"THE CHALLENGES AND ISSUES SURROUNDING THE DARK WEB, A CLANDESTINE COSMOS"

Kritika Singh*

ABSTRACT

Accessible only through special software by incognito users, the 'Dark Web' has turned out to be a major havoc for the global law enforcement agencies today. The 'Dark Web', essentially a collection of websites is one of the three layers forming the internet, the other two being, 'Surface Web' and 'Deep Web'.

The illegal activities taking place there include sale and trade of illegal goods and services, drug trafficking, online piracy, pornography, paedophilia and child pornography hitting 80 percent , terrorism, hacking ,online abuse, online fraud, etc.

With respect to the question of legality of accessibility of the Dark Net, using similar browsers browsing Dark Net is not illegal in India or any other country because the basic purpose of TOR is to provide anonymity but browsing or uploading illegal content through such browsers is completely illegal.

Key Words: Anonymity, Accessibility, Browser, Cyber Crimes, Dark Web, Illegal.

Crime is getting easier. Decade by decade crime has changed its form and means by which the perpetrators could commit it. It can be described both as a social as well as an economic phenomenon and roots back to the origin of human society. Considering the transformation in the form of crime, the physical involvement of humans has almost reduced to nil where the harm can be caused to a person or property with the use of technology without the offender being identified.

Technology has given an edge to people to hold out the foremost prosaic of tasks, like

* B.A.Ll.b.(Hon's), LL.M., Ph.D. Scholar at Faculty of Law, University of Allahabad.

placing order for groceries from the shop, to the most complicated activities, like performing a complex surgical operation, using a computer from a distant location.

Since criminals have adapted themselves with these technological advancements the general public is exposed to internet crimes on a regular basis. Apparently one of the most complicated and threatening problems existing in the world today is cybercrime. It is an all-inclusive term used to differentiate between two kinds of activities namely: 'cyber dependent' and 'cyber enabled' crimes.

Since the evolution of cybercrimes humans have been able to discover and identify the source from where these crimes are or have originated in some or the other way even though it might be impossible to bring the perpetrators to conviction because of jurisdictional issues or so but there is a third category of source where these crimes are originating and are on a rise. This source is known as the 'Dark Web' which is accessible only through special software by incognito users. The 'Dark Web' today has created a commotion for law enforcement agencies worldwide.

The present paper titled, "THE CHALLENGES AND ISSUES SURROUNDING THE DARK WEB, A CLANDESTINE COSMOS" deals with numerous facets of the 'Dark web' and its impact on the society, legality of accessibility around the world, the criminal activities arising out of it, the jurisdictional issues, the administrative public policy regarding it, the steps taken by law enforcement agencies of various countries in order to prevent it and other facets.

I. INTRODUCTION- KNOWING THE MYSTERY OF THE DARK WEB

Majority of the online users have access to the World Wide Web on daily basis yet they are oblivious of the basic structure of the internet and the ways in which its levels interact. It is only when the news about illicit activities and cases like that of Silk Road, Snowden leaks, Bazee.com, the Blue whale game challenge etc. hit the mainstream news channels to local newsfeed and pop-up notifications in the user's gadget, that the public in general comes to know about the deeper pool of sites and the information available on the internet. [1]

[1] Elizabeth Vandesteeg and Jeffrey Goldberg, "*What lies beneath the surface: The Dark Web*", Law Journal Newsletters, Newsletters.html.

'THE SURFACE WEB'

The structure of the web is always explained by comparing it with an iceberg the tip of which symbolizes the topmost stratum of the internet known as the 'Surface Web'. It is this surface web that forms the visible part of the web and is accessed in the form of indexed pages through a web browser; by millions of average users or consumers on daily basis. Though the surface web appears to be gigantic, in reality it forms only 4 percent of the entire web. After the surface web comes the silhouette which is formed by the other two layers of the internet namely the 'Deep Web' and the 'Dark Web'. Both these terms of web sound similar, however they are not. The Deep Web being accessible by entering password for protection is legal and much bigger whereas the Dark Web on the other hand is majorly illegal and can be accessed by some special browser as mentioned in the beginning e.g. TOR (the 'Onion Router'), I2P('Invisible Internet Project'), 'Whonix', Sub graph OS, TAILS(The Amnestic Incognito Live System) etc.

'THE DEEP WEB'

The 'Deep web' is beyond the reach of traditional web browsers like chrome or search engines like Google because the material which it accommodates is not indexed and secondly it requires a specific URL to access a particular page. [2] There always exists a concoction between the 'Surface Web' and the 'Deep web' in a way that the users that make queries in the search boxes of the conventional search engines might get directed to the non-indexed content relating to their query on the deep web. It becomes important to have clarity in mind that the 'Dark Web' is a part of the 'Deep web' and should not be mistakenly confused with deep web because of the terminology.

'THE DARK WEB'

The Dark web exists as an intentionally concealed space of the deep web which covers almost 0.03 percent of the entire web and is accessed by a very minor portion of the population.

It is because of the anonymity of the 'Deep web' that all kinds of crimes flourish here like selling off prohibited drugs, trade of child porn to even hiring killers on contract. The Dark

[2] Sophia Dastagir Vogt, *The Digital Underworld: Combating Crime on the Dark Web in the Modern Era*, 15 Santa Clara J. Int'l L. 104 (2017).
Available at: https://digitalcommons.law.scu.edu/scujil/vol15/iss1/4

Web also carries an unlicensed and illegal variant of 'eBay', known as 'The Silk Road', which puts on illegal sale of goods and services. The Dark Web also hides information behind the security terms and pay walls of certain companies.[3] Almost all the sites on the dark web are able to hide their identity with the help of 'Encryption service'. There are special softwares like 'TOR' also known as the 'ONION ROUTER' and the I2P also known as the 'Invisible Internet Project'; which are used to access the Dark Web. The question is how does it work? The answer to which is when suppose one connects with a TOR site then a meeting point is randomly generated between a randomly generated URL (uniform resource locator) and a random network connection thus generating anonymous communications in both directions.

II. THE HISTORY OF DARK WEB

The Dark Web has existed for a long time underneath the surface of the internet. The internet's development began in the 1960s as part of the U.S. Department of Defence's effort to network their computer systems, but the internet did not become a household name until the 1990s. The Dark Web itself remained obscure to most people, but it gained a measure of infamy in 2013, when Ross William Ulbricht (alias Dread Pirate Roberts), operator of the Silk Road, was arrested. The Silk Road was a marketplace for illegal goods and services accessed through Tor.[4]

A brief timeline of the evolution of the DarkNet is explained here as follows:-

- 1969- Invention of ARPANET for transmission of electronic messages which acted as a progenitor of the internet. It led to the setting of unlisted and covert networks using ARPANET framework.
- 1970's - ARPANET used for drug deals
- 1980's - the invention of 'Data Havens' for storing and keeping away the sensitive information out of the reach of authorities.
- 1990's- peer-to-peer file sharing of mp3s and music files through compression algorithms.

---

[3] Laverty, Shea. *"Advantages, Disadvantages and Risks of Deep Web Search Engines."* Small Business - Chron.com, http://smallbusiness.chron.com/advantages-disadvantages-risks-deep-search-engines-74087.html.

[4] Michael Chertoff (2017), "*A public policy perspective of the Dark Web*", Journal of Cyber Policy, 2:1, 26-38, DOI: 10.1080/23738871.2017.1298643

- 2000- Invention of a web browser named 'Freenet' by a software developer named Ian Clarke; which allows users to browse illegal and sensitive content on the internet in complete anonymity.
- 2002- Creation of TOR (Onion router) by a branch of US Naval Research Laboratory, to keep the law enforcement agencies and undercover operatives untraceable. Eventually it fell into the hands of wrong people only to be used for illegal purposes.
- 2002- Claim by Microsoft engineers in the paper titled, "The Darknet and the Future of Content Distribution." that information will spread easily and it would become extremely difficult to prevent theft of copyrighted content.
- 2005- Piracy of films and software programs were on a rise.
- 2008- Invention of 'Bitcoin' by Satoshi Nakamoto. Bitcoin is the digital currency that operates worldwide and is beyond the control of any government or institution i.e. money is being sent anonymously without the involvement of any bank or intermediary. This has lead to laundering of bitcoin services.
- 2011- Awareness about 'The SilkRoad' website- an online market for online sale of illegal drugs which required a TOR connection and digital payment (bitcoin).
- 2013- Discovery by the authorities, of terrorists communicating and coordinating attacks through sophisticated version of the DarkWeb.
- 2014- Shutdown of silkroad with the arrest of its creator (Ross Ulbricht) leading to launching of SilkRoad version 2 within a month.
- 2016- a study by King's College of London titled, 'Cryptopolitik and the Darknet', claimed to have found around 5,205 TOR websites on the DarkWeb, 57 percent of which were involved on offering illicit services and content like money laundering, firearm sales, counterfeit currency, stolen credit cards, sales of prescription and illegal drugs, hacking, violence such as hit men for hire, and adult material involving violence, children, and animals.[5]
- Present date- the conjunction between cryptocurrency and the DarkWeb continues to stay to keep the illegal activities undetected.

[5] https://www.ranker.com

III. LEGAL, JURISDICTIONAL AND TECHNICAL CHALLENGES FACED BY COUNTRIES IN PREVENTING CYBER CRIMES ORIGINATING FROM THE DARK WEB

The legal enforcement departments worldwide due to the intensification of the cybercrimes on the deep, dark and the surface web are facing difficulties in bringing the criminals to conviction because of its clash with consumer's privacy rights. The consumers demand technology that offers more privacy and anonymity. Just when the users become content or satisfied of the encryption services provided by various applications, social websites or portals, the next moment international or regional media comes up with a news of data leak by popular sites like Facebook or disclosure of government hacking operations that leads to a hue and cry, worldwide debate and criticism.

The kind of hacking methods that are used by the law enforcement for catching the alleged perpetrator on the dark web will result in data breach activities which might interfere with the sovereignty of other countries. The risk of ending up a government in other state is high while following up an electronic sequence in the process of hacking the dark web, therefore the government has to take into consideration the issue of sovereignty. The law of nations permits a foreign country to exercise criminal jurisdiction under following five circumstances: (1) acts with effects within the nation; (2) to protect the interests of the nation; (3) the offender's nationality; (4) nationality of the victim; and (5) universal jurisdiction.[6]

The issue is that when the administration begins hacking the dark web it does not have the slightest idea that whether there are impacts in its own region and is not aware of the nationality of either of the victim or that of the perpetrator. The real problem of this issue is the anonymity of the dark web. Until the government is able to track a criminal transaction it will not be able to assess any of the aforementioned aspects. Then only the government would be able to find about the nationality of either the victim or that of the offender, about any internal impacts, or if there exists universal jurisdiction. The ability of the hackers to adapt and create new destructions is equally proportional to the need of the nations to respond and prevent future cyber threats. This realization has resulted into foreign nations promulgating conventions aiming to avoid and reduce cyber crimes.

[6] McCormack, Wayne. "International Criminal Law: Cases and Materials.", West Academic Publishing, 2015, p. 30

The enforcement of law is bound by the jurisdictional boundaries created between states worldwide. Considering the impact of the Blue Whale Game Challenge which originated in Russia it caused numerous child suicides worldwide including India apart from 18 other countries, all that the Ministry of Electronics and Information Technology could do is request various internet companies like Facebook, Yahoo, Google etc. to remove all the links that directs to the lethal game, but the Indian Government could bring the creator of the game to conviction on extradition or by any other means. The Indian Government might need to introduce tougher laws because effective monitoring and removing such content on popular sites is impossible and secondly there is nothing to prevent such content from resurfacing on other sites, for example the Dark Net. Each legislation regarding a particular crime operates within the territory of a particular state in which it has been framed and it proves to be inconsistent when crimes cross boundaries. This territorial jurisdiction over which action can be taken differs throughout the boundaries of states and it affects their ability to cooperate with each other. It is a time-taking process and requires a lot of patience in negotiating with the governments which makes justice seem delayed. Almost all kinds of crimes that could be committed in the physical world can be carried out remotely not only across the country but from far-off places on the globe. The essence of the Dark Web lies in the anonymity of the user. The speciality of TOR is that it bounces the user's IP address multiple times a minute so that if one time the location it shows is India the next moment it will locate it in Istanbul or United Kingdom. Using TOR might bring a user under surveillance but the identity cannot be traced if the user is using TOR, I2P or a similar browser through VPN (Virtual Private Network).

One of the real obstacles that cyber investigations have to face are the long durations taken by experts in gathering evidence and following legal procedure (sometimes ending up to six to eight months or in some cases even 5 years). There are some countries that cannot afford advanced technical and human resources to deal with cyber crime cases. On the other hand highly trained specialists are most likely to work for private sector in expectation of an attractive salary.[7]

As far as India is concerned the only piece of legislation that deals with cybercrimes is, 'The Information Technology Act 2000' and its 'Amendment Act 2008', but it is not dedicated to prevention of cybercrimes rather it works in conjunction with the conventional laws to bring

[7] https://www.rsis.edu.sg/wp-content/uploads/2018/06/Event-Report-on-Cybercrime-Workshop-by-CENS.pdf

the perpetrators to conviction. This piece of legislation was enacted with the sole objective of providing legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, to give legal recognition to electronic documents and digital signatures, facilitate the filing of electronic documents with govt. Agencies and to amend certain Acts like the IPC, Indian Evidence Act, Banker's Book Evidence Act, Reserve Bank of India Act and other matters. When it comes to cybercrimes there is only a particular chapter, chapter XI titled 'Offences' that deals with the criminal liability and that too of specific offences. For the cyber offences which it does not cover there are provisions of other conventional laws to bring conviction.

Since the dark web has become a major source of drug dealing, especially drugs like cocaine, LSD and MDMA which are not produced in India, it becomes difficult to trace the dealers and vendors online because the transactions are done via bitcoins which are almost untraceable. The Information Technology Act does not deal with bitcoins in any of its provisions but a circular titled "Prohibition on dealing in Virtual Currencies" has been issued under various provisions of Acts like the Banking Regulation Act, the Reserve Bank of India Act and the Payment and Settlement of Systems Act prohibiting all kinds of banks, non-banking finance companies and payment service providers from carrying any sort of deals involving virtual currencies or providing services for facilitating any person or entity in dealing with or settling virtual currencies.

In order to get a better understanding of the abovementioned concept it becomes pertinent here to explain the concept of bitcoin. Unlike the fiat currency there are two types of currencies namely the 'Virtual Currency' and 'Cryptocurrency'. Virtual Currency digitally represents a value which can be traded digitally and it functions but it does not carry a status of a legal tender (a fiat currency or real money/paper money is treated as a legal tender) in any jurisdiction since it is not issued or guaranteed by any jurisdiction and it operates only through an agreement within a community of specific users of that virtual community. Cryptocurrency is convertible virtual currency protected by cryptography. In order to transfer the value from one individual or entity it relies on public and private keys and requires to be cryptographically signed every single time. Bitcoin is basically an example of cryptocurrency and is not recognised as a currency in India by the RBI.

Use and trade of Virtual Currencies, may however, raise privacy concerns, including of protection of information/sensitive personal data and information of every individual dealing with such Virtual Currencies requiring the use of Virtual Currencies, to adhere to the rules and regulation prescribed under the data protection laws of India, primarily the Information Technology Act, 2000 read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.[8]

Lack of technical skills and expertise among investigators and unavailability of experts hampers the cybercrime investigations. The expensiveness of the equipments and softwares used in tracking or monitoring activities on the darkweb is another significant problem in some countries which might slower down the process of investigation.

Building a case against cybercriminals requires a thorough knowledge of the characteristics of malware involved, such as how these programmes affect microphones recording, screen captures and webcams. Legal challenges are also involved. For instance, Orcus developers were careful not to use the programme themselves.[9]

Another reason for increase of cyercrimes on the DarkWeb is that there is abundance of information regarding basic techniques for committing cybercrimes and developing hacking skills and can accessed via youtube and other portals available on the surface web or deep web very easily.

There reason why the law enforcement agencies again find it difficult to address this situation is that there is a mushroom growth of such websites offering illicit services even if the authorities keep on monitoring these websites on the web and they are brought down.

IV. PREVENTION OF DARK WEB ATTACKS ACROSS THE GLOBE

Countries worldwide have been placed into two categories by the United Nations namely the developed and the developing countries; on the basis of technological advancement and industrial development. Policing activities on the DarkWeb requires creativity and exceptional level of intelligence matching to that of the perpetrators. There is no single method that has been tried by the law enforcement agencies across the world to curb such crimes.

---

[8]http://www.mondaq.com/india/x/583670/fin+tech/Legal+Status+Of+Virtual+CurrenciesCryptocurrencies+In+India

[9] Id. at 6

In developed countries coordinated policing i.e. the law enforcement agencies working in collaboration with the federal agencies have made it possible to track rackets online.

In July 2017, joint efforts by the U.S. Federal Bureau of Investigation (FBI) and Drug Enforcement Agency (DEA), Dutch police and Europol orchestrated the takedown of AlphaBay and Hansa, formerly among the largest darknet markets. The sting was creatively planned and well executed. First, law enforcement seized AlphaBay and made it known. This then prompted users switch to Hansa, which was under the control of law enforcement after they had seized the market's servers around the same time. They collected information on the users who logged in and obtained various IP addresses, which they used to build their cases.[10]

Secondly the developed countries constantly conduct researches into new ways of policing the activities on the DarkWeb. For instance the use of 'Artificial intelligence powered crawler' that scans the dark web for suspicious activities and alerts law enforcement when it comes across any such activity. However this technology has yet to be used universally, although it offers the promise to aid in the fight against crime on the dark web.[11]

Creation of special search engines like 'MEMEX' by U.S. Defense Advanced Research Projects Agency (DARPA) to uncover illegal activities on the Dark web and fighting human trafficking. It is similar to TOR but the only difference that exists between the two is that TOR is used to access the Dark Web while Memex is used to track the activities on the Darkweb.

Another technique is the 'Network Investigative Technique' which uses malware (a software designed for the purpose to gain unauthorised access to a computer or to disrupt and damage it) being sent to the users to identify the suspects.

[10] Dark%20Web%20Policing%20in%20Developed%20vs.%20in%20Developing%20Countries%20_%20Dark%20Web%20News.html (Home Page- https://darkwebnews.com/)

[11] Ibid

In 2012 in an investigation titled “Operation Torpedo”, the FBI utilized a method called NIT, also known as “network investigative technique,” to unveil the IP addresses of minimum least twenty-five individuals who visited kiddie porn websites on the dark web.
‘Poisoned water Hole’ is another technique used by police to track the suspect operating from a different geographical location and linking up information regarding that to the investigating agency conducting operation in that particular region. Inspite of existence of few of these techniques the criminals are finding new ways to evade capture and increasing their ability every day to carry on illicit activities on the Darkweb.

Talking about the Policing the Dark web by the developing countries they are still under the process of getting acquainted with the realities of the Dark Web and due to scarcity of resources they rely on the intelligence rendered by the developed countries . They apply the usual methods of identifying the suspects and capturing the perpetrators like infiltration or a tip off. For example India in its first case of arrest of vendors of drugs on the Dark web, the Delhi Police Crime Branch had arrested two people who were accused of running drug ring through dark web marketplaces in Delhi and Noida. [12] The Crime Branch worked in collaboration with the Narcotics Control Bureau and Ministry of Electronics and Information Technology to track the drug ring.

The Indian government is working with the Intelligence Bureau (IB) to amend the Information Technology Act, in order to deal more ruthlessly with dark web cybercriminals. The IT Act of 2000 was enacted by parliament and was signed by President K.R Narayanan back in 2000. The Act has been effective since then, and it has been addressing all issues regarding electronic documents, e-signatures, and other related records. The law also touches on the penalties to be given in cases regarding security data breaches such as damaging computer systems and taking part in cyber terrorism. As per a senior Union Home Ministry Official, the servers of popular internet companies, like the social media platforms, ‘WhatsApp’ and ‘Gmail’, are based outside India’s jurisdiction. The encrypted data and unshared keys are kept at bay for the law enforcement in India to monitor.[13]

Certain viable steps that need be addressed by the law enforcement agencies to check the illegal activities on the DarkWeb are discussed hereunder as follows:-

[12] https://www.indiatoday.in/india/story/dark-web-bitcoin-drug-dealing-dj-party-drugs-1080384-2017-11-06
[13] DeepDotWeb.com

- One of the expected amendments in the IT Act proposes the sharing of keys by popular internet companies whose servers are not located in India, with the security agencies of the India for effective monitoring.

  A similar action was taken by the Chinese and German governments regarding the company, Microsoft, which had to comply with set regulations. Therefore, a better environment was created for the law enforcement agencies to monitor their servers for any cybercrime occurring in their systems. [14]
- Cybercrime being dynamic phenomena its definition varies from nation to nation. Talking about India, the Information Technology Act, 2000 or IT Amendment Act does not define Cybercrime. Therefore similar to International Court of Justice there should be a global cyber platform or an apex body to deal with major threats like cyber terrorism, cyber warfare, dark web crimes, with the consensus and membership of various countries facing the territorial jurisdictional issues and infringement of sovereignty. There should be a popular consensus of the member countries as to what constitutes 'cybercrime'.
- In order to tackle the ever-changing nature of cybercrimes the law enforcement agencies should act vigorously in framing stringent rules regarding cyber security.

- The Dark Web is basically the hub of all and any criminal activity that can be imagined. The law enforcement agencies in order to penetrate into this hub needs to have access of criminal forums and communities, befriend criminals or suspects, and then put them to conviction. [15]
- 'Mutual legal assistance' can be one way which can be adopted since it facilitates international cooperation between nations, to provide assistance to each other regarding solving criminal cases. But it has its own drawbacks as conflict arises between the signatory nations regarding prohibition and compulsion to disclose data and secondly lack of clarity as to how much, when and with whom the data needs to be shared.
- Apart from Mutual Legal Assistance and as a part of it, courts must also determine which laws need to apply on interchange of data among various jurisdictions. The international community has developed a deep distrust in U.S. intelligence practices as a consequence of the Snowden leaks, thereby making collaboration more difficult.

---

[14] Ibid
[15] Id. at 6

- In the initial phase developing nations like India can rely on using 'honey pot traps' that portray to be related to illicit activities but are actually set by the investigative agencies to track the IP address of the web users.

  The tactic employed by the FBI was that the agency created a site called "Playpen" to lure internet criminals. This resulted in significant backlash as the site "included links to more than 23,000 sexually explicit images and videos of children including more than 9,000 files that users could download directly from the FBI." In response to the present activity of FBI using these files, the Justice Department stated that "children depicted in such images are harmed each time they are viewed, and once those images leave the government's control, agents have no means to prevent them from being copied and re-copied to other parts of the internet." The FBI continued to stand firm by their utilization of the files, with one official claiming that "there was no other way we could identify as many players" on the Dark Web. Aside from the ethical dilemmas posed by law enforcement participating in illegal activity to "trap" online criminals, there are further concerns regarding this method of enforcement.[16] On one hand for developed countries it might be a debatable question that this technique might not be the most effective method of policing the darkweb but for the developing countries it might work in the initial stage.
- Raising public awareness especially among the youth and children about the potential threats that dark web can cause because they are vulnerable to their curiosity and urge to access the misleading and suspicious websites, cookies and games thereby falling prey to the baits thrown by the cybercriminals from the darkweb leading to their victimisation. They need to be made aware of the psychological factors that trigger the urge to access such websites and the factors which facilitate online abuse. The older generation might appear to be vulnerable but they are mostly callous and unaware of the special browsers used to access the darkest part of the deep web and the technicality involved in it. They might fall prey to conventional forms of cyber crimes like hacking (unlike ethical hacking), cyber fraud, spamming, phishing etc.
- There has to be a nexus between manual monitoring and internet regulation. Strict checking needs to be done of courier and shipping services that make it possible for the import and export of drugs, animal trading, human trafficking after the online sale is

[16] Brad Heath, *FBI ran website sharing thousands of child porn images*, USA Today (2016). https://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346/

completed; by means of covert operations carried out by authorities of countries who are signatories to reciprocal agreements.

- Another way to reduce transboundary attacks is framing of international agreements and cybercrime legislations. Countries following these conventions experience attacks to a lesser extent than countries avoiding or violating the terms of such conventions.

  International bodies like INTERPOL and EUROPOL are important resources that are well placed to coordinate law enforcement activities over different jurisdictions.[17]

V.CONCLUSION

While it is completely impossible to end the Darkweb in its entirety, the best possible solution to reduce the effects of it on the society is to upgrade the existing methods and techniques to perfection and strengthening cooperation among the nations. There is a need to incorporate flexibility in the procedural methods to facilitate negotiation among the nations and a need to frame strict rules and regulations to deter the criminals from repeating the offence. Where there exists an international agreement it becomes easier to catch the criminals but the problem arises where there is unavailability of a reciprocal agreement for example countries like North Korea and certain other specific countries that do not have an extradition treaty signed with the superpower USA. As far as India is concerned she is carrying bilateral agreements with countries like USA, Russia, Israel etc. but what it required is a multilateral agreements which are effective. The Europe Council of Budapest Convention on Cybercrime is one such convention of which India needs to be a part in order to accelerate her efforts to combat cybercrimes at International level. The reason why India needs to be a signatory of this treaty is because it is a dynamic framework representing a triangle of standards commonly used in prevention of cybercrimes namely ‘follow-up’, ‘assessments’ and ‘capacity building’. Besides that this treaty is supported by various programs supported by 10 and more international organisations including INTERPOL, UN office on drugs and crime etc. which can be of major help to a country like India which has already started to establish its footsteps globally in major events, collaborations, international relations and negotiations.

Since she is gaining centre-stage attention day by day, India should work in the direction of improvising her relations with developed nations in consonance with reliance on latest methods facilitating cyber security, modern techniques, skilled expertise and gather funding for it.

[17] https://www.rsis.edu.sg/wp-content/uploads/2018/06/Event-Report-on-Cybercrime-Workshop-by-CENS.pdf

Lastly the traditional policing techniques cannot be ignored as cases have been solved by the law enforcement agencies by infiltrating the criminal communities.

