INTERNATIONAL JOURNAL OF CRIMINAL BEHAVIOR AND SOCIAL POLICIES

VOL: 12 ISSUE: 1
MARCH., 2023
ISSN: 3997-6678

EFFECTIVENESS OF CRIMINAL LAW IN TACKLING CYBERCRIME: A CRITICAL ANALYSIS

Ajoy P.B.
National University of Advanced Legal Studies,
Kochi, Kerala, India.

ABSTRACT

A significant number of nations around the world have enacted cybercrime laws for the purpose of controlling the occurrence of cybercrimes and mitigating its ill effects. However, in spite of enacting such cybercrime laws, available data show that the incidence of cybercrime is rapidly increasing. There are many factors that contribute to the failure of criminal law to fully control cybercrime. These factors include anonymity related issues, jurisdictional issues, extradition related challenges, problems associated with the law enforcement machinery, non-availability of data relating to cybercrime including non-reporting of cybercrimes, difficulties to identify, locate and arrest the cybercriminal, lack of experts, technology related issues, problems posed by international law etc. Since, at present, criminal law is not able to fully tackle cybercrime, there is a need to focus on cybercrime prevention strategies.

KEYWORDS: Cybercrime, Extradition, Anonymity, Digital Evidence, Cybersecurity.

INTRODUCTION

Internet, as is known today, had its humble beginnings on 29th October 1969, when a message was sent over a leased telephone line from a computer located at the University of California at Santa Barbara, to a computer located at Stanford Research Institute covering about 350 miles (Kleinrock, 2010). Over the next half century, the internet grew in leaps and bounds and became a network of networks which is today made up of millions of computing/communicating devices which are interconnected together by means of various types of telecommunication systems (Froomkin, 2003). In 2018, which marks the 50th year of existence of internet, about 51.2% of the global population, which accounts to about 3.9 billion people had access to internet (International Telecommunication Union (ITU), 2018).

The explosive growth of internet has been of great benefit to mankind. Millions of people use the internet every day for a variety of purposes, like entertainment, social networking, learning, trading, etc. At the same time, a small percentage of internet users use internet for committing various forms of illegal activities/behaviour. Consequently, nation-states have enacted a number of cybercrime laws for curbing this illegal online activities/behaviour. However, these cybercrime legislations have not been able toeffectively tackle cybercrime. This article seeks to identify some of the major factors that have rendered criminal law less effective in tackling cybercrime.

RESEARCH METHODOLOGY

Even though the writing of this article involved some amount of interdisciplinary research, the primary focus of the article is criminal law and criminology. Consequently, the primary method of research followed is doctrinal research. Secondary data has been used in this article and primary data has not been collected.

Cybercrime Statutes and Conventions

When cybercriminals began to extensively utilize the internet for committing various forms of deviant behavior like fraud, sale/distribution of child pornography, sale of guns/narcotics, causing damage to computer resources, etc.(Chawki*et al*., 2015), the nation-states around the world responded by criminalizing these deviant behaviors. For this purpose, they not only enacted criminal statutes but also entered into a number of cybercrime conventions. Some of the criminal statutes enacted areUSA: Computer Fraud and Abuse Act, 1986. The federal and state legislatures have also enacted several piece-meal legislations to deal with cybercrimes.

UK: Computer Misuse Act, 1990

Japan: Unauthorized Access Law, 1999

Singapore: Computer Misuse Act, 1993

India: The Information Technology Act, 2000

Sri Lanka: Computer Crime Act, 2007

UAE: Federal Law 5 of 2012 on Combatting Cybercrimes etc.

Some of the Important Cybercrime Conventions are

Council of Europe's Convention on Cybercrime,2001

League of Arab States Convention on Combating Information Technology Offences, 2010

African Union's Convention on Cybersecurity andPersonal Data Protection, 2014

Cybercrime Statistics

A number of published empirical studies point to the fact that the occurrence of cybercrime is increasing in spite of the enactment of cybercrime legislations. For example, the results of an empirical study published by Accenture Security in 2019 showed that there was a 67% increase in the number of cybersecurity breaches in the preceding five years. During the same period, the average cost of cybercrime (loss caused by cybercrime) rose by 72%(AccentureSecurity, 2019). Similarly, in USA, FBI's cybercrime complaint reporting center, IC3 reported a significant rise in the number of cybercrimes reported with it between 2016 and 2020.According to IC3, the number of cybercrime complaints which stood at 2,98,728 in 2016 rose to 7,91,790 in 2020. During the same period, the economic loss suffered by the complainants in the above said complaints rose from $ 1.5 billion in 2016 to $ 4.2 billion in 2020 (Internet Crime Complaint Center, 2020). Similarly, a study conducted by a private agency, in 2020 showed that there was a 50% increase in cyberattacks using mobile banking malware in the first half of 2019 compared to 2018 (Check Point Software Technologies Ltd., 2020).

Coming to India, the official statistics published by the NCRB (National Crimes Record Bureau) also show a significant rise in cybercrime with each passing year. India recorded 50,035 cases of cybercrimes in 2020 which represents a 11.85% increase of such

crimes over the previous year. The rate of cybercrime (incidents/lakhs of population) in India also increased from 3.3% in 2019 to 3.7% in 2020 (National Crime Records Bureau, 2020). The following table illustrates the ever- increasing rate of cybercrime in India.

Table-1: Total number of reported Cybercrimes in India (2011-2020)

Year	No. of reported Cybercrimes	Increase over previous year
2011	2213	-
2012	3477	57.12%
2013	5693	63.73%
2014	9622	69.01%
2015	11592	20.47%
2016	12317	6.25%
2017	21796	76.96%
2018	27248	25.01%
2019	44735	64.18%
2020	50,035	11.85%

The above quoted statistics clearly point to the fact that the incidence of cybercrime is rapidly increasing. This is happening, in spite of the fact, that nations across the world have enacted several cybercrime statutes. Consequently, through a process of logical reasoning it can state that criminal law has been ineffective to curb the surge of cybercrimes.

Factors/Challenges Inhibiting Criminal Law from Effectively Controlling Cybercrime

There are a large number of factors/challengesthat inhibit criminal law from effectively tackling cybercrime. The most important of them are discussed below.

Anonymity Related Factors

The technical features of internet enable criminals to commit cybercrimes in cyberspace anonymously without revealing their identity(Pont, 2001). The anonymity features of cyberspace areexploited by criminals to commit a wide variety of unlawful acts like fraud, sale or distribution of child pornography, sale of gems and narcotics etc.(Chawki*et al.*, 2015).Many theories of cybercrimes including theSpace Transition Theory developed by K Jaishankar suggest that anonymity is one of the most important factors responsible for rapid rise in cybercrimes (Jaishankar, 2007). People due to their social status and position do not indulge in crimes in the terrestrial space. However anonymity offered by cyberspace removes these restraints and they commit cybercrime(Assarut*et al*., 2019).

Jurisdictional Challenges

The world is currently organized on the principle of state sovereignty and independence within the territorial limits of a nation-state. This implies that eachnation-state has the authority and jurisdiction to make and prescribe laws, enforce them and also adjudicate disputes arising out of the enactment andenforcement of laws(Houck, 1986). Consequently, the criminal justice system developed by each nation-state is enforceable only within the territorial limits of that state.

Cyberspace is however not limited by the geographical borders of nation-states. Crime committed by criminals in cyberspace transcends nation-states and territorial boundaries. A cybercriminal sitting in the comforts of his home located in one country can commit a cybercrime, the effect of which could be felt in any other country in the world(Ajayi, 2016). When the victim of the cybercrime is located in another country, many complex issues relating to jurisdiction arises. The victim's country would face a large number of legal and practical hurdles in enforcing its criminal laws against the perpetrator of the cybercrime.

Extradition Related Challenges

Extradition is a formal process by which a person usually accused of having committed an offence, is surrendered by one state to another state (Bassiouni, 2014). Relatively very few conventional crimes involve extradition as there is always some degree of physical proximity between the criminal and the victims (Chawki*et al*., 2015). However, that is not the situation so far as cybercrimes are concerned. Technologies associated with cyberspace enable a criminal to commit crimes at locations thousands of miles away from his location, at other jurisdictions (Brenner, 2004a). Consequently, relatively large number of cybercrimes is perpetuated across national borders. Hence extradition is a real issue in the enforcement of cyber-criminal laws.

Under the international law, there is no instrument or customary law that obliges a sovereign nation to automatically return criminals including cybercriminals for trial(Ajayi, 2016).Extradition is made possible through bilateral and multilateral treaties between nations. In the absence of such treaties, extradition is possible only by following the procedure prescribed in the national legislation of the country from where the extradition is sought. Such national legislations usually require the requesting state to approach a designated court/judicial tribunal. Either way, the extradition process is lengthy and cumbersome(Bassiouni, 2014).

ChallengesPosed by the Existing Law Enforcement System

The current criminal investigation system/law enforcement system including the operational procedures has been evolved to deal with traditional crimes. The same system is now being employed to deal with cybercrimes and cybercriminals. However, the existing system is not able to tackle/deal with cybercrime as cybercrime does not possess many of the features of real-world conventional crime(Brenner, 2004b). For example, real world crimes are on mostoccasions one-to-one crimes due to its corporeal nature.(Jetha, 2013) However, there is no such assumption in case of cybercrimes. In fact, cybercriminals can multiply the number of times a cybercrime is committed in a given duration of time by using automation techniques. The traditional system of investigation/prosecution is not equipped to deal with crimes of such large scale and can very easily get overloaded(Brenner, 2004b).

Challenges in Apprehending the Cybercriminal

Experience of law enforcement officers revealthat apprehending a cybercriminal is not an easy task (Brenner, 2004a). The unique technical features of cyberspace enable criminals to hide their identity and physical location at the time of commission of

offences(Pont, 2001). This anonymity makes it extremely difficult for law enforcements officials to trace the culprit. Additionally, the criminal may also make use of technology to assume the identity of an innocent person for the purpose of confusing investigators(Brenner, 2004a). Further, in case of cybercrimes there is no need of any physical proximity between the criminal and the victim. The nature of cyberspace is such that it allows a criminal located in one place to commit cyber-crimes like online fraud, intellectual property related offences, hate speech etc., the effect of which can be felt many thousand miles away(Brenner, 2004b). The lack of physical proximity between the cybercriminal and the victim as well as the huge physical distance between the place of investigation and the location of the cybercriminal has made it extremely difficult for law enforcement officers to apprehend the cybercriminal.

Factors Relating to the Scale of Commission of Cybercrimes

Technologies associated with cyberspace permits a large number of crimes to be perpetrated in an extremely short period of time. Further, many cybercrimes like online fraud can be automated enabling the cybercriminal to multiply by many times the number of cybercrimes that can be committed in a given period of time (Brenner, 2004a). Automation also permits the perpetrator to start the process of victimization and there after let the automated systems complete the process without any further involvement of the perpetrator(Brenner, 2004b). In this way, offenders can use technology to exponentially increase the number of cybercrimes that can be committed in a given period of time(Brenner, 2004a). The existing criminal justice system is not equipped to tackle such issues.

Factors Relating to the Nature of Evidence

Physical or tangible evidence, which iscommon in case of real-world crime, is rare in cybercrime prosecution. Since cybercrimes are committed in cyberspace which is a virtual environment, the evidence that is required to be presented in a court of law to secure the conviction of acriminal is for most part intangible digital evidence(Brenner, 2004a). The collection of such evidence presents new challenge to investigating agencies which were hitherto accustomed to the collection of tangible evidence. Digital evidence is difficult to handle and can be easily altered or erased (Casey, 2011). Digital evidence is usually voluminous requiring investigators to spend substantial time processing the evidence to identify evidence which is relevant to the case(Brenner, 2004a). Presently, a large segment of the law enforcement officers is not trained to deal with digital evidence.

FactorsRelating to Search and Seizure Procedures

Most of the cybercrime related laws enacted by nation-states around the world do not lay down any special procedure for search and seizure of digital evidence. Consequently, law enforcement officers rely on the traditional procedural law of search and seizure for collecting digital evidence. However, when the law that was evolved to address actions taken in physical world is extrapolated to deal with conduct that occurs in the cyberspace, numerous challenges arise(Brenner &Schwerha IV, 2002). For example, unlike real world physical evidence, digital evidence is extremely difficult to handle and can be easily corrupted(Casey, 2011). Consequently, digital evidence must be properly

collected and preserved. This involves huge investments both in equipment and training of law enforcement personnel. Currently, most countries around the world are not in a position to make such huge investments.

ChallengesPosed by the Lack of Effective Reporting and Dearth of Data

One reason that is significantly contributing to the difficulty in enforcing cybercrime laws is the lack of reporting of cybercrimes by victims particularly bybusinesses and corporate. The Commercial Victimization Survey (CVS) conducted in United Kingdom in 2013 is reported to have found that just 2% of online crime incidents were reported by businesses to law enforcement agencies. This was considerably lower in comparison to the reporting rates of other crimes like vehicle theft (100%), burglary (80%), etc. In case of general public, as well, the trend is no different. The Crime Survey for England and Wales (2007) reveal that only 1% of adult internet users reported hacking/unauthorized access to data.

The lack of effective reporting of cybercrime has resulted in the lack of sufficient data/statisticsrelating to cybercrime. Consequently, the public/businesses are not aware of extend of cybercrime(Ajayi, 2016). Further, the non-availability of data regarding cybercrime has made it difficult for cybercrime law enforcement policy makers to draw up long-term plans for dealing with cybercrime.

ChallengePosed by the Lack of Effective/Adequate Legislation

The non-enactment of adequate cybercrime legislations by nation-states has also contributed to the failure of criminal law to tackle cybercrime. A study conducted in 2015 showed that only 79 of the 201 countries in the world have enacted cybercrime legislations. This implies that only about 40% of the countries in the world have enacted cybercrime laws. More importantly 47 of the 79 countries which enacted cybercrime laws are European nations(Ajayi, 2016). This alarming situation has helped cybercriminals escape prosecution by basing their illegal action in a safe haven country which has not enacted cybercrime laws(Goldstone & Shave, 1998). Further, the extradition of such a perpetrator is not possible due to the principle of double criminality, according to which extradition is permissible only if, the alleged deviant behavior is an offence in both the requesting state and the requested state(Williams, 1991).

Challenges Posed by the Lack of Experts in Prosecuting Cybercrimes

There are no special courts to try cybercrimes. The same criminal courts that deal with the trial of real-world crimes also conduct trial of cybercrime cases. Consequently, the prosecution of both real-world crime cases and cybercrimes cases are conducted by the same public prosecutor. The qualification to be appointed as a public prosecutor is usually a minimum prescribed period of practice of law. For example, in India an advocate with minimum seven years of practice can be appointed as a public prosecutor. No special technical qualification is prescribed. However, the prosecution of cybercrimes requires special skill andknowledge(Brenner &Schwerha IV, 2002). Consequently, ordinary prosecutors would find it difficult to conduct cybercrimes cases as they do not have expertise/knowledge regarding technical aspect of internet/information and

communication technology. This is a serious handicap which is most likely to affect the conviction rate.

ChallengesPosed by Ill-Equipped and Ill-Trained Law Enforcement Agencies

Investigation of cybercrimes involves the use of technology. Costly equipment and gadgets have to be used by the investigating agencies to trace cybercriminals. For this purpose, law enforcement officers have to properly train in the use of technology and various equipment and gadgets. Only a few agencies like the FBI in USA have the financial resources to purchase costly gadgets and sufficiently train its workforce in the use of technology. However, due to lack of funds, vast majority of the law enforcement officers in most other countries around the world are not properly trained in the investigation of cybercrimes(Ajayi, 2016).

Challenges Posed by the Easy Availability of Devices/Tools and Access/ Instructions to Commit Cybercrime

An important reason for the failure of cybercrime statutes to control deviant behavior in cyberspace is the easy availability of technical devices like computers, hand-held devices, etc. necessary to commit cybercrime(Gercke, 2012). In the initial days of internet, a lot of technical knowledge was also requiredto commit cybercrimes(International Telecommunication Union (ITU), 2013). However today specialized software tools which facilitates commission of cybercrimes are readily available. Consequently, the need of the cybercriminal possessing technical knowledge is greatly reduced (Gercke, 2012). Most of these specialized software tools not only help the cybercriminal commit cybercrime, but also helps him hide his identity. Most nation-states are yet to enact laws prohibiting the use of such specialized software. So long as technology is permitted to assist cybercriminals commit cybercrimes, there will always be a steady growth in cybercrime.

ChallengesDue to the Limitations of International Law

The international law as it exists today is based on the concept of sovereignty of nation-states. Consequently, international law has no enforcement mechanism and it relies on the nation-states themselves for enforcement (Payandeh, 2010). Transnational cybercrimes are growing exponentially primarily due to the inability of international law to deal with the situation. For example, the Council of Europe's Convention on Cybercrime has come into force in 2004. However, the Council of Europe cannot compel the state parties to enforce those provisions within its territories. The Council of Europe cannot also compel any state party to provide international assistance in the investigation of cybercrimes as provided in the Convention. Consequently, the non-binding nature of international law coupled with the lack of enforcement mechanism has prevented the proper enforcement of cybercrime laws (Ajayi, 2016).

CONCLUSION

A large number of factors including those described above have cumulatively made it difficult for criminal law to effectively curb cybercrimes. All this point to need to establish an International Court or Tribunal for the investigation and prosecution of transnational cybercrimes particularly those of a grave nature. There is no international consensus at

this point of time, facilitating the creation of such an international tribunal/court. Even as such an international mechanism is being thought of, there is a need to adopt cybercrime prevention strategies to reduce cybercrimes. Various methods, technical or otherwise, that help reduce the opportunity to commit cybercrime should also be encouraged. Creating awareness regarding cybercrime among citizens, cybersecurity measures, privatepolicing of the internet etc. are some of the most important cybercrime prevention strategies adopted in actual practice.

REFERENCE

Accenture Security. (2019). *The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study*.https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Ajayi, E. F. G. (2016). Challenges to Enforcement of Cyber-crimes Laws and Policy.*Journal of Internet and Information Systems*, *6*(1), 1–12.https://doi.org/10.5897/JIIS2015.0089

Assarut, N., Bunaramrueang, P., &Kowpatanakit, P. (2019). Clustering Cyberspace Population and the Tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory. *International Journal of CyberCriminology*, *13*(1), 84–100. https://doi.org/10.5281/zenodo.3550473

Bassiouni, M. C. (2014).*International Extradition : United States Law and Practice* (6thed.). Oxford University Press. https://doi.org/10.1093/law/9780199917891.001.00 01

Brenner, S. W. (2004a). Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law andTechnology*, *9*(13), 1–52. https://www.researchgate.net/publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles

Brenner, S. W. (2004b). Towards a Criminal Law for Cyberspace : Distributed Security. *Boston University Journal of Science and Technology*, *10*,1–114. http://www.bu.edu/law/journals-archive/scitech/volume101/brenner.pdf

Brenner, S. W. (2010). *Cybercrime: CriminalThreats From Cyberspace*. Praeger. http://choicereviews.org/review/10.5860/CHOICE. 48-0685

Brenner, S. W., &Schwerha IV, J. (2002). Transnational Evidence Gathering and Local Prosecution of International Cybercrime.*The John Marshall Journal of Computer and InformationLaw*, *20*(3), 347–395. https://repository.law.uic.edu/cgi/viewcontent.cgi?a rticle=1139&context=jitpl

Casey, E. (2011). *Digital Evidence and ComputerCrime :Forensic Science, Computers and theInternet* (3rd ed.). Academic Press. https://dl.acm.org/doi/book/10.5555/2021194

Chawki, M., Darwish, A., Khan, M. A., &Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction* (1st ed.). Springer

InternationalPublishing.https://doi.org/10.1007/978-3-319-15150-2Check Point Software Technologies Ltd. (2020).*Cybersecurity Report*.https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

Froomkin, A. M. (2003). Habermas@Discourse. Net: Toward a Critical Theory of Cyberspace. *Harvard Law Review*, *116*(3), 749–873.https://doi.org/10.2307/1342583

Gercke, M. (2012).*Understanding Cybercrime: Phenomena, Challenges and Legal Response* (1sted.). International Telecommunication Union. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime legislation EV6.pdf

Goldstone, D., & Shave, B.-E.(1998). International Dimensions of Crimes in Cyberspace.*Fordham International Law Journal*, *22*(5), 1924–1971.https://ir.lawnet.fordham.edu/ilj/vol22/iss5/2/

Houck, J. B. (1986). Restatement of the Foreign Relations Law of the United States (Revised): Issues and Resolutions. *The International Lawyer*,*20*(4), 1361–1390. https://scholar.smu.edu/cgi/viewcontent.cgi?article =2444&context=til

International Telecommunication Union (ITU). (2013). *Electronic Crimes: Knowledge-based Report (Assessment)*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/ICB4PAC Assessment Eletronic Crime.pdf

International Telecommunication Union (ITU). (2018). *Measuring the Information Society Report(Volume 1)*. https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx

Internet Crime Complaint Center.(2020). Internet Crime Report 2020.In *Federal Bureau of Investigation*.https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Jaishankar, K. (2007). Establishing a Theory of Cyber Crimes.*International Journal of CyberCriminology*, *1*(July), 7–9. https://doi.org/10.5281/zenodo.18792

Jetha, K. (2013). Cybercrime and Punishment: An Analysis of the Deontological and Utilitarian Functions of Punishment in the Information Age. *ADFSL Conference on Digital Forensics, Securityand Law,* 15–20. https://commons.erau.edu/adfsl/2013/monday/7/

Kleinrock, L. (2010). An Early History of the Internet.*IEEE Communications Magazine*, *48*(8), 26–36. https://doi.org/10.1109/MCOM.2010.5534584

National Crime Records Bureau.(2020). *Crime inIndia-2020Statistics(VolumeII)*.https://ncrb.gov.in/sites/default/files/CII 2020 Volume 2.pdf

Payandeh, M. (2010).The Concept of International Law in the Jurisprudence of H.L.A. Hart.*European Journal of International Law*, *21*(4), 967–995.https://doi.org/10.1093/ejil/chq065

Pont, G. F. du. (2001). The Criminalization of TrueAnonymity in Cyberspace.*Michigan Telecommunications and Technology Law Review*,*7*(1), 191–216. https://repository.law.umich.edu/cgi/viewcontent.c gi?article=1142&context=mttlr

Williams, S. A. (1991). The Double Criminality Rule and Extradition: A Comparative Analysis.

Nova Law Review, *152*(2). 581–624. http://digitalcommons.osgoode.yorku.ca/scholarly_ works