VOL 4 ISSUE 3
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

CYBER CRIMES IN INDIA: A CRITICAL ANALYSIS

- Sanjivani Biswas, Anshudeep Maitra &Rahul Takuli[1]

ABSTARCT

Computers and the Internet since their origin has continued to pervade the life of humans in everything. Being one of the most rapidly expanding sectors, internet has become one of the most vital part of our life from work to entertainment but it comes with a price of our privacy. Individuals or groups uses Cyberspace to not only disrupt the privacy of an individual but also to threaten International governments, or terrorize the citizens of a country.

The information technology is a double-edged sword, which can be used for destructive as well as constructive work. Thus, the fate of many ventures depends upon the benign or vice intentions, as the case may be, of the person dealing with and using the technology. For instance, a malicious intention forwarded in the form of hacking, data theft, virus attack, cracking, phishing, child pornography etc. can bring only destructive results, which also falls into the category of cybercrime.

"Cybercrime encompasses criminal acts that involve computers and networks. Thus, Cybercrime is a broad term that describes everything from electronic hacking to denial-of-service attacks that causes e-business websites to lose money, from leaking of private and confidential data to corrupting the network or systems, from misfunctioning of technological machineries to abuse of data usage."

In this paper we will analyse the possible threats and strength of the people who try to spoil the cyber ecosystem through various cyber-crimes and what are the preventive measures as per the Information Technology Act, 2000 and other available provisions as per the law, which can be taken to protect from cyber-attacks or cyber-crime.

Keywords: - Cybercrime, Hacking, Cracking, Phishing, Virus Attack, Child Pornography, Information Technology Act, 2000

[1] Students, Siddhartha Law College, Dehradun

Introduction

"The chief problem is any community cursed with a crime, is not the punishment of the criminals, but the preventing of the young from being trained to crime." – W. E. B. Du Bois

Cyberspace

The virtual space created for a network of information from person to person in mass media through the internet. This platform of exchange of information and data is called cyberspace.

Cybercrime

The activities are done with intent to harm a person, his property, or any organization in whole through the internet; it is called cybercrime.

Cyber Laws

The legislative issues made out to keep cyberspace in a check of legal boundaries of the constitution of that state. And the laws also help define the structure of the network to be established within a territory; closed, open, or partly both.

How Cybercrime Works?[2]

- Cybercrime attacks can begin wherever there are digital data, opportunity, and motive.
- Cybercriminals include everyone from the lone user engaged in cyberbullying to state-sponsored actors, like China's intelligence services.
- Cybercriminals use various attack vectors to carry out their cyberattacks and are constantly seeking new methods and techniques for achieving their goals while avoiding detection and arrest.
- Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime.
- Phishing emails are another important component to many types of cybercrime but especially so for targeted attacks, like business email compromise (BEC),

[2] https://searchsecurity.techtarget.com/definition/cybercrime

in which the attacker attempts to impersonate, via email, a business owner in order to convince employees to pay out bogus invoices.

Effects of Cybercrime

A primary effect of cyber-crime is financial; cyber-crime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cyber-criminals may also target an individual's private information, as well as corporate data for theft and resale.

Due to which the security of a person's identity, money, or valuable private information of any person or organization is at stake of risk, towards which remedy is provided by a law governing such circumstances in specific; i.e. cyber laws.

Effects of Cybercrime on National Defence[3]

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.[4]

[3] https://searchsecurity.techtarget.com/definition/cybercrime
[4] https://en.wikipedia.org/wiki/Cybercrime ...Legislation

Cybercrimes may have public health and national security implications, making computer crime one of DOJ's top priorities. In the United States, at the federal level, the Federal Bureau of Investigation's (FBI) Cyber Division is the agency within DOJ that is charged with combating cybercrime. The Department of Homeland Security (DHS) sees strengthening the security and resilience of cyberspace as an important homeland security mission, and agencies such as the U.S. Secret Service (USSS) and U.S. Immigration and Customs Enforcement (ICE) have special divisions dedicated to combating cybercrime.

USSS' Electronic Crimes Task Force (ECTF) investigates cases that involve electronic crimes, particularly attacks on the nation's financial and critical infrastructures. USSS also runs the National Computer Forensics Institute (NCFI), which provides state and local law enforcement, judges and prosecutors with training in computer forensics. The Internet Crime Complaint Center (IC3), a partnership among the FBI, the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA), accepts online complaints from victims of internet crimes or interested third parties.[5]

Effects of Cybercrime on Businesses[6]

The true cost of cybercrime is difficult to assess accurately. In 2018, McAfee released a report on the economic impact of cybercrime that estimated the likely annual cost to the global economy was nearly $600 billion, up from $45 billion in 2014.

While the financial losses due to cybercrime can be significant, businesses can also suffer other disastrous consequences as a result of criminal cyberattacks, including the following:

- Damage to investor perception after a security breach can cause a drop in the value of a company.
- In addition to potential share price drops, businesses may also face increased costs for borrowing and greater difficulty in raising more capital as a result of a

[5] https://searchsecurity.techtarget.com/definition/cybercrime
[6] https://searchsecurity.techtarget.com/definition/cybercrime

cyberattack.

- Loss of sensitive customer data can result in fines and penalties for companies that have failed to protect their customers' data. Businesses may also be sued over the data breach.

- Damaged brand identity and loss of reputation after a cyberattack undermine customers' trust in a company and that company's ability to keep their financial data safe. Following a cyberattack, firms not only lose current customers, but they also lose the ability to gain new customers.

- Businesses may also incur direct costs from a criminal cyberattack, including increased insurance premium costs and the cost of hiring cybersecurity companies to do incident response and remediation, as well as public relations (PR) and other services related to an attack.

Cyber Laws in Different Countries

- Former-President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way.
- The European Union adopted directive 2013/40/EU. All offences of the directive, and other definitions and procedural institutions are also in the Council of Europe's Convention on Cybercrime.

- It is not only the US and the European Union who are introducing new measures against cybercrime. ON 31 May 2017 China announced that its new cybersecurity law takes effect on this date.[7]

- The U.S. Department of Justice (DOJ) divides cybercrime into three categories:

1. crimes in which the computing device is the target -- for example, to gain

[7] https://en.wikipedia.org/wiki/Cybercrime ...Legislation

network access;

2. crimes in which the computer is used as a weapon -- for example, to launch a denial-of-service (DoS) attack; and
3. crimes in which the computer is used as an accessory to a crime -- for example, using a computer to store illegally obtained data.

Various U.S. government agencies have been established to deal specifically with the monitoring and management of cybercrime attacks. The FBI's Cyber Division is the lead federal agency for dealing with attacks by cybercriminals, terrorists or overseas adversaries. Within DHS is the Cybersecurity and Infrastructure Security Agency (CISA). This group coordinates between private sector and government organizations to protect critical infrastructure.

The Council of Europe Convention on Cybercrime, to which the United States is a signatory, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements.

- Massachusetts law cites that online harassment is a crime that is punishable with a fine of up to $1,000, a maximum of two-and-a-half years in jail or both. In Tennessee, online harassment and stalking is considered a Class A mis - demeanor, and a convicted cybercriminal can face a jail sentence of, at most, 11 months and 29 days, a fine of up to $2,500 or both.[8]

Need of Cyber Law

In today's era where technology plays vital role, the world is becoming digitally advance and so are the crime related to it. Initially, internet was developed for information sharing for research, but was unregulated manner. As time passed, internet and its uses became more conventional and transactional with e-commerce, social-networking, entertainment platforms, etc.

[8] https://searchsecurity.techtarget.com/definition/cybercrime

Cyber laws govern legal issue related to internet crime. As the use of internet is increasing, the need for cyber laws is also increasing; and their application has also gathered great momentum.

Technology, never a disputed issue but at what cost, and for whom, there has been the ambit of governance, with very undefined and weak applicable laws.

The law of real world cannot be interpreted in the light of emerging cyberspace to include all aspects relating to different activities in cyberspace. Internet requires an enabling and supportive legal infrastructure in tune with the times.

Proposal Of A Concept Of The Law In India

The Information Technology Act, 2000 is the primary law in India dealing with cybercrime and electronic commerce. It is based on the UNCITRAL Model Law on International Commercial Arbitration recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

The applicability of cyberspace and internet may have been a constant. But the increase in users may increase the chance of the misuse of its application as well.

In recent days, a bill was introduced to the parliament, named as Personal Data Protection Bill.

The Personal Data Protection Bill 2019 was tabled in the Indian Parliament by the Minister of Electronic and Information Technology on 11 December 2019. As of 17th December 2019, the Bill is being analyzed by a Joint Parliamentary Committee (JPC) in consultation with various groups.

The Bill covers mechanism for protection of personal data and proposes the setting up of a Data Protection Authority of India for the same. Some key provisions the 2019 Bill did not such as that the central government can exempt any government agency from the Bill and the Right to Be Forgotten has been included.

Forbes India reports that "there are concerns that the Bill… gives the government blanket powers to access citizen's data."In July 2017, the Ministry of Electronics and Information Technology set up a committee to study issues related to data protection.

The committee was chaired by retired Supreme Court judge Justice B. N. Srikrishna. The committee submitted the draft Personal Data Protection Bill, 2018 in July, 2018. After further deliberations the bill was approved by the cabinet ministry of India on 4 December 2019 as the Personal Data Protection Bill 2019 and tabled in Lok Sabha on 11 December 2019.

The Bill aims to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the fundamental rights of individuals whose personal data are processed to create a framework for organizational and technical measures in processing personal data, remedies for unauthorized and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected there with or incidental thereto.

The revised 2019 Bill was criticized by Justice B. N. Srikrishna, the drafter of the original Bill, as having the ability to turn India into an "Orwellian State". In an interview with Economic Times, Srikrishna said that, "The government can at any time access private data or government agency data on grounds of sovereignty or public order. This has dangerous implications". This view is shared by a think tank in their comment number 3.

The original intention towards the research over this scenario was to protect the privacy in order to protect the fundamental right in such circumstances, bypassed as information is so broadly available over the cyberspace; as internet generation gets uplifted with 4G market boom in India, through smartphones.

This idea of controlling the protection of every individual's personal data in relation with the term of controlling flow of such data is a blanket over the original concept of protection.

Conclusion

India has stepped into the generation of internet where there is access to the service of global information; and each entry on the web network is stored for future access and getting access towards the service provided by each platform provide, as specific

websites and there concept of service providence in their business market establishment.

In short terms, 'India is in the market of information, also known as internet'. And for every single piece of information, there is a buyer in the global market, you just need the proper connection with that buyer. The government office controlling the market helps reduce the risk externally possible. But, this information when in control of the government office also has a chance of setting up another internal market of such information, and here the information is not for economic transaction, but power of the government office to discharge information at office holder's will and interest; which in turn becomes an invincible power of information. Not blaming the corruption, which is a human nature, and towards that solution is yet not researched. This power of information can induce a person in charge of such power to misuse it. So, we agree with retired judge of Supreme Court Justice B. N. Srikrishna about the revised version of Personal Data Protection Bill, so introduced in the parliament by Mr. Ravi Shankar Prasad, on 11th December 2019.

And, the cyber laws must be more defined and profound, to establish the proper setting of individual's privacy over this network of information; but not at the cost of streamlining the flow and providing disputed powers to the office head. In a slow democracy, with terrorism and religious outburst on present going out over CAA/NRC; we get that even wrong flow of information can cause destructive measures, and to maintain balance and not chaos in mass public, this bill must be revised and presented.