New York Science Journal

Websites:
http://www.sciencepub.net/newyork
http://www.sciencepub.net

Emails:
newyorksci@gmail.com
editor@sciencepub.net

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

Cyber Crime : A Global Perspective

Kapil Dhundhwal

Pursuing LLM, at Department of Laws, Panjab University, Chandigarh- 160014 (India)
E-mail- kapilsingh376@gmail.com

Abstract: With the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue. It has created an entirely new set of problems for law enforcement agencies all over the world. It has equally become cause of serious concern for the legal fraternity to find effective ways and means to combat cyber criminality because of its worldwide devastating effect. With the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue. It has created an entirely new set of problems for law enforcement agencies all over the world.2 It has equally become cause of serious concern for the legal fraternity to find effective ways and means to combat cyber criminality because of its worldwide devastating effect.
[Dhundhwal, K. **Cyber Crime : A Global Perspective.** *N Y Sci J* 2023;16(4):14-17]. ISSN 1554-0200 (print); ISSN 2375-723X (online). http://www.sciencepub.net/newyork. 04.doi:10.7537/marsnys160423.04.

Keywords: Cyber Crime, Global Prospective, India

Introduction

Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act. Cyber crime is the most prevalent crime playing a devastating role in Modern India. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation it can be said that, Cyber crime includes any illegal activity where computer or internet is either a tool or target or both. The term cyber crime may be judicially interpreted in some judgments passed by courts in India, however it is not defined in any act or statute passed by the Indian Legislature. Cyber crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark sides too.1 Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyberdefamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet.

Cybersecurity constitutes one of the top five risks of most firms, especially in Big Tech and Banking & Financial Services. A weekend reading led to some interesting data points from various sources such as AV-Test and Coveware, among others, and that further led to me pondering over the mitigating actions that we can take as individuals and as organisations for some, if not all, of these cybercrime risks. I extend my thanks to the respective experts who shared their knowledge, enabling me to piece together some parts of the larger jigsaw puzzle.

Worldwide, many countries have enacted their own criminal laws, computer laws, information technology laws or intellectual property laws etc. to respond to the problem of cyber criminality, but keeping in view the international dimensions of these crimes, problems often do arise, particularly where the crime relates to individual citizens of two or more foreign countries. The crucial problem, therefore, is that internet as a global media may be accessed throughout the world and can be viewed in any part of the universe, hence which particular law will be applicable for the disputed transaction, becomes a ticklish question because of the variation in cyber laws of different countries. Under these circumstances, the development of a universal law governing cyberspace transactions would make it much easier to decide about the applicability of law to regulate a particular online activity. It really calls for a coordinated action for all alike including the people, institutions, industries, governments and above all, the states. Since cyber crime have an international ramification,

it has to be tackled through a common legal strategy which has universal acceptance and recognition.

Any sort of crime committed using a computer either as the object of the crime or as a tool to commit the offense is called cybercrime. In 2015 consumers in the UK reported a loss of more than 1.7 billion pounds due to cybercrime. This is way more than other serious crimes like illegal drug trafficking. This sharp increase in crime is due to the growth in e-commerce and online banking. In the last few years alone there have been hundreds of millions of cases of credit card theft; cases of compromise in Social Security Numbers and health care records. Crimes like these are committed by hackers who exploit the vulnerabilities in software which are sometimes caused by naive mistakes made by the people while using the software.

People committing cybercrime cannot be pinned down to a specific class of individuals. They may belong to any race, religion or sex. It could be a teenager from high school who just wants to impress his girlfriend or even a member of a terrorist group. Countries are now not only equipping their regular armies to fight crime but also their cyber army. In fact, the next world war might not be fought with weapons but with computers which could be used to shut down national water supplies, energy grids, and transportation systems.

By Google Security Princess Parisa Tabriz, an attacker can infect someone's computer in two ways. The first way is to deceive the person into installing a program on their computer. Many viruses are often disguised as security updates. The second way is to use the vulnerability in the software already installed in the system. In such a case the attacker doesn't even need permissions to install a virus. Once the virus is installed then the system's data is compromised. The attacker can then steal sensitive data like bank account details etc. He can also remotely monitor and control the computer. He can even create a digital army with millions of computers and plan a full-fledged attack and even take down websites. This kind of attack is called a Distributed Denial of Service attacks (DDoS).

A denial of service is when hackers overwhelm a website with too many requests. Most of the websites are ready to handle a large number of requests. But if the requests are in the order of billions and trillions then the servers will be overloaded and they stop responding. Hackers also send out a large number of spam emails which deceive the user into giving their sensitive information. Information such as passwords to bank accounts can be collected from unsuspecting users by making them logging into their bank accounts. This is called a phishing scam. Hackers then use the newly obtained passwords to steal money from bank accounts.

Cyber-crime: GlobalProspective

In Australia, cybercrime has narrow statutory meaning as used in the Cyber Crime Act 2001, which details offenses against computer data and systems. In the Council of Europe's (CoE) Cyber Crime Treaty, cybercrime is used as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copy-right offenses.

The Spam legislation scenario mentions "none" about India as far as E-mail legislation in India is concerned. The legislation refers to India as a "loose" legislation, although there is a mention in Section 67 of ITA 2000. About 30 countries have enacted some form of anti-spam legislation. There are also technical solutions by ISPs and end-users.

Inspite of this, so far there has been no significant impact on the volume of spam. Spam is used to support fraudulent and criminal activities. As there are no national boundaries to such crimes under cybercrime realm, it requires international cooperation between those who seek to enforce anti-spam laws.

Thus, the global dimension of cyber crime is made it difficult to handle and dealt with. The evolution of internet technology has given us so many advantages to deal with future problems and grow with rapid rate but also it has provided the scope for criminals to commit their crime with least chance of detection. The cyberspace has proved a boon to the deviant behaviour in the society. The concept of cyber crime has gained speed and we are facing great threat of its impact on world society. The human society is become vulnerable to cyber crime due to more and more dependence on technology.

The children especially adolescents are in modern world want to explore everything on information highway. The children in today's generation have access to internet and computer's at home, the internet and computer are part of their studies. The access to computer and internet makes them vulnerable to the potential danger of internet. The children are sometime curious about sexuality and sexual explicit material. The parents don't have too much control over the children and the children are busy exploring the internet and other medium to fulfill their wishes through the on-line access. Sex–offenders exploit these conditions and fulfil the need of children. The child at this tender age doesn't understand and recognise the potential danger of these contacts. The

internet is highly used by the abusers to abuse children sexually worldwide. The children in India become viable victim to the cyber crime, as internet becomes the household item in India. The children are becoming victims to the aggression of pedophiles.

Cyber-crime: How does it impact India

India has the second highest number of Internet users in the world (in 2017). Most of the Internet access happen from cyber cafes. The age group of most of Indian Internet users is between 18 and 35 years. It is reported that compared to the year 2006, cybercrime under the Information Technology (IT) Act recorded a whopping 50% increase in the year 2007. A point to note is that the majority of offenders were under 30 years. The Indian government is doing its best to control cybercrimes. For example, Delhi Police have trained 100 of its officers in handling cybercrime and placed them in its Economic Offences Wing.

India is no exception to the global trends in cyber-crime and expects cyber frauds to continue to rise in 2021. India ranks 11th worldwide in the number of attacks caused by servers that were hosted in the country, with 2.3 million incidents reported in Q1 2020. Cyberattacks reported in 2020 were up nearly three times from 2019 and more than 20 times compared to 2016.

While digital transformation, move to cashless transactions and zero contact communication supported with proliferation in internet and mobile phone usage, cyber risks in India have risen exponentially during the pandemic. According to the annual IBM X-Force Threat Intelligence Index, India reported the second-highest number of cyber-attacks after Japan in the Asia-Pacific region in 2020, accounting for 7 percent of all cyber-attacks observed in Asia in 2020.

The cybersecurity market in India is expected to grow to over $3 billion by 2022, at about 150% of the global rate. A 2019 report by IBM revealed that cyberattacks cost India ₹12.8 crores on an average between July 2018 and April 2019, while the average cost of a data breach globally was 27 crore. Besides these financial losses, cyberattacks can and have caused huge dents in organizational brand value.

45% of adult Indian internet users faced identity threat in 2020, up almost 40% since 2019, at 2.7 crore – over 2 percent of India's entire population.

A German cybersecurity firm, Greenbone Sustainable Resilience, reported that medical records of over 120 million Indian patients (mostly from Maharashtra and Karnataka) were leaked on the Internet. The leaked records included pictures of the patients, X-rays, CT scans and MRIs.

Stuart Solomon, COO of Massachusetts based Recorded Future, had made an interesting claim based on malware tracing. He alleged that a Chinese group called Red Echo, "has been seen to systematically utilize advanced cyber intrusion techniques to quietly gain a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure." The firm claimed that the electricity outage in Mumbai on 13th October 2020, was orchestrated by Red Echo. Whether Red Echo was acting as a state actor or not, the threat is nonetheless real.

The latest one in the country is a fake SMS message, that claims to offer an app to register for Covid-19 vaccination in India. Once the link is clicked, this installs malicious code that gains permissions to the user's data, such as contact lists, and spreads via SMS to the user's contacts.

Paris Cyber Crime Conference (2000)

A 3-day Cyber Crime Conference was held in Paris in May, 2000 which was attended by nearly 300 delegates including judges, police officials, diplomats, legal experts, leading businessman and industrialists from G-8 countries. The conference stressed on the desirability of a global law to tackle the hackers, software pirates, crooks and virus attackers who were making the life of internet users miserable. The members unanimously agreed that there was a need for an international convention to deliberate on cyber crime related issues and urgency of setting up an International Criminal Tribunal having global jurisdiction to deal with cyber crime and criminals. It was further resolved that the nature of cyber crime demands that the concerned countries should actively cooperate and coordinate in the investigation and prosecution of these hi-tech crimes regardless of their territorial boundaries. There should be prompt exchange of evidence in case of cross-country cyber crimes. Therefore, all efforts should be made by the member nations to initiate measures for security of networks on priority basis.

Cybercrime and the Extended Enterprise

It is a continuing problem that the average user is not adequately educated to understand the threats and how to protect oneself. Actually, it is the responsibility of each user to become aware of the threats as well as the opportunities that "connectivity" and "mobility" presents them with. In this context, it is important to understand the concept of "extended enterprise." This term represents the concept that a company is made up not just of its employees, its board members and executives, but also its business partners, its suppliers and even its customers. The

extended enterprise can only be successful if all of the component groups and individuals have the information they need in order to do business effectively. An extended enterprise is a "loosely coupled, self-organizing network" of firms that combine their economic output to provide "provide "products and services" offerings to the market. Firms in the extended enterprise may operate independently, for example, through market mechanisms or cooperatively through agreements and contracts.

Seamless flow of "information" to support instantaneous "decision-making ability" is crucial for the "external enterprise." This becomes possible through the "interconnectedness". Due to the interconnected features of information and communication technologies security overall can only be fully promoted when the users have full awareness of the existing threats and dangers. Governments, businesses and the international community must, therefore, proactively help users' access information on how to protect themselves.

CONCLUSION

An overview of the international perspective of law on cyber crime suggests that despite internet and cyberspace laws having been enacted by several countries, many complicated legal issues that have emerged in cyberspace (which know no boundaries and physical environment), still remained unresolved in the existing legal regime. In the context of India, though the Information Technology Act, 2000 has been introduced as a comprehensive legislation to prevent and control cyber crimes, yet it is only a gap-filler and has no applicability in many situations. The legal position as regards electronic transactions and civil liability for the acts executed in cyberspace still remain hazy in the absence of an adequate global law on this crucial issue. The impact of internet and gravity of the problem of cyber crime in the context of the existing global regime can be well appreciated by the fact that US Congress had to introduce more than 50 Bills pertaining to internet and e-commerce in the first 3 months of 1999 alone. The issues which need to be addressed urgently at the international level are security of transactions, privacy protection of children against pornography, validity of contracts, uniformity in procedural rules of evidence, certainty of jurisdictional issues and a host of other related problems. It is well known that cyber cries include a variety of criminal activities which are done in the cyberspace. A cyber criminal may destroy websites and portals by hacking or planting viruses, carry out frauds by illegally transferring funds, gain unauthorized access to highly confidential and sensitive information by breaching security, intrude in personal privacy, cause e-mail threats or harassment and indulge in cyber pornography and commit many other similar activities. In fact, the whole world has become a operational canvas for cyber criminals to commit innumerable other crimes on the internet. Though most countries have introduced anti-cyber crime legislation to tackle the problem domestically at the national level but there is a need for global control mechanism to combat these crimes. Therefore, the countries should rise above their regional conflicts and stand together to give a tough fight against the menace of cyber crimes in a spirit of mutual understanding and cooperation.

References:

[1]. Abraham D. Sofaer, Seymour E, .The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press, 2001.

[2]. David Engel, Internet Service Provider on the Hooke, Communication Law Review, Vol. 4, (1999), p. 140.

[3]. Gaur, K.D., Text book on Indian Penal Code, Fifth edition, 2014, Universal Law Publishing Company Pvt. Limited, New Delhi

[4]. Jim Puzzanghera, 'U.S. Law Makers Clamoring to Regulate Internet", San Jose Mercury News, April 9, 1999

[5]. Stambaugh, H., et. al, Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Report, Washington, Dc: U.S. Department of Justice, March 2001.Available at : https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf (Accessed at 04th February, 2016)

4/12/2023