VOLUME 4 ISSN 2456-9704

ANONYMITY IN BROWSING AND ITS ADVERSE EFFECTS IN CYBERSPACE

By *B.K. Dhyana*
From *Damodaram Sanjivayya National Law University, Visakhapatnam*

ABSTRACT

With the evolution of computer technology there has been a concomitant increase in cybercrimes. Most cybercrimes that surface in the web are detectible by the law enforcement agency by tracing the internet protocol address of the perpetrator but the problem arises when these cybercrimes are committed in the dark web where the user's right to anonymity and privacy while browsing the dark web protects the perpetrators. Virtual anonymity or browsing the internet incognito makes cyber criminals more fearless in their operation and further using crypto currency as payment for any transaction in the dark web has increasingly made it difficult for the law enforcement agency to shut down their operations. This research explores the complexity of the problem of anonymity in dark web which poses a grave threat to the cyberspace in India.

Keywords: World Wide Web, Deep web, Dark web, Crypto currency.

LIST OF ABBREVIATIONS

1. CERT IND Indian Computer Emergency Response Team
2. CSAM Child Sexual Abuse Material
3. FBI Federal Bureau of Investigation
4. HTML Hypertext Mark-up Language
5. IRS Internal Revenue Service
6. IP Internet Protocol
7. ISIS Islamic State of Iraq and Syria
8. ISP Internet Service Provider
9. UN United Nation
10. URL Uniform Resource Locator
11. v. Versus

OBJECTIVES OF THE STUDY

- Understanding the dangers that lurk in the deep web and the software used to browse the deep web anonymously.
- Understanding the threat posed by combination of crypto currency and dark web.
- Exploring the measures adopted by Indian government relating to internet censorship.
- Examining the cyber law in India.

SCOPE OF RESEARCH

This research is limited only to anonymity in browsing the dark web and does not deal with user's privacy in the internet which is a subject still under debate. This research extends only to the criminal contents hosted in the deep web and does not deal with whistle-blowers who use the deep web. It doesn't go into broader study of crypto currency used in transactions done in dark web but just gives an understanding of how the combination of anonymity and crypto currency in dark web poses a serious threat to the law and order in a society.

LITERATURE REVIEW

The following literatures are reviewed for the purpose of this research:

Carmine Dipiero (2017) in his study on abuse of crypto currency in the dark web has suggested reformulating the approach of the investigative agency to locate the

perpetrators. His study suggests that the FBI should focus more on having undercover agents to uncover the cybercriminals in the dark web than focussing just on locating servers of the users or cracking Tor. The study is limited to the problems faced by investigative agency in U.S.A. in locating the perpetrators of the crime. On the subject of privacy in dark web, he affirms that there must be a fine line between fighting against dark web markets and infringing on privacy and libertarian values.

Sophia Dastagir Vogt in The digital underworld , combating crime on the dark web(2017) has dealt extensively on privacy law in U.S.A and on combating international crime in the dark web. Her research gives an understanding on how the courts developed the third party doctrine while combating activities in dark web. The doctrine is explained as 'a person has no legitimate expectation of privacy in information when he voluntarily turns over to third parties'. Apart from expectation of privacy, the author deals with conflicts of law and has suggested closer cooperation with foreign law enforcement agencies for overcoming jurisdictional obstacles in combating cybercrimes in the dark web.

Dominick Romeo in Hidden threat: The dark web surrounding Cyber security(2016) has dealt on the subject of dark web and how it poses a serious threat to national and domestic cyber security. His research has given rise to many critical questions about the state of cyber security and has suggested collaboration between federal government and private enterprise to combat this threat.

STATEMENT OF PROBLEM

Cyber criminals operate clandestinely deep within the World Wide Web protected by anonymity. Various nefarious activities *inter alia* transmitting Child pornography, Sale of contraband substances, drugs etc. are carried out and these transactions are paid by crypto currency. The literature on the dark web is very limited. Therefore, the need arises to explore into the problem of abuse of anonymity and crypto currency as it poses a grave threat to the international community. The importance of this research is to primarily explore the dark web and explain the ambit of cyber laws in India in combating the problem of abuse of anonymity and crypto currency.

RESEARCH METHODOLOGY

This is a doctrinal research designed to be exploratory in nature for the purpose of providing an insight on the operation of criminal activities in the dark web and for understanding how online anonymity combined with crypto currency have added to the problem of increasing cybercrimes. It further goes on to examine the cyber law in India in coping with such problem. This research seeks to provide complete understanding of misuse of anonymity in dark web so that it could help future researchers to further probe into this area of study. Primary sources such as legislations, rules, decisions of courts and Secondary sources such as Articles, Journals and books, online resources were referred for the purpose of this research.

CHAPTER 1INTRODUCTION TO THE SURFACE WEB, DEEP WEB AND THE DARK WEB

VOLUME 4 ISSN 2456-9704

Before the advent of technology, communication between people around the world was very slow and difficult. Innovation began growing at a fast pace only since the 19th century, as a result of which personal computers, smartphones, tablet computers etc were invented for storing and sharing information. The most important development of all was the internet which became the quickest means of connecting people. Sir Tim Berners Lee, a British scientist at CERN, invented the World Wide Web in 1989 by conceptualising the idea of sharing information from one computer to another. The World Wide Web is just one part of the services provided in the internet which consists of numerous websites or webpages containing information. These websites or webpage in the World Wide Web can be accessed through web browsers such as Chrome, Morzilla, Microsoft Edge, Safarietc just by using internet. Internet became the fastest means of communication and it has ever since kept people connected across the globe just by a click of the mouse. A webpage is a HTML document containing information available in the World Wide Web. The websites found in the World Wide Web contain a collection of webpages accessible through the internet by typing its unique address in the web browser and this will open up the website's main web page otherwise known as homepage. Once the World Wide Web was made available to the public at large, many businesses started creating web sites sharing information about their business and products. Soon internet was made available commercially on payment of certain fee by internet service providers to access the World Wide Web. There are other services apart from World Wide Web provided by the internet such as electronic mail, messaging services, information services, file transfer etc. At present,46.7% of internet users are there in Asia of whom23.8% of the internet users are from India.[1]

The contents in the World Wide Web are extensive; many web pages are being created on daily basis. To access the web pages in the internet, search engines such as Google, Bing, yahoo etc. were designed to search the contents in the World Wide Web. Since there were many web pages in the World Wide Web, the need arose to index the web pages so that they are discoverable in the search engine. The indexed web contains at least 4.59 billion web pages.[2] These indexed web pages is the surface web and can be easily accessed through web browser. Those web pages that were not indexed by the search engines became a part of the deep web and they cannot be found and accessed through standard search engines. This is the stark contrast between the surface web and the deep web. Within the deep web, there are some websites that host criminal activities and these sites came to be known as the dark web. The dark web forms a small portion of the deep web and it is a platform for illegal activities, terrorism etc. The deep web and dark web cannot be accessed through standard web browsers but require some

[1] Internet world stats, (2017) *World internet usage and population statistics* (table) *available at*http://www.internetworldstats.com/stats.htm (last visited on Oct.12,2017).

[2]Maurice de Kunder, (2017) *The size of the World Wide Web*(graph) *available at* http://www.worldwidewebsize.com/ (last visited on Oct.12, 2017)

specific software to access it. To summarise, the World Wide Web contains the surface web that are visible in search engine, the deep web and dark web that are hidden from search engines.

CHAPTER 2THE DARK CORRIDOR TO THE WORLD WIDE WEB

ACCESSING THE DEEP AND DARK WEB

The deep web contains all such websites, online communities that are hidden from surface search engines because they are not indexed. It is also home to many academic library databases. The deep web is otherwise known as the hidden web or invisible web. The political dissidents across the world, who cannot express their views freely in the surface web, use the deep web as a means for communicating their views without fear of being persecuted. The reason behind it is that, the deep web can be accessed only through specific software that allows anonymous browsing. It is difficult to trace the person who is browsing the deep web as his internet traffic is diverted through many relays due to which the location of the user cannot be traced. One such software that allows anonymous browsing of deep web is the Tor browser. Before looking into the working of Tor project, it is first necessary to understand the difference between anonymity and privacy for the purpose of this research.

ANONYMITY AND PRIVACY have been used synonymously but they have distinct meanings. In terms of anonymous user of the internet, it means the user remains unknown and unidentified by others. Through anonymity, a person's name, identity details, gender, IP address is unknown to others in the web. By remaining anonymous, the user's location cannot be tracked nor can the user's activities be monitored. The user can go by various pseudonyms covering his true identity. Whereas privacy of a user of the internet means that the right of the user to choose what personal information needs to be protected and to whom it is to be revealed. A user's information is protected in a public domain thus protecting his private space in the internet. Anonymity is narrowed to the concept of identity whereas privacy deals with protecting personal information and personal space from others.[3] This research only focuses on anonymity while browsing the web and not the right to privacy.

TOR PROJECT was first developed by U.S.Naval Research Laboratory for sharing military documents in the internet anonymously and in 2012 it was launched to the public at large.[4] It is a free and open software that can be downloaded by anyone from https://www.torproject.org/.It's a software that protects the user's anonymity. Tor requires a lot of assistance from its users across the globe to volunteer for the purpose of running relays, that is, to divert internet traffic of the person browsing the website so that his IP address remains hidden. In other

[3] Mari KarkeaAho, *Anonymity and privacy in the electronic world*, (Nov. 28, 2009), http://www.tml.tkk.fi/Opinnot/Tik-110.501/1999/papers/anonymity/anonpriv.html (last visited on Oct. 12, 2017)

[4]Tor Project, https://www.torproject.org/ (last visited on Oct. 14, 2017)

words, the internet traffic is run through Tor relays which mean that once the internet traffic of the user is received by a volunteer, it is passed along to another across the globe.[5]Tor aims to protect the users' privacy and gives them a sense of freedom by allowing them to access the internet anonymously. It is difficult to trace the Internet Protocol address[6] of the user and therefore the location of the user remains hidden. The Tor browser encrypts all data sent and received by the user. Tor browser blocks plugins such as flash, real playersetc since these plugins or add-ons reveal the user's IP address. It also takes measures in preventing users from opening the downloaded content in the browser since this might reveal their IP address. Such is the anonymity and protection given to the user of the Tor browser.

Tor by default uses the search engine known as DuckDuckGo which enables a person to access information in the deep web as well as other websites in the surface web anonymously. This search engine does not track the user's location. The domains in Tor browser use '.onion' suffix addresses unlike other domains like '.com' , '.net' etc. Tor works on onion routing which protects a person from traffic analysis attacks, letting users to communicate with each other anonymously. So while analysing the internet traffic, it will be hard to figure out who is communicating with whom. Just as how onions have multiple layers, Tor wraps several layers of encryption over the communication so that the identity of the user remains untraceable.

USERS OF TOR: There are 100,000 users world-wide who use Tor every day and 5% of users are from India.[7]Activists, whistle-blowers, the political dissidents and those who are persecuted from their country are more likely to voice their views freely by using Tor since they feel safe that their identity is protected by the software. It helps people to communicate sensitive information anonymously. Tor thus became a haven for political dissidents, persons who are persecuted from their country, Journalists working in danger zone, to those who want their activities to be private from advertisers and to those evading censorship. People can access myriad database of knowledge that has been hidden away by national firewall and censorship laws in their country by using Tor. Some countries which have strong censorship policy have blocked Tor project making it difficult to download it directly from their website, but Tor has hosted mirror websites in such countries so that the users will be able to access it.

Tor software is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destination or content.[8] It not only protects the user's anonymity while viewing the contents in the internet but also helps them to host websites

[5] The Electronic Frontier Foundation, https://www.eff.org/torchallenge/what-is-tor.html (last visited on Oct.14,2017)

[6]Prof. Alan Woodward, *Viewpoint:How hackers are caught out by law enforcers*, BBC NEWS (Mar.12,2012) http://www.bbc.com/news/technology-17302656 (last visited on Oct.14, 2017)

[7]Oxford Internet Institute, (2014) *The anonymous internet* (cartogram) *available at* http://geography.oii.ox.ac.uk/?page=tor(last visited on Oct. 14,2017)

[8]Tor Project, *Supra* Note 4.

and services anonymously. Instead of taking a direct route from source to destination, it takes its users through many relays run by volunteers making it difficult for anyone to snoop into the websites that have been visited by the user. It also prevents the websites from learning the physical location of the user. The location of the server which hosts the website is also hidden from others. The benefits of Tor are encryption, right to anonymity and privacy protection. However, over the years, it has been misused by criminals and terrorists. What began as a medium of free speech and expression soon became a hideout for those involved in criminal activities.

COMBINATION OF ANONYMITY AND CRYPTO CURRENCY: The criminals have created a network within the deep web that came to be known as the dark web where drugs, stolen credit cards, fake passports etc are being sold, pornography contents such as child pornography are readily available, assassins and hit men can be hired and such other nefarious activities are being operated. Dark web is similar to a black market that is hidden deep in the web, where anything illegal is available. The payments for transactions in these sites are entirely done through crypto currencies. The most recent crypto currency that has gained popularity among the internet users is Bitcoin[9].This currency is protected by high levels of encryption making it hard to trace the names of the buyers and sellers in a virtual transaction. Whatever a person buys or sells using Bitcoin is entirely private and cannot be traced back to them. The payments made through Bitcoins are entirely anonymous. Thus, more and more cyber criminals in the dark web use bit coins for any transactions that takes place, thus protecting themselves and the buyer. Anonymous browsing through Tor along with crypto currency has made the cyber criminals bolder in their operation as their identity cannot be traced and the payments also cannot be traced back to them. When these two forces combine, the cybercriminals become invincible. Some of these nefarious websites in the dark web are hereinafter analysed to give some insight to this problem.

PROMINENT WEBSITES IN THE DARK WEB

SILK ROAD is one such website that introduced the terminology ‘dark web’ into a layman’s vocabulary. The investigation into the operation of this website opened the pandora’s box of various complex issues. The first and foremost difficulty into the investigation was tracing an invisible trail left by an anonymous person who launched the website in the dark web. At first glance, Silk Road might seem like any other e commerce site but the oddity is that anyone could purchase or sell contraband drugs, narcotics etc in this website that is operated in the dark web and pay for these transactions entirely through Bitcoins. Since it’s operated in the dark web and the payments were done entirely through crypto currency, it was very difficult for the investigative agency to trace the administrator of the site who went by the pseudonym Dread Pirate Robert. Silk Road

[9] Tal Yellin et al., *What Is Bitcoin?*,CNN MONEY, http://money.cnn.com/infographic/technology/what-is-bitcoin/ (last visited on Oct 14, 2017).

by 2013, was making sales of $1.3 million every week.[10]It came to be known as one of the most notorious online marketplace for illicit drugs. The U.S. government had been trying to shut the website down for over two years but was unable to find the server from which it was operating. The Federal Bureau of Investigation with the help of an IRS agent finally arrested Dread Pirate Robert whose real name was Ross Ulbritch. Soon after his arrest in 2013, the FBI shut down the website. The arrest of Ross Ulbritch was possible only due to his own human error *inter alia* using his email id with his original name while advertising Silk Road in an online forum. His own mistakes helped the FBI to trace him; otherwise it would have been very difficult to link Silk Road to RossUlbritch. The FBI orchestrated Ulbritch's whole arrest, by waiting until he logged on to his computer, ensuring that all the data remained intact, before arresting him in a public library at San Francisco. Robert Ulbritch was in his 20's when he was arrested and was operating within USA. The true potential of dark web came to light only because of Silk Road prosecution. Ulbricht was formally charged with the following offenses" Distributing narcotics by means of the Internet, conspiring to commit narcotics trafficking, engaging in a continuing criminal enterprise, computer hacking conspiracy and conspiring to commit money laundering." [11]Justice Katherine B Forrest of the U.S. District Court, New York termed the crime as "planned, comprehensive and deliberate scheme which posed serious danger to public health and community"and sentenced Robert Ulbritch to life imprisonment without possibility of parole.[12] The judgment of the District court was affirmed by the court of appeal.[13] The most deterring punishment was given in his case but this did not stop other cybercriminals in the dark web from hosting Silk Road 2.0within weeks the original site was shut down.

FREEDOM HOSTING A large child pornography website that operated in the dark web was shut down by the FBI. The FBI sought extradition of an Irish man who was the administrator of the website. A study found that over 80%of Dark Web visits are related to paedophilia.[14]It's seen that the conviction of cyber criminals becomes a problem when the person who commits the crime is working outside the country.

HIDDEN WIKI is a dark web directory that provides link to other hidden services in the

[10]*Silk Road: Google Search unmasked Dread Pirate Roberts*, BBC NEWS, (Aug. 19,2017) *available at*http://www.bbc.com/news/av/magazine-40977474/silk-road-google-search-unmasked-dread-pirate-roberts (last visited on Oct. 15, 2017)

[11]Press Release of Federal Bureau of Investigation, *Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison* (May 29, 2015),*available at* https://www.fbi.gov/newyork/press-releases/2015/rossulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison (last visited on Oct.15, 2017)

[12] United States v. Ulbricht,1:14-cr-00068,No.183 (S.D.N.Y. Feb.5,2015)

[13]*United States v. Ulbricht*, No. 15-1815 (2d Cir. May 31, 2017)

[14] Andy Greenberg, *Over 80Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED (Dec. 30, 2014)*available at* http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited on Oct.15,2017)

dark web including uncensored links relating to money laundering, contract killing, child pornography etc.

C'THULHU provides services relating to assassination and hiring hit men and also takes crypto currency for its services.[15]

DEADPOOL is a service that allows users to pool in bitcoins and predict assassination of people and the user who guesses it correctly can claim the entire pool.
The above mentioned list are not exhaustive, there are many number of websites hosting similar services in the dark web.

These criminal activities in the dark web are mostly unnoticed by law enforcement agencies due to the anonymity that Tor offers to its users. It is dangerous for any faint hearted person to venture into the dark web because of the graphic contents of violence posted in it. Dark web is the greatest threat to national security as there is a great danger that terrorist organisation may use it as a means of communication. The digital footprints of the cyber criminals are hidden completely from the eyes of the law enforcement agency. More and more criminals are exploiting anonymity in the internet and this has become the biggest problem which the world faces today. The cyber criminals across the globe are using the onion routing (TOR) software for carrying out their nefarious activities and making profit in a short time. This poses a real danger to the law and order situation in a nation and also a major threat to the security of international community at large since these crimes have no borders and it is difficult for any agency to trace the location, let alone catch the perpetrator. The drug cartel activities in the dark web are the most prolific and profitable of all in the dark web, it has high clientele across the globe. The UN drug report shows that there is a 50% increase of drug transaction in the dark net from 2013 to 2015.[16]The cyber criminals in the dark web stand tall knowing well that operating anonymously will protect them from being arrested.

Chapter 3EFFORTS OF THE INDIAN GOVERNMENT AND JUDICIARY TO BLOCK WEBSITES HOSTING PROHIBITED CONTENT

India has moved towards digitisation and has initiated Digital India Campaign to transform the country into a digitally empowered society. In order to protect India's cyberspace, the government of India has created a separate ministry under it known as the Ministry of Electronics and Information Technology which oversees many divisions *inter alia* Cyber laws and E security division for protecting India's cyber space. However, when it comes tointernet freedom, India has ranked 41 among the world,the reason being Indian government's active involvement in blocking

[15] Aaron Sankin, *Searching for a hitman in the Deep web,*TheDaily Dot,(Oct. 10,2013)https://www.dailydot.com/crime/deep-web-murder-assassination-contract-killer/ (last visited on Oct.15, 2017)

[16] United Nations Office on Drugs and Crime, (2017)*World Drug Report* (Graph)*available at*https://www.unodc.org/wdr2017/index.html (last visited on Oct. 17, 2017).

websites.[17]For the purpose of this research, it is important to look specifically at the cyber laws in India in relation to blocking of websites that hosts prohibited/illegal contents. This will give an insight on the preparedness of the government to tackle the criminal activities in dark web.

I. **LAWS AND RULES RELATING TO BLOCKING WEBSITES**: The Information Technology (amendment) Act, 2008 permits the Central government to block websites *inter alia* to protect the safety and security of the nation and for maintaining public order.[18]In exercise of its powers under section 87(2) (z), the Ministry of Electronics and Information Technology has prescribed rules relating to the procedure for sending complaints regarding websites that hosts prohibited content and also laid down rules relating to blocking these websites in Information Technology (Procedure and safeguard for blocking for access of information by public) Rules, 2009. As per the said rules, complaints relating to prohibited contents in websites shall be sent by public to the nodal officer of the concerned organisation who examines the complaint and forwards it to the designated officer. On receipt of the complaint, the designated officer will issue notice to the intermediary or the person who hosted the information to clarify the matter within 48 hours and if it sees fit shall direct the agency of government or intermediary to block such website. The Act further prescribes punishment for intermediaries such as Internet Service Providers, web hosting service providers etc who fail to comply with the directions relating to blocking of websites for a term that may extend to seven years and shall also be liable with fine. [19] The Information Technology (Intermediaries Guidelines) Rules, 2011 framed by the government in exercise of its powers under section 87(2)(zg)imposes obligation on the intermediaries such as Internet Service provider, web hosting service providers etc to take down websites that deal with criminal activities within 36 hours upon obtaining knowledge or upon acting on some complaint. [20] It also lays down certain due diligence standards which the intermediary must follow.[21]

The constitutional validity of section 69A of Information Technology (amendment) Act, 2008 and the rules relating to the Information Technology (Procedure and safeguard for blocking for access of information to public), 2009 were upheld by the Supreme court. [22] It also upheld the validity of the Information Technology (Intermediaries Guidelines) Rules, 2011.[23]

With regard to interception, monitoring and decryption of online information by the Union and States, the rules relating to its procedure have been laid down in the

[17] FREEDOM HOUSE, (2016) *Freedom on the Net*(chart)https://freedomhouse.org/report-types/freedom-net (last visited on Oct.17,2017)

[18] Sec.69A, Information Technology (Amendment) Act, 2008.

[19] *Supra* Note 18.

[20] Rule 3(4), Information Technology (Intermediaries Guidelines) Rules, 2011.

[21] Rule 3, Information Technology (Intermediaries Guidelines) Rules, 2011.

[22] ShreyaSinghal vs. Union of India AIR 2015 SC 1523

[23] *Ibid.*

Information Technology (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009. It also prescribes the procedure to be adopted at the time of emergency when obtaining prior directions are not feasible.[24]

II. **BLOCKING WEBSITES RELATING TO CHILD PORNOGRAPHY**: The Information Technology (Amendment) Act, 2008prescribes punishment for publishing or transmitting obscene or sexually explicit materials and also materials relating to children in sexually explicit form.[25] Further, in exercise of powers under section 87(2)(zg) read with section 79 of the Information Technology Act, the Ministry of Electronics and Information Technology has issued Information Technology (guidelines for cyber café)Rules 2011, permitting cyber cafés to use filtering software to prevent access to child pornography and obscene materials.[26] For the purpose of curbing Child Sexual Abuse Material online, the cyber laws and e-security division under the ministry in exercise of its powers under section 87(2)(zg) has issued an order dated 18.04.2017 recommending solutions to curb the problem. It was observed that there was no central agency to monitor CSAM and that most of these websites were hosted outside India. Based on these observations, The Cyber laws and E security Division in its order directed the Internet Service Providers to remove online CSAM by following the list of those URLS maintained by the Internet Watch Foundation.[27]

In *Kamlesh Vaswani* v. *Union of India* [28]The petitioner approached the court, for directing the government to block all websites relating to pornographic content *inter alia* child pornography. The Supreme Court has made several observations relating to child pornography and the need to curb it. On July 31, 2015, DoT ordered ISPs to block access to 857 URLs for hosting pornographic content.[29] The notification stated that the websites were found to be violating morality and decency under Article 19(2) of the Constitution of India, read with Section 79(3)(b) of the Information Technology Act.[30] The centre later clarified that only child pornography may be blocked.[31] Though the Supreme Court made reservations on blocking pornography as anyone would challenge that under Article 21, it felt otherwise about child pornography.

[24] Rule 3, Information Technology (Intermediaries Guidelines) Rules, 2011.

[25] Sections 67, 67 A , 67 B Information Technology (Amendment) Act,2008.

[26]Rule 6(5), Information Technology (guidelines for cyber café)Rules, 2011.

[27] Ministry of Information, Cyber law and E-Security Division, *Order: Measures to curb online sexual abuse material*, (Apr. 18,2017) *available at* http://www.meity.gov.in/writereaddata/files/Order%20regarding%20online%20CSAM.pdf (last visited on Oct 17,2017)

[28] Kamlesh Vaswani v. Union of India& others W.P.C. No. 177 of 2013

[29]BBC, *India Blocks 857 porn sites*, BBC NEWS (Aug.3, 2015) http://www.bbc.com/news/world-asia-india-33754961(last visited on Oct.17,2017)

[30]*Ibid.*

[31]Letter from Government of India, Ministry of Communication & IT to All internet service licensees (Aug.4,2015) *available at*http://www.thehindubusinessline.com/multimedia/archive/02498/Centre_revokes_ban_2498028a.pdf (last visited on Oct. 17,2017)

III. **THE COMPUTER EMERGENCY TEAM** (CERT IND) had been created under the Ministry of Electronics and Information Technology to respond to any security threat to India's cyber space. CERT-IND has been authorised by the ministry to issue instructions to the Department of Telecommunications (LR Cell) to block the websites hosting prohibited content after checking the veracity of the complaint.[32] It is the duty of the Internet Service Providers to block such websites and inform CERT IND.[33]The following persons can approach CERT IND for the purpose of blocking websites:

1. Secretary, National Security Council Secretariat.
2. Secretary, Ministry of Home Affairs, Government of India.
3. Foreign Secretary in the Department of External Affairs or a representative not below the rank of Joint Secretary.
4. Secretaries, Departments of Home Affairs of each of the States and of the Union Territories.
5. Central Bureau of Investigation, Intelligence Bureau, Director General of Police of all the States and such other enforcement agencies.
6. Secretaries of Heads of all the Information Technology Departments of all the States and Union Territories not below the rank of Joint Secretary of Central Government.
7. Chairman of the National Human Rights Commission or Minorities Commission or Scheduled Castes or Scheduled Tribes Commission or National Women Commission.
8. The directives of the Courts.
9. Any others as may be specified by the Government. [34]

As seen above, government surveillance plays a vital role in discovering such criminal activities in the web. The above mentioned government authorities can approach CERT IND to block these websites.

IV. **CENTRAL MONITORING SYSTEM** has been set up in Delhi and Mumbai by the Ministry of Electronics and Information Technology for surveillance of online traffic. This will help detect the activities of cybercriminals. Although there might be concerns of violation of privacy, this approach by the government is a step towards bringing an effective system in place to monitor websites in the dark web. Though the government has taken several measures to block child pornography, many new sites are popping up in the dark web on a daily basis and the only way that the Central Monitoring System can block such contents is by taking proactive action.

Measures are yet to be taken to block websites relating to online sale of drugs which has become a menacing problem in India. Many incidents have been reported about teenagers being arrested for possessing contraband substances which they purchased from the dark

[32] Sec.70B, Information Technology(amendment) Act,2008.

[33] Ministry of Electronics and Information Technology, http://meity.gov.in/content/it-act-notification-no-181 (last updated on June 26, 2015)

[34] *Supra* Note 33

web.[35]Terrorist's organisations such as ISIS use dark web for the purpose of spreading jihad and to fundraise for their activities.[36]Using crypto currency to hire hit men and assassins, exotic animal trade, and trade of illegal substances, Fake identity cards, passports etc are all websites that have not been brought to the notice of the nodal agency that oversees threats to cyberspace in India. Bit coins though not recognised by the Reserve Bank of India, are still being used for transactions online. Money laundering and gambling websites using crypto currency is being operated in the dark web and less attention is paid to monitoring it. Most of the websites that operate in the dark web are hosted outside India and the perpetrators remain unscathed. The Information Technology Act, 2000 applies to all such offences that have been committed by any person outside India irrespective of his nationality if that person uses Indian network.[37] The need of the hour is coordination among the investigative agency and the CERT IND to address the concerns of criminal activities in dark web. The provisions of this Act may help in monitoring and taking down the indexed content in the World Wide Web or those that are visible in the search engine, but whether it would effectively help in blocking websites in dark web is a question left for further analysis.

CONCLUSION

Eric Jardine, a research fellow for the Centre for International Governance Innovation, stated that "*The anonymity of the technology of the Dark Net cuts both ways — while people can use the network for villainous purposes, people can also use it for good. Despite public opinion, shutting anonymity networks is not a viable long-term solution, as it will probably prove ineffective and will be costly to those people that genuinely benefit from these systems*." [38] But the argument posed here is should such level of anonymity be allowed so as to threaten the national security. This research has provided some insight on the *modus operandi* of cybercriminals in the dark web where they misuse onion routing and crypto currency and exploit anonymity. The challenge is to shut down these dark websites which would

[35] Imran Gowhar, *Three held on charge of peddling drugs bought through Darknet*, THE HINDU (Mar. 29. 2016) *available at* http://www.thehindu.com/news/cities/bangalore/three-held-on-charge-of-peddling-drugs-bought-through-darknet/article7505322.ece(last visited on Oct.18,2017)

Prakruthi PK, *While porn is keeping us busy, Kids are buying hash online*, BANGALORE MIRROR (Aug.6,2015) *available at* http://bangaloremirror.indiatimes.com/bangalore/cover-story/porn-net-online-drugs-hash-agora-website-drug-market/articleshow/48366559.cms (last visited on Oct.18,2017)

KK Abdul Rahoof, *Hyderabad criminals in deep web*, DECCAN CHRONICLE (Jan10,2016) *available at* http://www.deccanchronicle.com/150615/nation-crime/article/hyderabad-criminals-deep-web (last visited on Oct.18,2017)

[36] Gabriel Weimann, *Terrorist migration to the dark web, available at* http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html (last visited on Oct.18, 2017)

[37]Sec.75, Information Technology Act ,2000.

[38] Sean Zohar, *The "Dark Net should be shut down : CIGI-Ipsos global survey: But what about its benefits?* (Mar.24,2016) https://www.cigionline.org/articles/dark-net-should-be-shut-down-cigi-ipsos-global-survey-what-about-its-benefits (last visited on Oct.18,2017)

require discovering numerous secret servers located worldwide which is a mammoth task for any country. These are crimes committed across borders, that is, the website maybe hosted by a person in one country, the buyer and sellers might be from different countries. The international community should work together for shutting down these nefarious activities. This research has thus far, explored the complex issue of anonymity in operating the dark web that has led to prominent criminal network in the dark web, making it a major challenge for the international community at large. Though laws may be sufficient to punish the perpetrators, the most obvious concern is to locate these perpetrators who shield themselves in the cloak of dark web.

BIBLIOGRAPHY

BOOKS AND ARTICLES:

1) Aparna Viswanathan, *Cyber law Indian and International perspectives*, Lexis Nexis (2017)
2) A. Dominick Romeo, *Hidden Threat: The Dark Web Surrounding Cyber Security*, 43 N. Ky. L. Rev. 73, 86 (2016)
3) Carmine DiPiero, *Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web*, 2017 U. Ill. L. Rev. 1267, 1298 (2017)
4) NS Nappinani, *Technology laws Decoded*, Lexis Nexis (2017)
5) Sophia Dastagir Vogt, *The Digital Underworld: Combating Crime on the Dark Web in the Modern Era*, 15 Santa Clara J. Int'l L. 104, 125 (2017)

STATUTES:

1) Information Technology (amendment) Act, 2008.
2) Information Technology (Intermediaries Guidelines) Rules, 2011.
3) Information Technology (guidelines for cyber café) Rules, 2011.

WEBSITES:

- https://www.torproject.org/
- http://www.bbc.com/news
- https://www.cigionline.org/
- http://www.thehindu.com/news/
- http://bangaloremirror.indiatimes.com/
- http://www.deccanchronicle.com/
- http://meity.gov.in/home
- https://freedomhouse.org/
- https://www.wired.com/
- http://money.cnn.com/
- https://freeross.org/?v=47e5dceea252
- https://www.fbi.gov/

*****