RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
JUNE 2020

DOI: 10.5281/zenodo.3909907

Surge in Dark Web Crimes, the Indian Legal Scenario and 'International Cooperation' as the Way Forward

Shubha Ojha

Shubha Ojha, B.A. LL.B. (Hons.) National Law University Jodhpur, India, shubhaojha0698@gmail.com

ABSTRACT: In today's technology-driven world, advancements in the internet domain seem to know no bounds. However, while the internet arena has created multiple avenues of development, it has, at the same time, opened up gates for a flurry of illicit activities. Dark web crime has emerged as one such ominous activity that looms over the virtual world and threatens legal systems all across the globe. What started off as the first major internet debacle brought about by the 'Silk Road' episode, has now become a source of serious concern for establishing rule of law in the information society. This article delves into the turbid cloud of dark web crimes thriving in the cyber space and the current legal scenario in India to regulate the surge in such malpractices. What stands as a stumbling block before the law enforcement agencies is the transnational element of dark web crimes. While the Indian Penal Code and other legislations comprise provisions related to both territorial and extra-territorial jurisdiction, the extra-territorial jurisdiction is such that it leaves a lot of ambiguity in terms of applicability of Indian laws to cyber offences that may be committed by foreign nationals overseas but the effects of which are felt in India. The author, through the course of this article, brings to light loopholes in the criminal and cyber laws of India, proposes international cooperation as the need of the hour, and analyses if the Budapest Convention on Cybercrimes provides an efficacious solution in this context.

KEYWORDS: dark web crime, Silk Road, cyberspace, extra-territorial jurisdiction, Budapest Convention

Introduction

Internet provides a platform for individuals to interact with one another. This platform, over time, has widened its ambit and has gone to the extent of providing an avenue where goods and services are transferable. It has also opened the door for the transfer of illegal good or services. In fact, one among the first things to be purchased and sold online was marijuana, which was a transaction between students at Stanford and MIT in the early 1970s (DiPiero 2017, 1268; Anderson 2013). In the contemporary times, there has been a surge in the trade of illegal substances or services through the technical and sophisticated methods provided by the cyberspace. This has resulted in increased concerns over cybercrimes and the effectiveness of government surveillance. One of the first platforms for dark web was provided by a dark net market "Silk Road" and the users of the Silk Road website could buy anything-drugs, child pornography, arranged murders, hacked credit cards, and countless other illicit activities and substances-using the virtual currency of bitcoin (Anthony 2013). This website was shut down by the US government, however this turned out to be the initial source of momentum that paved way for a plethora of similar websites, not only in the US but all over the world, including India. Multitudinous platforms involving Agora, Evolution, Andromeda, Pandora, Outlaw, Pirate, Tor Bazaar, Alpaca, and Cannabis Garden, etc. emerged ever since the shutdown of Silk Road (Thakurta and Jain 2017).

This article deals with the increasing dark web crimes in the cyberspace and the current legal scenario in India to regulate such malpractices. While the Indian Penal Code provides for both territorial and extra-territorial jurisdiction (Section 4, the Indian Penal Code, 1860), its extra territorial jurisdiction is such that it leaves ambiguity in the applicability of the IPC to cyber offences that may be committed by foreign nationals overseas, but in a way, their impact is felt in India (Rastogi 2014, 5) This transnational element of dark web crimes calls for greater international cooperation which would further require investigation of offences in other nations and the arrest of cybercriminals of other nationalities will require established extradition treaties

and special permissions. This article provides for a solution to these loopholes by suggesting India's ratification of the Budapest Convention on cybercrimes.

What is Dark Web?

There are three essential layers of the Internet-Surface web, Deep web, and Dark web. First, there is the "Surface Web", which refers to anything that typical search engines like Facebook, Google and Yahoo can find (Bright Planet 2014). Secondly, Deep Web is that layer which generally provides access to academic databases, proprietary databases, user databases, web-forums requiring registrations. Basically, these are the web pages that cannot be accessed directly through the typical search engines. Then comes the third layer that is the "Dark Web" which is a small part of the Deep Web that has been intentionally hidden. This can be ingressed only through specialised interfaces such as the Tor network (Romeo 2016, 75). A network like Tor can be downloaded by anyone and it lets its users browse the web anonymously. This network was developed to protect online communication among military and governmental agencies in the US and to facilitate open source intelligence gathering (Romeo 2016, 76). Dark web networks such as Tor let users exchange messages while maintaining their anonymity through a process known as "onion routing" (Romeo 2016, 76). Analogous to the layers of an onion, dark web hides identities by wrapping layers around people's communications, making them untraceable. With the advent of the case of Silk Road, Dark Web became a major perpetrator of cybercrimes, thus negatively impacting cyber security.

Acceleration of the Growth of Dark Web Crimes through Cryptocurrency

Use of bitcoins as a medium of exchange has opened gates for the prospective growth of transactions in the cyberspace. However, it has also opened gates for the misuse of the lucrative prospects provided by the cyberspace. Cryptocurrencies, like Bitcoins, have become the most extensively used instrument for carrying out illicit transactions in the Dark Web (Chertoff 2015, 5). It is a completely self-sufficient, democratized currency that is not backed by any country or national bank and it also allows users to maintain their anonymity, thereby paving way for its instrumentality in Dark Web markets. It becomes almost impossible for a purchaser or seller to know where the currency is being transferred (Christopher 2014, 14).

Following the country's adoption of cryptocurrency, activities of dark web-based illicit traders has increased in India. The Information Technology Act, 2000 embodies the Indian law regulating cybercrimes, however, even though there have been reports of many cybercrimes since 2014, no prosecutions have involved illegal activities occurring on the dark web.

The Indian Legal Scenario

For the Indian legal scenario, cybercrime is a contemporary branch which has arisen as a result of the extensive use of computer network. With the evolution of the information society and its dependence on information and communications technologies ["**ICT**"], the vulnerability of societies worldwide to cybercrime has increased considerably and India is no exception. According to the National Crime Records Bureau, 9,622 incidents of cybercrime were recorded in 2014 under the Information Technology Act, the Indian Penal Code and state and local laws (Seger 2016).

The most commonly committed dark web offences involve sale of illegal goods or human trafficking. Thus, what results is the loss of property or persons which is punishable under the Indian Penal Code. Sections 370 and 370A of the Indian Penal Code deal with the offence of human trafficking. Section 370 criminalises offence of trafficking against one person, against more than one person, against a minor, against more than one minor, trafficking of minor on more than one occasion and trafficking by a public servant or a police officer. The online sale of illegal articles is governed by the conventional laws in India depending upon the article involved

in the illicit transaction. Internet activities involve persons and computer networks located in different parts of the world and considering the fact that each nation seeks to regulate the disputes involving its citizens or territory through its own law, there arises the issue of contradictory laws. Although there have been several theories and principles for the resolution of conflict of laws, none of these have been universally accepted (Chaubey 2012, 643). Thus, for effective regulation of dark web crimes, the need of the hour is *"International Cooperation."*

International Cooperation to Dodge the Bullet of Dark Web Crimes

The element of anonymity makes the platform of dark web a deadly piece of weaponry in the hands of cyber criminals (Chaubey 2012, 168). They have elements of high latency and very low exposure levels (Chaubey 2012, 169). It will become a tedious job for the law enforcement bodies in India to track such criminals as they usually operate from other countries. This corroborates the fact that it is not possible for a country to independently tackle the problems associated with dark web crimes.

United Nations

Computer network-related crimes have been the subject of explicit resolutions on part of the United Nations General Assembly ("UNGA") on a few occasions-

1. In 1990, UNGA endorsed the recommendations of the 8th United Nations Congress on the Prevention of Crime and the treatment of Offenders, which among other things, also involved a resolution on computer-related crimes (UN General Assembly Resolution, 45/121 of 14 December 1990).
2. In 2001, a second UNGA resolution was adopted for Combating the Criminal Misuse of Information Technologies, which made a series of recommendations to its member states regarding the need to eliminate safe havens and to improve cooperation between national law enforcement agencies (UN General Assembly Resolution, 55/63 of 22 January 2001).
3. UNGA, vide its resolution 65/230, initiated a study to convene an open-ended intergovernmental expert group to conduct a comprehensive study on the problem of cybercrime.

At a meeting during the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, held in April 2005 in Bangkok, it was reported that the UN is in the process of negotiating and formulating a UN Convention of Cybercrime (Chaubey 2012, 677). However, no further information with respect to the progress of this initiative and to giving the idea a concrete form has been published till date. The Twelfth Congress, held in 2010 in Salvador, also did not deal with this aspect. India should definitely look forward to any further developments regarding the above prospect. However, to meet the need of the hour India has to focus on the Budapest Convention on Cybercrime.

Budapest Convention on Cybercrime

The Council of Ministers had adopted the "Convention on Cybercrime", which was opened for signature in Budapest on 23rd November 2001 (The Convention on Cybercrime, European Treaty Series-No. 185 of 23 November 2001) and entered into force on 1st July 2004. The component of this convention which is of significance to India is that the Convention contains a mechanism whereby a non-member can sign and ratify the Convention (Art. 37 of The Convention on Cybercrime). For instance, Montenegro became a non-member signatory in April 2005 (Chaubey 2012, 670). The Preamble to the Convention lays down its aim that is to pursue *"a common*

criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international cooperation" (Sharma 2011, 366).

The Budapest Convention on Cybercrime has a threefold purpose. Firstly, it defines material criminal law in Chapter II, Section 1, which is a legislative harmonization effort aimed at creating a common crime base, secondly, Chapter II, Section 2 deals with the harmonization of investigation measures and criminal proceedings and, thirdly, the ways for International Cooperation are opened up in Chapter III of the Convention (Moise 2017, 28). The Convention also has a comparatively wide-ranging scope. The offences under the Convention are categorized into 4 groups. The first group of offences relates to offences against the confidentiality, integrity and availability of data and information systems, the second category of offences relates to computer-related offences, such as computer-related forgery and computer-related fraud, the third group of offences includes offences related to content, such as offences related to child pornography and the fourth and last category of offences includes offences related to infringements of intellectual property and related rights (Moise 2017, 29).

In 2003, the Additional Protocol to the Council of Europe Convention on Cybercrime was signed in Strasbourg on the criminalization of acts of a racist and xenophobic nature committed through computer systems (Additional Protocol to the Convention on Cybercrime, European Treaty Series-No. 189 of 28 January 2003). Moreover, various Articles of the Convention in a way fill the cavities caused by the lacunae in the domestic laws of various nations. For instance, Article 2 of the Convention embodies a stipulation as to the illegal access by safeguarding the integrity of computer systems by the way of incriminating unauthorized access to a computer system. The analysis and observation of various approaches with respect to illegal access to a computer system in the domestic law of various nations indicates that the provisions adopted therein sometimes cause a commotion between the illegal access and the offences committed after illegal access, or seek to restrict the incrimination of the accused only in cases involving serious infringements (Schjolberg 2003). The regulation of illicit trade through the medium of dark web can be effectively regulated under Article 8 of the Convention, which provides guidelines to criminalise acts involving the production, sale, procurement for use, distribution or otherwise making available of a device or a computer password, access code, or similar data, that can be prospectively used for committing dark web crimes and the Article also attributes intention on part of the actor. The offences related to child pornography and the offences related to infringement of copyright and related rights which are some other emerging cybercrimes within the ambit of the dark web are dealt with Articles 9 and 10 of the Convention, respectively. Thus, the Convention provides a platform wherein the unfilled gaps with respect to regulation of dark web crimes in India can be effectively mitigated.

The Convention also addresses the issues related to extradition under Article 24, mutual legal assistance between national law enforcement agencies under Article 25 to 34 and the establishment of 24/7 network of points of contact to support such assistance within Article 35. Article 40 of the Convention stipulates that at the time of signature or while depositing instrument of ratification, a nation can declare that it avails itself of the possibility of requiring additional elements as provided under Articles 2, 3, 6, 7, 9 and 27. An instance of application of Article 40 is provided through the example of Denmark, wherein it was stated that in relation to child pornography, Denmark's domestic law shall not criminalize images "*appearing to be a minor engaged in sexually explicit conduct, as permitted under Article 9 (4)*" (Reservation contained in the instrument of ratification deposited on 21 June 2005).

The comprehensive and extensive nature of the Convention, as well as the territorial buildout of its signatories substantiates the fact that the Convention is likely to remain the most important legal instrument in the field of dark web crimes and other cybercrimes. There have been other international initiatives in the field of cyberspace as well on part of APEC (Asia-Pacific Economic Cooperation) states, Organization of American States, the International Police Organization (INTERPOL), however, the Budapest Convention continues to be the most significant and efficient among the lot. The Budapest Convention has provided a stimulus for the

international compliance with respect to regulation of cybercrimes not only on the basis of the large number of signatories, including some of the non-European states and non-member states, but also on the basis of its other initiatives for international cooperation in the cyberspace such as the Commonwealth "Model Computer and Computer-related Crimes Bill" that caters to the requirements of around 53 nations (Chaubey 2012, 672).

Conclusion

An effective investigation, scrutiny and prosecution of cybercrime calls for a proper legislation. However, it must be kept in mind that the internet regime is dominated by the element of dynamism with constant developments taking place at the snap of a finger. Thus law-makers must be vigilant about such developments and ensure that the existing provisions are in consonance with them, that their effectiveness is monitored accordingly, especially keeping into consideration the turbulent developments in network technology. Thus, a full-fledged national law in the realm of cybercrime calls for a lot of investment in terms of time to establish legislations regulating new forms of cybercrime. Offences that would fall under the law will have to be reviewed and constantly updated.

It will be an onerous job for domestic law makers to execute the drafting process for cybercrime without international cooperation, due to the dynamism of network technologies and their complex structures. A separate cybercrime legislation may result in wastage of time, money and other resources and may also lead to significant duplication. While dealing with dark web crimes, it is also necessary to keep track of the development of international standards and strategies as crimes within the cyberspace cannot be limited to the developments in India. Efficacious confrontation with the surge in trans-national dark web crimes will fall under the pit, owing to the incompatibility and inconsistency of domestic laws and therefore international harmonisation of domestic legal provisions is the need of the hour. The Budapest Convention on Cybercrimes has come forward as a constructive international attempt for the purpose of such harmonisation. It has encouraged harmonisation worldwide and in fact the United Nations has recommended that its member states may develop an internal legal framework in the realm of cybercrimes by using this convention (Moise 2017, 36).

The Indian legal framework can greatly benefit by ratifying this convention. Cybercrime is a phenomenon dominated by dynamism, due to the constant changes occurring in technologies, along with criminal behaviour, across the globe and thus for combating the threat of dark web crimes India must move under the blanket of harmonization bestowed upon the international community by the Budapest Convention.

References

Anderson, Brian. 2013. "The First Thing to be Bought and Sold on the Internet was Some Weed." October 10, 2013. *Vice.com.* https://www.vice.com/en_us/article/qkkgep/the-first-thing-to-be-bought-and-sold-on-the-internet-was-some-weed.

Anthony, Robert. 2013. "The Craziest Things You Could've Bought on Silk Road, the Black Market of the Internet." *Elitedaily.com.* October 9, 2013. https://www.elitedaily.com/envision/the-craziest-things-you-couldve-bought-on-silk-road-the-black-market-of-the-internet.

Bright Planet. 2014. "Clearing Up Confusion - Deep Web Vs. Dark Web*"*. September 26. http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.

Brownlee. 2016. "The Deep Web and the Dark Web-An Overview for Lawyers." Intellectual Property Due Diligence in Corporate Transactions. § B.1:5.

Chaubey, R.K. 2012. *An Introduction to Cyber Crime and Cyber Law*. Kolkata: Kamal Law House.

Chertoff, Michael and Tobby Simon. 2015. "The Impact of the Dark Web on Internet Governance and Cyber Security." Centre for International Governance Innovation. https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

Christopher, Catherine Martin. 2014. "Whack-A-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering." *Lewis & Clark Law Review* 18(1):1-36.

DiPiero, Carmine. 2017. "Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web." *University of Illinois Law Review* 3 (2017): 1267-98.

Moise, Adrian Cristian. 2017. "A Few Comments on the Council of Europe Convention on Cybercrime." *Journal of Law and Administrative Sciences* 8 (2017): 28-38.

Rastogi, Anirudh. 2014. *Cyber Law, Law of Information Technology and Internet*. LexisNexis.

Romeo, A Dominick. 2016. "Hidden Threat: The Dark Web Surrounding Cyber Security." *Northern Kentucky Law Review 43*. No. 1 (2016): 73-86.

Sameeh, Tamer. "Bitcoin, the Dark Web and India." DeepDotWeb, Available online at https://www.deepdotweb.com/2017/06/07/bitcoin-dark-web-india/.

Schjolberg, Stein. 2003. The Legal Framework-Unauthorized Access to Computer Systems-Penal Legislation in 44 Countries. April 7. https://itlaw.wikia.org/wiki/The_Legal_Framework%E2%80%93Unauthorized_Access_to_Computer_Systems.

Seger, Alexander. 2016. "India and Budapest Convention: Why not?" *ORF online.* October 20. https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/.

Sharma, Vakul. 2011. *Information Technology Law and Practice*. New Delhi, India: Universal Law Publishing.

Thakurta, Paranjoy Guha and Shinzani Jain. 2017. "Excerpt: Silk Roads Emerge as Avenues of Illegal Online Trading." December 11, 2017. https://www.thequint.com/lifestyle/books/excerpt-silk-roads-emerge-as-avenues-of-illegal-online-trading.