Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By:
Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

Cite this article as:

MR. SANDEEP MISHRA, "*The Dark Web: A Safe Harbour for Cybercriminals",* Vol.3 & Issue 1, Law Audience Journal (e-ISSN: 2581-6705), Pages 375 to 382 (14th May 2022), available at ***https://www.lawaudience.com/the-dark-web-a-safe-harbour-for-cybercriminals/.***

Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

Publisher Details Are Available At:

https://www.lawaudience.com/publisher-details/

Editorial Board Members Details Are Available At:

https://www.lawaudience.com/editorial-board-members/

Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By:
Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

ABSTRACT:

"Security on Internet is one of the biggest challenges which are faced by countries all around the world. The challenges to protection of citizens ***(including corporate entities)*** *and nations alike, from internet attacks are increasing with the technological advancement in the field of online accessibility and communications. The most vulnerable or exposed to these attacks are the developing and the under-developed nations. Compared to developed nations, the developing and under-developed nations lack adequate cyberinfrastructure and technological know-how to protect themselves from online criminal activities like data leaks, cyber terrorism, DDOS attacks, etc. As more and more people are connecting to internet for various purposes such as news, social media, research and education, entertainment, etc., the need for a better protection strategy has to be considered.*

In order to develop a strong security protocol over the internet, the farthest-reaching dimensions of the internet and the World Wide Web must be studied diligently. India as a developing nation needs to keep its cyber dimensions intact with strong security protocols and solid technological reinforcements".

Keywords: Internet Layers, Layers of Web, Computer Crimes, Cyber Crime.

I. AIMS AND OBJECTIVES:

The Dark Web, which is not a recently developed phenomenon, still remains unknown by majority of the global phenomenon. Thus, in order to give an understating of the umbrella under which the research functions, the researcher try to obtain a conceptual understanding of the layers of internet, its origin and development. Further in his study researcher analysed the role of dark web in spread of cyber-crimes such as circulation of child pornography, drug marketing, cyber terrorism, etc. Online resources of the developing countries are more open to exploitation by online attackers. The research concerns itself with the Indian cyber infrastructure and providing suggestions to possible increments to cyberinfrastructure.

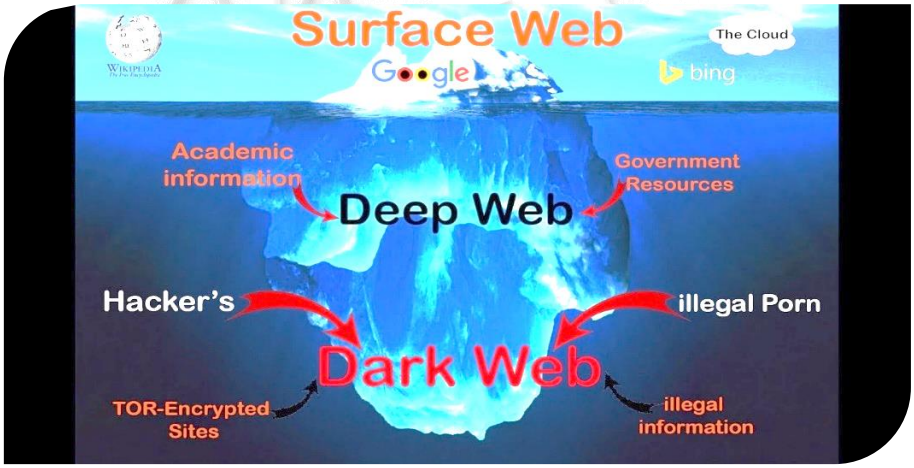
Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

II. THE LAYERS OF THE WEB:

The terms internet and World Wide Web are often used interchangeably. While they are related, they are not synonymous. Internet is a network of networks. It is an infrastructure of networks. The internet facilitates millions of computers and like devices to connect globally and thus creates a '*network*' whereby these connections can communicate with each other. The World Wide Web on the other hand, acts as a means to access information available on the Internet, i.e., the information as shared by the computer networks. ***The World Wide Web consists of three layers:***

1. *The Surface Web*
2. *The Deep Web*
3. *The Dark Web*



Layers of Internet[1]:

II.I THE SURFACE WEB:

The surface web is the most common form of a web where we spend a lot of time for example by reading this you are navigating the surface web. Consider the World Wide Web as an ocean. The Surface Web is the top of the ocean, which can be seen by everyone and is accessible to all. The surface web is available to the general audience and is accessible through commonly used web browsers such Google Chrome, Mozilla, Internet Explorer, etc.[2]

[1] https://www.google.com/search/layers+of+internet.
[2] Available at https://www.lawyersmutualnc.com/blog/understanding-the-3-layers-of-the-internet.

Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

II.II THE DEEP WEB:

According to the Experts 96 % of internet data is comprised of the Deep web. Below the surface and in the depth, lies the Deep Web. This area of the web is hidden to the eyes of general audience as the web pages on this web are not indexed. This means that it cannot be accessed through regular web browsers like Chrome, etc. as it uses modified version of the HTTP language, which is the language used by regular web browsers to access the internet. Access to Deep web requires log in or specific IP address. It includes academic journals, databases, private networks such as Lexis Nexis, Westlaw etc.[3]

II.III THE DARK WEB:

"This is a place on the internet where you really should not want to go." The third and the least accessible layer is the Dark Web; the bottom of the ocean. It requires specific tools and softwares for access, such the TOR browser and I2P. The information on this layer is highly protected through most advanced encryptions and has the element of anonymity, which means the data is uploaded anonymously. Encryptions, which are almost impossible to break, are used to remain anonymous and due to the rapid changing IP addresses, the poster becomes impossible to track down. This is what makes the Dark web to frightful.[4]

III. DIFFERENCE BETWEEN DARK WEB AND DEEP WEB:

The difference between these two layers of internet depends upon their use and accessing procedure. One can access the deep web with proper credentials and authorization without any special tool or software. Data available on deep web is not hidden. It's just difficult to find the data easily by existing search engine. On other hand Deep web is mysterious side of internet. The intention behind deep web is anonymity. The dark web is mostly used for criminal and illegal activity. However, mere accessing of deep web is not a crime itself, but trading of illicit material on internet through deep web is an offence. No one can access deep web without special tools or software like TOR browser. Due to special feature of anonymity

[3] Available at https://ifflab.org/the-layers-of-the-web-surface-web-deep-web-and-dark-web.
[4] Ibid.

Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

the Dark web is mostly used by criminals for selling illegal data, porn trading drugs, weapons, organs and much more.[5]

IV. DARK WEB: DARKER SIDE OF THE INTERNET:

Accessing the Dark web is not in itself an illegal act, however due to the level of threat it possesses and felonious use of the platform, users are advised to stay away from it. The Dark web is accessible through some specific kinds of softwares. The two most popular tools are The Onion Router or TOR and Invisible Internet Project or I2P. These softwares act as browsers to reach the un-indexed webpages of the internet and at the same time, once logged in, they protect the user's IP address by changing it frequently. Rather than making a direct connection, the TOR or I2P routes the data through a virtual tunnels and thus maintains anonymity of user and organisation. The web traffic is routed or piggy-backed through different users and it thus becomes next to impossible track the original user. This attribute of the Dark Web makes it the most popular platform to organise cybercrimes. Payments on Dark web are another attribute that make it a threat. The payment is done through crypto-currencies and the most popularly and widely used crypto-currency for making transactions is the Bitcoin. It is a digital currency which provides for a peer to peer anonymous payment transactions. The block chain technology acts as a public ledger, where these transactions are recorded, however it only records the bitcoin address not the unique address of the parties.

From criminals to state sponsored spies, the dark web used by a number of anti-social entities to commit the most heinous of crimes. Due to its characteristics, coordinating and action becomes easy as the risk of detection is significantly low. Counterfeiting currency, fake passports, drug market, terrorist conspiracies, child porn, selling of private information such as banking details, account login details, etc., are some of the illegal activities that take place on the dark web. Terrorists have been using dark web to further their agendas and motives. After close monitoring of its activities on the surface web, the terrorist organisation turned to the dark web. These organisations use dark webs to receive funds and keep the identities of

[5] Ibid.

Law Audience Journal, Volume 3 & Issue 1, 14th May 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-3-issue-1/, Pages: 375 to 382,

Title: "The Dark Web: A Safe Harbour for Cybercriminals", Authored By: Mr. Sandeep Mishra, Research Scholar, Department of Legal Studies, Dr. Ram Manohar Lohiya National Law University, Lucknow, Email Id: juris.sandeep@gmail.com.

their supporters hidden. Often videos of killings, mutiny, beheading are circulated through the dark web forums to further their agendas. While the data is still not clear as to the magnitude of information available on internet, a report suggests that as of April 2020, there are 5.53 billion webpages indexed by webpages[6]. No matter how staggering this number may sound, it only contributes to 4% of the total data available on the internet the rest 96% is hidden.

V. SOME FAMOUS INCIDENTS OF CYBER OFFENCES USING THE DARK WEB:

A 2020 Niti Ayog report suggests that number of internet users in India is estimated to be 730 million. This number comprises of online shoppers which add up to around 175 million. After nullification of Article 370, the ***Global Research and Analysis Team, APAC*** reported that Indian cyberspace was under attack for around 4,00,000 times, mostly from hackers relocated to China and Pakistan.[7] More than 1,00,000 scanned ***AADHAR, PAN*** and passport copies of Indian Nationals was put up for sale on the dark net. This was reported by an intelligence firm by the name of Cyble. It said, "*We came across a non-reputed actor who is currently selling over 1 lakh Indian National IDs on the dark net. With such a low reputation, ideally, we would have skipped this; however, the samples shared by the actor intrigued our interest -- and also the volume. The actor is alleged to have access to over 1 lakh IDs from different places in India*."[8]

In 2013, the Federal Bureau of Investigation shut own an online marketplace by the name of "Silk Road" which sold contraband drugs, weapons and narcotics. It showed up again in 2013 as "Silk Road 2.0". It reportedly generated revenue of around 9.5 million bitcoins which roughly estimates to $183 Million (in 2014-15). It had around 3800 vendors and 145,000

[6] The Deep Web: Surfacing Hidden Value, vol. 7, issue 1, 2001. *JEP*.
[7] Availableon,https://niti.gov.in/sites/default/files/201907/CyberSecurityConclaveAtVigyanBhavan Delhi_1.pdf.
[8]Available at https://www.business-standard.com/article/current-affairs/.

buyers[9]. On 20th February 2015, Peter Scully an Australian national was arrested on the counts of abduction, rape and murder of under aged children. Using the Dark web, Scully created a ring of international ring of child sexual abuse and a website, where he circulated child pornography on a pay per view basis costing up to $10,000. It was only after the video was surfaced by one of the viewers, an international manhunt for his arrest begin. By that time, Scully had allegedly claimed 75 victims, all of which were under aged children.

In the year of 2017, the Anti-Narcotics Cell of Mumbai arrested five students in connection with 1400 LSD dots worth 70 Lakh. The students used to send money through bitcoin to their friend settled in the United States who would then place the order of these drugs on the dark web and would get them delivered to their delivery address.[10] An incident of offence occurred on November 2020, India's online grocery delivery giant, Big Basket was attacked by hackers. A subsequent perusal of the attacks rendered that data of 20 million users was put up for sale on the dark web for $40,000.[11] An incident was reported in January 2021 that a Bangalore based gateway for making digital payments, Juspay suffered a cyber-attack from a group of hackers. As a result of this attack, 10 Crore data records were allegedly accessed by hackers and were put up for sale on the Dark web in exchange of Bitcoins. While the spokesperson for the company denied the number, leak of data was admitted.[12]

.

VI. REGULATING THE WEB: ISSUES AND CHALLENGES:

Although the move for *Digital India* is a bold initiative and need of the hour keeping in view the changing global order, Indian cyber security regime is infested with some deficiencies which first need to be addressed. While India has one of the most skilled IT professionals, their skills mostly remain un-harnessed, potentially due to improper or no schemes focusing

[9] Jones, Beata. The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, International Journal of Cyber Criminology 10(1):40-61.
[10] Available at https://timesofindia.indiatimes.com/city/mumbai/ story dated 30/ 03/2017.
[11] Available at, https://www.indiatoday.in/technology/features/story/bigbasket-confirms-data-breach story dated 09/11/2020.
[12]Available at, https://www.thequint.com/news/india/100-million-card-details-leaked-to-dark-web-in-juspay-data-breach story dated 06/01/2021.

in this area. The Indian economy is a highly heterogeneous market, which involves players from around the globe, especially in the telecom sector. Telecom companies from China, which is one of the biggest nemeses of India, have a substantial amount of contribution to the Indian telecom sector. Unlike countries like US, where over 44% mobile phone users use Apple powered I-phones with high security standards, only 1% or less use these phones in India. The majority of Indian populations rely on Chinese companies like ***Xiaomi, Oppo, Vivo, OnePlus, etc***. this also suggests that India suffers from lack of indigenous players in this sector. Thus there is need for domestic players to grow in the market of telecom. This can be done by providing incentives and reducing the taxation for Indian owned and funded start-ups in the telecom sector.[13]

India suffers from multiplicity of cyber security organisations, for instance there is CERT for every state and no single umbrella organisation to look over all other organisations. This creates ambiguity in quick response. There is a lack of comprehensive law on internet protocols and internet privacy of citizens. A little is derived from Information and Technology Act, 2000, but it is not enough. Although there are agencies at national level, there is no protocol for coordination. There is no law that protects India's cyber-security interests outside its territorial jurisdiction. For example, a strong need for stricter law and procedure is there in India as it is constantly under attack from hackers. Another significant point is that India is not a signatory of the Budapest Convention on Cybercrime which "*seeks to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.*"[14] Lack of cyber security awareness is also one of the challenges faced in building a strong cyberspace. This can be uprooted by initiatives making *netizens* aware of various threats which are active online and security protocols needed to be observed by them while accessing the web. Individual should know importance of digital data protection and use internet in a secure manner. Most of the critical infrastructure with respect to cyber-security is either owned by

[13]Available at https://www.dsci.in/content/cyber-security-challenges.
[14] Available at https://www.coe.int/en/web/cybercrime/the-budapest-convention.

the military or owned by private sector. There is a lack of ICT infrastructure in other areas. For instance, the Indian Judicial system is still to come at par with other sectors in technological means. Many nations have advocated the approach where private industries are invited to contribute to protecting cyberspace as part of a National strategy. India can also adopt this market based approach by proposing relevant protocols and tax incentives.

VII. CONCLUSION:

Perhaps not necessarily designed for evil, the Dark Web is has now become the most perpetrator-friendly platform in the recent times where private data of individuals and confidential government secrets are openly leaked and circulated. Due to its attributes, tracking and identifying illegal transactions becomes a humongous task for the law enforcement authorities. India, as a participant of the cyberspace, has not remained untouched from these attacks. Already multiple companies have suffered data leaks and there are regular attacks on government databases. Discussions, deliberations and promulgation of subsequent measures is highly recommended at this very point of time as citizens and corporate entities alike, fear their online security in the light of increasing tech organized crime administered through the Deep Web & Dark Web. Strong cyber security infrastructure needs to be established and administered by the regime. The crucial deficiencies found in the Indian cyber-security regimes make it vulnerable to cyber-attacks and threaten the privacy of citizens and India's sovereignty. India has one of the most skilled IT experts in the world. In order to develop a strong cyberspace that withstands the anti-India cyber-attacks, Government must harness their efficiency and professionalism.