such sites, new ones will appear, and if the government brings charges against the users, it becomes difficult to identify the regular user and the criminals. But, looking at the vulnerability of its use for criminal activities, it is very important to work out for the government policies and put them in place for proper enforcement. We can also conclude that accessing dark web is not illegal, but the task you are performing decides its legality. India needs strong laws and provisions in the Indian Penal Code 1860. Also, from this a comprehensive legislation is demanded to curb the menace of increasing crimes related to dark web.

References

[1] https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643
[2] https://blog.ipleaders.in/laws-relating-dark-web-india/
[3] https://www.kaspersky.com/resource-center/threats/deep-web
[4] “The Dark Web and Regulatory Challenges”, Debopama Bhattacharya”, Manohar Parikar Institute of Defence Studies and Analysis, https://idsa.in/issuebrief/the-dark-web-and-regulatory-challenges-dbhattacharya-230721
[5] Mihnea Mirea, Victoria Wang & Jeyong Jung , “The not so dark side of the darknet: a qualitative study”, https://link.springer.com/article/10.1057/s41284-018-0150-5, page 102–118
[6] https://www.helpnetsecurity.com/2016/11/03/dark-web-legal/
[7] https://www.torproject.org/
[8] S. Nazah, S. Huda, J. Abawajy and M. M. Hassan, "Evolution of dark web threat analysis and detection: A systematic approach", IEEE Access, vol. 8, pp. 171796-171819, 2020.
[9] P. B. Patel, H. P. Thakor and S. Iyer, "A comparative study on cyber crime mitigation models", Proc. 6th Int. Conf. Comput. Sustain. Global Develop. (INDIACom), pp. 466-470, Mar. 2019.
[10] Chiranji Lal, Harshit Kiran, “Laws relating to E Commerce in India: Issues & Challenges”, Amity Journal of Computational Sciences (AJCS), Volume 6 issue 1 July-Dec 2022
[11] Ankita Tandon, Shailesh. N. Hadli, Chiranji Lal, “Ethical and Legal Implications of Artificial Intelligence on Human Rights”, Amity Journal of Computational Sciences (AJCS) Volume 5 issue 2 Jan-June 2022 ISSN: 2456-6616 (Online)