International Journal of Cyber Criminology
Vol 14 Issue 2 July – December 2020

Global Surge in Cybercrimes – Indian Response and Empirical Evidence on Need for a Robust Crime Prevention System

Mohammed Shamiulla Arab[1]
Presidency University, Bengaluru, India

Abstract

Cybercrimes have increased with the increased use of computers. Measures have been developed at the national level to address the cybercrime issues; however, due to the nature of the crime, there is a need to adopt global frameworks. Various nations have developed internal legal measures to prevent cybercrime. The success of the measures can be fully effective through global integration. The international conventions have been developed to bring nations together and ensure that they join hands in fighting cybercrime. This paper addresses the history and introduction of cybercrime and their implications at the global level. Also, it analyzes the various measures used in addressing the crime and the challenges faced. Based on the analysis, the future of cybercrime can be easily analyzed to determine based on the effectiveness of the existing measures and policies governing cyber criminology and justice systems globally.

Keywords: Cybercrime, internet, cyber-terrorism, impulsivity, India.

Introduction

According to Lee, and Sanchez (2018), cybercrime is on the high increase, and this presents a major threat to various organizations. Cybercrime developed is as a result of the high technological advancement and the increased use of internet among the populations. The new trends of cybercrime are arising, and they are committed by both individual and groups. Companies have majorly invested in the data automation where they can store all their data digitally. The electronic system allows easy retrieval of important information that may be needed for business transactions. On the other hand, such companies are also at high risk of suffering from the cybercrime, and this requires that they advance their security systems to ensure data integrity and avoid loss associated with data breach (Rana, 2018). Additionally, cybercrime influences moral erosion and threats to the internet users who are likely to be exposed to the material or contents they did not intend to see. Furthermore, the increasing terrorism threats has been advanced by the online radicalization. Apart from the internal organization, policies are developed at the national

[1] Professor and Head, School of Law, Presidency University, Bengaluru, India. Email: mslegal2015@gmail.com

and international levels to curb the highly increasing and threatening menace. The purpose of this paper is to explore the legal perspective of the global response to cybercrimes.

According to Jigar (2016), internet usage continues to increase globally, and this means that the risks of cybercrimes and the victims increase significantly. For example, the number of internet users in India by 2016 was estimated to be 462,124,989 (Jigar 2016). With the increasing internet penetration, there is a need to safeguard the citizens from the growing cybercrimes. The common forms of cybercrimes may including hacking into an individual's or company's information systems and accounts, forgery, online gambling, cyber trafficking, child pornography and cyberbullying among others (Sarre, Lau, & Chang, 2018). Also, more dangerous forms of cybercrimes may include the cyber-terrorism, distribution of the pirated software, cyber warfare and possession of unlawful information (Sarre, Lau, & Chang, 2018). As a result, the general society is at high risk of suffering from any of the threats the more they use the internet. The purpose of this study is to explore the global legal framework used to prevent the cybercrime and the challenges experienced in the process.

Legal Response

The Internet has made the world a global village where people can engage and communicate easily regardless of their geographical distance. All the internet users are at risk of cybercrimes which may be committed by people from other parts of the world other than where they are located (Kerstens, & Veenstra, 2015). Due to this, there was a need to develop transnational policies that foster global security for all internet users. Therefore, a real and sound response to cybercrime requires international cooperation which involves equal input from all the parties involved in the international community (Sarre, Lau, & Chang, 2018).

On the other hand, some challenges present in the process of developing the legal frameworks to reduce incidences of cybercrimes in the society. Some of the common challenges include lack of cooperation and laxity among the members to enforce the global prevention programs and lack of legal measures to use in investigation and response to the threats (Lee, & Sanchez, 2018). The risks associated with cyber threats were minimal when the internet was first introduced. Throughout the historical experiences, people have been seeking to expand the scope of internet use in international integration as others seek to achieve their self-interests. The increasingly technological development mainly propagates the game power of the cyber threat. The development of cyberspace has developed both possibilities and threats as new players emerge and people scramble for opportunities, as well as others fighting to dominate the space.

New technology and the ubiquity of the internet has led to the world getting more connected than ever. The internet increment across the world is rapid. This has been seen to be more helpful. However, it has come with negative implications too. Cybercrime, software piracy, illegal downloading, hacking and cyberbullying are some of the negative vices. Illegal downloading has led to problems such as copyrights and loss of large amounts of money from companies. Hacking can pose security problems and also devastating to individuals, companies, or countries alike. Illegal downloading of software, movies, and most music has become an issue of concern. Some studies have tried explaining downloading and online piracy, and they include the social learning theory and self-control theory. Peers go online, find a copy of a movie and download it for free,

download a Cd illegitimately under these circumstances. As a result, the social learning approach associates deviant peers with an increased likelihood of committing software crimes, movie or music piracy. Research concerning digital piracy and self-control is scarce and often done in conjunction with social learning theory. The peers would go to the website with the intention of downloading the CD under this circumstance (Patney, 2017). This does not specify whether the CD is a movie, music or software. Thus the author encompassed all the possible types of digital piracy, and at the same time being difficult to differentiate them. Thus, low self-control and the impulsivity subscale are significantly associated with the intention of illegal privacy.

Indian Cybercrime Laws

The modern driven age and ensuring online privacy is becoming a major challenge. The exponential growth in the internet use presents both advantages and disadvantages. The initial cybercrime case was recorded in 1820 and the incidences have continued increasing daily thus triggering a lot of emotional, legal and political responses (Rana, 2018). The cyber laws in India are part of the general legal system dealing with cyberspace, internet and their respective legal issues (Rana, 2018). Cyber laws mainly cover the various elements including the freedom of expression and access to usage of the internet and ensuring online privacy. The information Technology Act of 2000 was passed in India and its main role was to deal with the cybercrime and the electronic commerce. The law was reviewed and amended in 2008 to incorporate section 66A which penalizes people for sending offensive messages (Rana, 2018). In addition, section 69 allowed the authorities to monitor and decrypt information through the computer resources. Furthermore, laws were developed to protect children from porn and other harmful materials. People transmitting absence or abusive materials online or in electronic form are subject to punishment as per the Indian legal system. In addition, the Indian Computer Emergency Response Team was created as an agency to respond to the computer security issue as per the definitions in the Information Technology Amendment Act 2008 (Rana, 2018).

Comparatively, cyber police were the strongest amongst all the agencies in tackling malicious online activities (Efthymiopoulos, 2016). The control went above beyond the imagination of people from the outside world. Users should only go online and do what is right or else be tracked down by the police. Those found guilty would be blacklisted, secretly detained and investigated or even publicly arrested. Those who violated the laws and regulations would face punishment of different severities depending on the crime committed. However, the actual controllability of online misconducts have been weak, this is due to outdated computer protection equipment imported in the 1980s and 1990, and the related slow development of computer protection products.

The major means for the control of cybercrimes was a blockage. This was to create a 'internet' exclusively with the Indian internet. This once seemed impossible, but later it materialized, this included limiting access to banning certain contents. The most effective way to control online activities was through control over access to the network. In the 1990s and early 2000, cyber cafes were a very popular business in India, which was facilitated with the then newest generations of computers and fastest network connections (Li, 2015). This could become the centre of law enforcement as online conducts and messages could be tracked here. As a method of blockage, close down of cyber cafes was an idea which was greatly welcomed by the police officers, which in other terms could

benefit them by ways of transferring equipment under their control or by taking bribes from owners of the businesses (Jaishankar, 2018).

Surveillance by the governments can be an important measure of deterring the cybercrime levels in the society. Additionally, society can be educated on the measures of crime prevention and mitigation. The International Conference on Cyber and Computer Forensics is enforcing international relations aimed at fighting the cybercrimes; however, the success of such measures depends on the willingness of the various nations to enforce policies that deter the crime. For example, the Indian Information Technology Act deals with the acts where the computer is used as a tool for a criminal offense (Sarre, Lau, & Chang, 2018).

Internet was introduced sometimes back, and it presents with various advantages to the users. The increasing advantages of the internet make it pleasing to many people. As a result, the number of people using the internet on a daily basis continues to arise. The increase is also attributed to the social sites where people can interact in a virtual environment and communicate with one another (Farrell, & Birks, 2018). The communication role attracts new users each day. Unfortunately, some of the users do not understand the potential threats they are likely to encounter from the internet use. For instance, some people may come across non-useful materials such as pornographic material which is harmful especially to the youths.

Additionally, lack of proper security measures caused by lack of awareness also contributes to the increasing threats resulting from the internet use (Udris, 2016). However, the global integration works to ensure that internet users are safe and can only surf contents they have strategically planned to access. On the other hand, total inhibition of the cyber threats cannot be achieved 100% because the perpetrators use new techniques from day to day. The uniqueness and dynamic nature of the techniques used by the cyber offender limit the application of the international policies (Moore, 2014).

Educating the public on the threats of cybercrime is an important and essential step of reducing the negative effects associated with the experience. The awareness ensures that the users keep their accounts safe by having secure passwords and being cautious with the people they interact with online considering that some of them are unscrupulous and uses the internet to propagate their criminal purposes (Brewer, Cale, Goldsmith, & Holt, 2018). The reason why the internet has become a good harbor for getting criminal victims is that there are many people using internet on a daily basis and some of them are innocent and naïve; they have limited understanding of cyber security. Therefore, educating the public will help sensitize them to be cautious and avoid being caught up by the tricks users by the cybercrime offenders (Jaishankar, 2018).

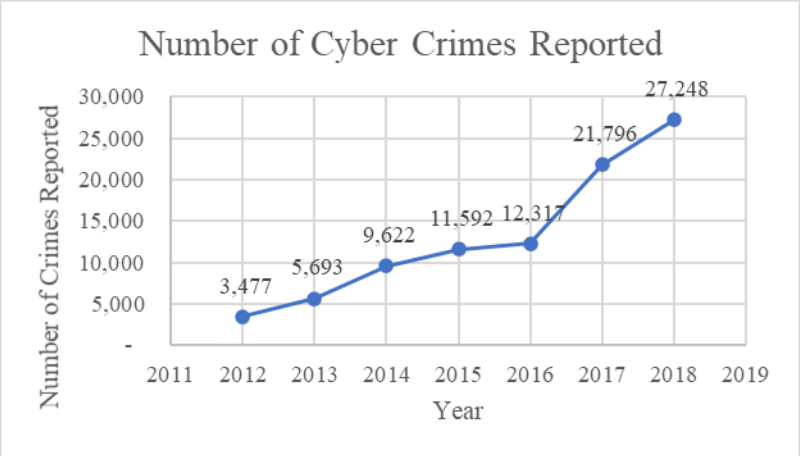
The address of the cybercrime threats can also be explored from the theoretic perspective. Various theories exist that explain why cybercrime exist; therefore, the international bodies associated with cyber criminology can apply the theories in developing reliable and ethical regulation and policy framework that prevents the penetration of the criminal act. For instance, the social learning theory and the routine activities theory among others are the commonly used ones in the explanation of the incidences of cybercrime; however, their applications have not been fully developed (Jaishankar, 2018). Additionally, the space transition theory explains the nature and behaviors of the individual engaging in the cybercrime. According to the space transition, people's behaviors vary from one person to another when they move from one space to another. However, it is important to note that not all people occupying a similar space

behave similarly. There is a need to explore the concept of cyber criminology from the global perspective further to understand its scope of operation for easy development of appropriate measures to curb it (Jaishankar, 2018).

Internet use continues to grow from day to day, and it has become accessible due to its great importance (Brown, 2015). On the other hand, the combination of the increasing usage and the global threat requires that legal responses are developing to address the possible harms likely to be caused in the society (Brown, 2015). There is a need to identify both the criminal and their territorial competences to effectively fight the increasingly global threat. Identification of the internet offense perpetrators is still a major challenge in the current society, and this has made it difficult to fully impose the legal responses to the threat. The anonymity presented by the internet challenges both the police involved in the investigation and the judicial principles of the individual nature of the penalty. There is a need to develop adequate measures to counter cyber threats (Gillespie, 2015).

The cybercrimes go hand in hand with the political goals and demands; as a result, this poses a major challenge in addressing the issue fully. The liberal democracy is based on the fact that people have the freedom to debate their political views and the messages presented on the internet. The greatest challenge emerges when the states are incapable of reaching the agreement of the universal definition of the crime. The cybercrime is a concept that has been discussed widely with some scholars arguing that it should only be limited to the cyber-attack which are done by the terrorists. On the other hand, some scholars contend that it ought to involve all the use of the internet for terrorism only.

India needs to develop robust IT crime prevention systems

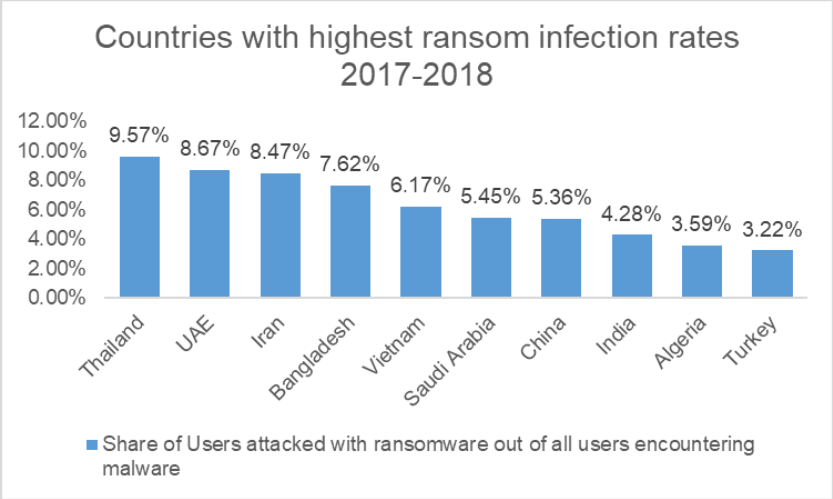


[Source: NCRB (India)]

From 2012 to 2018, there were more than 90,000 cybercrime incidents reported across India. Out of these, over 27 thousand cases were registered in 2018 alone, marking an increase of 121 percent since 2016. Majority of the cases were registered under the IT Act with the motive to defraud, or sexually exploit victims. It was estimated that in 2017, consumers in India collectively lost over 18 billion U.S. dollars due to cybercrimes. However, these estimates are true as far as to the reported cases. In a country like India, it is highly likely that the actual figures could be under-reported due to a lack of cybercrime awareness or the mechanisms to classify them. Recent government measures such as a

dedicated online portal to report cybercrimes could also be the main factor behind a sudden spike in online crimes from 2017 onwards.

The positive side of the analysis is that the recent Government initiatives have brought a collective awareness about cybercrimes. People find trust with the Police and have faith in the systems installed to fight cybercrime. Sensitive areas like that of sexually exploiting, targeting minors and women are being reported in higher numbers year on year. On the other hand, the negative side of the statistics is that cybercrimes might have increased. If we assume to have a correlation between number of crimes reported and number of crimes occurred, it proves that our IT systems of protection need to be strengthened. With the advent of mobile payments, mobile applications and fake websites, data thefts are difficult to control. The pace of strengthening the systems to tackle crimes needs to match with the pace of digital penetration and usage.



[Source: KSN Report]

This statistic shows the countries with highest ransomware infection rates from 2017 to 2018. It can be inferred that developing countries are at greater threat of getting infected with ransomware crimes. Once a malware is encountered, we need to identify, track and attack that malware to eliminate the threat of a crime. However, in India this system is not yet matured enough to prevent such incidents. Due to the IT business boom in countries like India, Thailand, Bangladesh etc. due to BPO and Call centres springing up, digital exposure of its citizens has increased. With more digital penetration and initiatives like Digital India, it is high time that India needs to develop robust IT crime prevention systems. Further, it is important to have AI and other technologies to identify and tackle the malware rather than cyber police dealing with every individual case.

Theories Used in Guiding Global Legal Response to Cybercrime

Hacking, which originally had a positive connotation and was attributed to individuals with exceptional skills for being able to hack or find shortcuts, has been distorted. Social learning theory has been used frequently to analyse hacking. The measurements of hacking included items such as; "tried to guess another password to get into his or her computer files or account", "accessed others' computer account or files without his or her knowledge", and "wrote or used a program that would destroy someone's computerized

data such as a virus, logic bomb or Trojan horse". Both differential association and differential reinforcement/punishment are both significant predictors of the aforementioned hacking behaviors (Brewer, Cale, Goldsmith, & Holt, 2018).

Besides the social learning theory, self-control theory has also been frequently used to study hacking; it is most widely used in criminology. While some hackers argue that being a hacker means having self-control, discipline, and commitment to learning systematically. However, previous studies have shown that there is no connection between self-control and hacking intentions. A group of researchers however strongly suggest that there is a strong connection between self-control and hacking in a significant way (Brewer, Cale, Goldsmith, & Holt, 2018). Apart from these two theories, parent-child relationship and depression enhance s willingness to hack and risk propensity and rationality to hacking behavior. Also, introversion has been associated with hacking and related computer crime activities.

As the spread of technology and internet advances, more issues concerning cyber deviance are expected. Family, school, and neighbourhood play different but significant roles in cyber deviance. According to Yar et al., 2005, hacking culture encourages more males to engage in the activity than females; For instance, his study found hacking to be overwhelming among males (8.29% versus 2.5% females). When it comes to downloading, gender distribution is more even -54.60% of males versus 42.24% of females. The biggest predictor for both was the easy access to computers at home; this suggests that affordability plays an important role. Computers at school get monitored easily and put more constraints on what should be downloaded, furthermore download of illegal staffs can call for punishment or even expulsion from school.

Gender and grade are significant predictors of both downloading and hacking. For downloading, males were 1.46 times more likely perpetrators; however, when it comes to hacking, the difference was much more pronounced; up to 2.85 times more likely than females. Having a positive attitude towards violent behaviours was a significant predictor for downloading and hacking. Positive attitude toward violent behaviour is linked to both physical and verbal violence.

Secondly, Parental attachment plays a significant role in cyber deviance; therefore, some of these social factors must also be considered in ensuring the effectiveness of the measures used to prevent cybercrime. Having a bad relationship with either mother or father have identical negative associations with downloading. In contrast, the odds ratio for getting along with mother was twice the size of the father regarding hacking. Parental control, such as knowing the respondents' friends is significant in knowing their deviant behavior. Furthermore, effective parenting has been shown to foster high levels of self-control which in turn can theoretically reduce the chance of downloading and hacking due to low self-control (Kostakos, 2018). In addition, school bonding is significantly and negatively associated with both downloading and hacking. Several studies have shown that increased attachment to school promotes conforming behaviour, whereas lower school attachments have been associated with bullying, and later initiation to deviant behaviours such as drinking and smoking, delinquency and cyber victimization. School disorganization is also positively associated with downloading and hacking.

Lastly, neighbourhood integration is significantly and negatively associated with downloading. The neighbourhood disorganization relatively showed a less significance to the deviance behaviour. This statement seems awkward, however, if a neighbourhood is described as well- off or organized, which should be the antithesis of social disorganization

for instance, neighbourhoods that have been associated with community problems in general, poverty and deviant behaviour. This is possible that affordability and socioeconomic status are the factors to be considered. Middle-class children access the internet more often thus the prevalence connection between more frequent downloading, better neighbourhoods and neighbourhood attachments.

Government institutions all over the world are aware of the need to take legal actions and limit the progress of cybercrime; for example, President Barrack Obama declared the digital infrastructures in America as a national asset and developed the Cybercom, a unit that would regulate all the internet activities in the region. On the other hand, other nations still lack the capabilities impose appropriate security measures to eliminate cyber threats. For example, the United Kingdom government leaders are not adequately preparations to foster security against cybercrimes and attacks. As a result, they announced the development and investment into measures and policies that would promote the defense of the National Cyber Security. Furthermore, the NATO has been raising awareness on the need to develop international laws applicable to the cyber warfare globally. As a result, it presents that cybercrime affects nearly all nations in the world and it is an issue in the global domain that must be addressed in time.

Various theories have been published to address the cybercrime at the global level; popular cybercrimes indicates that a lot of things are conducted differently by various people. Therefore, the theoretical framework to the analysis and regulation of the threat is embedded in the legal-political measures, innovation and the monetary talks among others. The legal-political framework requires that international bodies investigate and develop standards that should apply to all nations globally.

Integrated Responses and International Conventions

The core mechanism concerning the responsibility and control over online services was the liability of both macroscopic and microscopic approach both in both central and local government. If officials were regarded as negligent when malicious conduct happen, they could equally face criminal or administrative punishments. The purpose of this regulation was to enhance state stability (Li, 2015). This is because many people than ever had started using the information networks to propagate their anti-revolutionary, liberalist, and separatist ideas made more complains and expressed more discontentment. Unlike China, other countries have exposed free information that is useful to commerce and technology, China's regulation on the internet was designed to eliminate harmful information while conserving useful information. While people from other countries worried that this regulation would have a negative impact on the protection of human rights and the development of the economy, which is just contrary to the internet spirit (Li, 2015).

Cybercrimes are mostly missed in the criminal justice area, and this oversight indicates the difficulties encountered in the criminal equity realization. The under-detailing of the cybercrimes is a major issue in fighting cybercrimes at the global level. Fighting cybercrime can be described as the war that operates within the air as the media (Lee, & Sanchez, 2018). Therefore, the war against the cybercrime requires a full understanding of the domain shape and exploring the principles of kinetic warfare (Hamin, & Rosli, 2018). The fight against cybercrime is based on eight principles which include the dual use, the information as the environment of operation, control of infrastructure, kinetic effects, and lack of physical limitation, stealth, inconsistency, and mutability (Udris, 2016).

The convention of cybercrime is the only binding multilateral treaty that has been used in combating the cybercrime. The convention was drafted in 2001, and it provides a good framework on the cooperation between the various parties, and it was open for ratification for the nations that are not members of the Council of Europe. This is an example of a substantive multilateral agreement that was mainly objectively developed to address the cybercrime threat (Lee, & Sanchez, 2018).

The convention attempts to cover the crimes of illegal access and criminal associated with the wrong use of the internet. Also, offense perpetrates by the use of computer systems such as the computer-related frauds the provision addresses transmission of immoral materials such as pornographic. As a result, the convention completely addresses some of the issues that were being left out by the scholars initially (Kostakos, 2018). The convention has a binding framework that addresses computer-related offenses, offenses against confidentiality such as infringing into the accounts of the companies or even national system to steal information and then criminal copyright infringement. According to article 23 of the convention, the arrangement on the legal framework is based on the development of standardized systems to promote integration among the global countries. As a result, the nations are expected to get into bilateral treaties (Gercke, 2012).

The Convention on Cybercrime of the Council of Europe remains one of the relevant international legal system governing the cybercrime and electronic evidence. Also, the level of cooperation among the members continues to increase as the treaty evolves to accommodate the new and emerging tactics used in the cybercrime field (The Budapest Convention on Cybercrime: a framework for capacity building, 2016). The conventional operation and formula of success are based on the dynamic triangle. Its operation is guided by the need for strengthening the security and confidence in the IT sector and reinforcing the rules and laws protecting the human right from cybercrime (Keyser, 2017). The convention provides the common standards to be undertaken when investigating cybercrime and the international police and judicial cooperation. Also, the criminalization of the cybercrime victims is based on the treaty. Also, the convention leads to the formation of other international bodies such as the Global Cyber Space Conference which protects nations from Europe, America and some of the African nations.

The international integration is important in ensuring a successful fight against cybercrime threats globally. The development of the international standard as evident in the NATO conference is key in ensuring that all nations read from the same page when it comes to addressing computer-related crimes. Considering that cybercrime occurs in a virtual environment with no physical boundary, the national regulatory measures may not be successful since people can still perpetuate the crime from any part of the world. Developing the global legal framework is key and important in the realization of safe internet use (Miquelon-Weismann, 2017). As the use of internet continues, so do the need to develop international legal frameworks emerge. Technology presents a lot of advantages to the users, and this means that people cannot be banned from using the internet; however, policies must be developed to control the content posted on the sites as well as internet activities that may have harmful effects to the online users. However, as nations develop the integrated cybersecurity measures, it is important that guidelines are developed to handle the hearing and prosecution of the cybercriminals. For example, in case a person commits the crime in a nation by operating from a different nation, where will that person be prosecuted? The integration will make it easy for the offenders to be caught and legal actions were taken against them; however, there are some aspects in the

global legal framework dealing with cybercrime that must be addressed. Cyberstalking is mainly caused by the victims; therefore, it is also within the responsibility of each internet user to ensure that they uphold appropriate security measures. The implementation of the measures developed by the international bodies can only be a success if internet users are willing to adhere by them.

Furthermore, tight legal and regulatory frameworks have been gradually introduced through the cyber police who are mandated with surveillance and monitoring of the activities undertaken by the internet users. Therefore, even as the issue of the legal framework in addressing cybercrime from the global perspective gets a significant concern, it is important to explore the future of cybercrimes considering that technological advancements continue to occur. The intensity of cybercrimes increases with technological developments.

According to Mittal and Sharma (2017), the transnational aspect of the cybercrime came along with various issues of sovereignty and jurisdictions which must be addressed for effective cooperation. As a result, there is a need for the transnational conventions to unite all the nations and enhance the cohesion among the nations as they fight against cybercrime. For example, the Council of Europe Convention on Cybercrime is the only effective international body dealing with cybercrime, the body alone cannot be able to eradicate the crime; as a result, there is need to form other conventions to support the agenda of the Council of Europe Convention on Cybercrime. Also, the non-member states of the international bodies should join to echo a common voice against cybercrime.

In as much as various measures have been developed to address the increasing incidences of cybercrime at the global level, the enactment of the global legal measures still receives various challenges. Some of the challenges include definition of the cybercrime and the acts defining the crime. In addition, the boundaries between cybercrime and the traditional crimes continue to increase. The development of international conventions was meant to help address the cybercrime incidences; the international integration in cyber criminology presents a good solution in the future considering that they are dynamic and changes with time to address comprehensively the changing nature of cybercrime.

References

Brewer, R., Cale, J., Goldsmith, A., & Holt, T. (2018). Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents. *International Journal of Cyber Criminology*, *12*(1).

Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.

Efthymiopoulos, M. P. (2016). Cyber-security in smart cities: the case of Dubai. *Journal of Innovation and Entrepreneurship*, *5*(1), 11.

Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop?. *Crime Science*, *7*(1), 8.

Gercke, M. (2012). *Understanding Cybercrimes: Phenomena, Challenges, and Legal Response*. International Telecommunication Union.

Gillespie, A. A. (2015). *Cybercrime: key issues and debates*. Routledge.

Hamin, Z., & Rosli, W. R. W. (2018). Cloaked By Cyber Space: A Legal Response to the Risks of Cyber Stalking in Malaysia. *International Journal of Cyber Criminology*, *12*(1).

Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution, and Impact1. *International Journal of Cyber Criminology*, *12*(1).

Jigar S. (2016). A Study of Awareness About Cyber Laws for Indian Youth. *International Journal of Trend in Scientific Research and Development (ijtsrd)*, 2456-6470, 1-1.

Kerstens, J., & Veenstra, S. (2015). Cyberbullying in the Netherlands: A criminological perspective. *International Journal of Cyber Criminology*, *9*(2), 144.

Keyser, M. (2017). The Council of Europe Convention on Cybercrime. In *Computer Crime* (pp. 131-170). Routledge.

Kostakos, P. (2018). Public Perceptions of Organised Crime, Mafia, and Terrorism: A Big Data Analysis based on Twitter and Google Trends. *International Journal of Cyber Criminology*, *12*(1).

Lee, G., & Sanchez, M. (2018). Cyber Bullying Behaviors, Anonymity, and General Strain Theory: A Study of Undergraduate Students at a South Eastern University in the United States. *International Journal of Cyber Criminology*, *12*(1).

Li, X. (2015). Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology*, *9*(2).

Media.kasperskycontenthub.com. 2020. Ransomware And Malicious Cryptominers 2016-2018. (p.10) [online] Available at: <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf> [Accessed 3 May 2020].

Miquelon-Weismann, M. F. (2017). The convention on cybercrime: a harmonized implementation of international penal law: what prospects for procedural due process?. In *Computer Crime* (pp. 171-204). Routledge.

Mittal, S., & Sharma, P. (2017). A Review of International Legal Framework to Combat Cybercrime.

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Ncrb.gov.in. 2020. Crime In India 2018 - Volume 2. (p. 751) [online] Available at: <https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%202.pdf> [Accessed 3 May 2020].

Patney, V. (2017). *Asian defense review 2016*. New Delhi: KW Publishers Pvt Ltd in association with Centre for Air Power Studies.

Rana, R. (2018). Cybercrime in India: A study of legal response with special reference to Information Technology Act, 2000. *Global Journal for Research Analysis*, *6*(5).

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends.

The Budapest Convention on Cybercrime: a framework for capacity building. (2016, December 7). Retrieved from https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime

Udris, R. (2016). Cyber Deviance among Adolescents and the Role of Family, School, and Neighbourhood: A Cross-National Study. *International Journal of Cyber Criminology*, *10*(2).