International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 10; Issue 05 (D); May 2021; Page No.24509-24518
DOI: http://dx.doi.org/10.24327/ijcar.2021.24518.4863

Research Article

DEVELOPING HYBRID MODEL OF LAWS FOR CYBERCRIME & CYBER SECURITY IN INDIA THROUGH CROSS COUNTRIES STUDY

Ananta Aggarwal[1] and Kajal Mittal[2]

[1]Amity Law School, Amity University, Noida, UP
[2]Maharaja Agrasen Institute of Management Studies, GGSIPU, Delhi

A R T I C L E I N F O

Article History:
Received 10th February, 2021
Received in revised form 2nd March, 2021
Accepted 26th April, 2021
Published online 28th May, 2021

Key words:

Cybercrime, cyber security, Information technology Act, computer – oriented crime

A B S T R A C T

This paper is an in – depth study of various modes of Cybercrimes in the world and the cross- country models of Cybercrime and Cyber security. This paper also gives a study about Information Technology Act, 2000 which is drafted to state the legislations about cybercrime and its punishments. Information technology Act, does not define 'cybercrime' directly. Cyber crime means an illegal activity carried out or be blame to the use of computer and gubbins or necessaries indulged with them as data, documentation, software, and sites together as task – oriented or operational tool which further call forth for cyber-crime, hacking or dissent services and prohibition for use of services.

Cyber security is way to safeguard the social media users and other networking sites form cybercrimes. According to Information Technology Act, 2000 "cyber security" means safeguarding information, digital devices, computer resource, communication devices and information stored therein from unguarded and uncertified examine, serve, declaration, destruction, tempering or disordering.

There is a gap and need of improvisation in cyber laws stated in "Information Technology Act, 2000" as there is need to cover all modes of cybercrimes as to safeguard the privacy, personal data, confidential information and users of computer from cybercrimes. A hybrid model for cybercrimes and cyber security along with legislations is to stop cybercrimes is formulated as to fill the gap. It is an approach as to draft a model to improvise the "Information Technology Act, 2000' as to shield the safety and security of users of computer, networking sites and other digital devices from computer – oriented crimes.

INTRODUCTION

As the advancement of technology and IT sector, the world is now totally dependent on technology, and has become a slave of it. Internet has gifted us an ultra – modern and imaginative world which we called as virtual – world or cyber- space. As everything in this world is two faced like - wise this cyber world also has two faces as its pros and cons.

In today's world everything is open and disclosed on news channels and social media. Social media domain is connected to economic, cultural and social aspects of our life. Merits of internet and cyber world are we can make our own virtual games or movies, can invent various gadgets like robots which can help us in our daily routine work; we can do bookings of tickets or do bank transaction by just one click.

Corresponding author:* **Ananta Aggarwal
Amity Law School, Amity University, Noida, UP

As things are two faced so these are some demerits or limitations of cyber world – we can lose our data, confidential secrets, or some formulas which are secretively protected; we have also suffered financial loss as by uploading our bank details.

One of major issue or stumbling block in the virtual world is cyber-crime. The word cyber – crime is profound by Sussman and Heuston in 1995. So, in layman language cybercrime is a troupe or series of illegal acts which are construed from a digital device, information system or tool. We can also say that the cybercrime is a non – profitable crime as to disclose the secrecy and confidential data of a person or a company or organization by hacking its computer system or any other unlawful or mud – slinging way as to cause financial loss to individual or company.

By this we can articulate or bring forward two overhanging spheres or elements of computer crimes or digital crimes that are –

- First sphere, related to illegal activities carried out or be blame to the use of computer and gubbins or necessaries indulged with them as data, documentation, software's, sites together as task – oriented or operational tool which further call forth for cyber- crime, hacking or dissent services and prohibition for use of services.
- Second sphere, relate to protection of data, and information which is used by unsanctioned and illicit ways which encompass property law, company laws, privacy laws and intellectual property laws.

By fetching and cumulating spheres, domains and elements we formalized an explanatory definition of cyber – crime i.e., "An economic or non – economic crime committed or perpetrated using computers and internet services. It includes distributing viruses, illegal downloading files, phishing and phrasing and stealing personal information like data or confidential secrets. A crime can be demarcated or designated as a cyber – crime if the central and dominator players are computer and internet." Cybercrime will further lead to cyber – threat and cyber – attacks. Cyber – threat is a risk or danger to hardware and software system of a computer system. The cyber – threat is a prior ultimatum or warning given to companies or individual digital device which later on stimulate to cyber – attack. As cyber – attack is more daredevil and unpredictable than a normal robbery or fraud. There are no boundaries or limitation in cyber – crime. These are some overlapping objectives or cognition of cyber – attackers –

- Economic Crime – Attacker is well systematic and pigeonhole in his work. It is an extraordinary funded to serve and do hacking in system and include IT sector tools to create an unguarded way to commit fraud.
- Espionage – In today's, world of telecommunication most important information related to intellectual property and includes documents and property. These attackers do not even come to notice as their work is related to IPR sector that is highly confidential and secretive, which in turn made them actual formulator of product.
- Terrorism – These types of attackers are properly trained and their target is set to private sector of a country. As it includes confidential data of nation's security and economic system of a country which constituted the groundwork and structure of a nation.

Cyber – crime is a mechanism which causes global and nationwide threat and a high – risk warning to the social, economic and security system of a country. Today there is rapid increase of cybercrimes which still do not have complete securitize and shield legislative measures to cut the mustard out of the cyber – crimes.

In this paper we are doing exploration and research work on various domains or arenas of cyber – crimes along with its legislative and preventive measures as to work out and terminate cyber – crimes from cyber – world

Origin and Evolution of Cybercrime

As we get the invention of internet and technology, and as everything is two – faced, the internet has its pros and cons. The cybercrime came as a bad and stubborn son of internet. The first cybercrime was documented and evident in France in 1820 by a textile manufacture.

This is a detailed overview at how both cybercrimes and cyber security have advanced over the years, and the milestones that have defined their progression.

1960s: Password protection

At that time there was no network or internet, so people are only concerned about the physical course of action as to intercept access of password and understanding of how computer work. To protect the computer the passwords are created as multi – layered by various safety programs which were installed in the device. Fire Safety Measures were also enforced to certify that the stored data was shielded.

1970s: From CREEPER to REAPER to PHREAKERS

Cyber security tracks its antiquity from 1970s as a researcher Bob Thomas blueprint or draft a computer program, which was able to move ARPANET's network. He named the program '*CREEPER*' as this message was public: "I'M THE CREEPER: CATCH ME IF YOU CAN'. Later on, Ray Tomlinson enhanced Creeper and developed *REAPER* which is self – reproducing and is the first antivirus software.

In 1970, hacking become apparent when a malicious association, hacked telephone system which was their main goal. By technology sharpness individuals does this malicious act known as *"PHREAKERS",* which originate right codes and tones that help in long – distance conversations. The hackers operate and employ their resourcefulness to reshape the hardware and software to abscond the long – distance telephonic conversations.

1980s: The internet goes mad

At this time computer systems and internet was utilised all over the world at a large scale as it connects public at large. Major drastic step came up in 1988, as Morris Worm initiated in New York, institute against security of networking sites. Robert Morris was first one to be charged under Computer Fraud and Misuse Act of New York and Computer Emergency Response Team (CERT) was established as to stop cyber issue.

1990s: The rise of firewalls

As internet was used by public or society, public slowly and gradually started uploading its personal information and documents online. It was difficult to protect the data. So, the NASA researcher who invented firewall program, frame a computer virus attack with assistance of his team. The team of researcher constructed a virtual 'firewall' which is shaped on physical infrastructure to escape actual fire in buildings.

Historical genesis and evolution of cybercrime in India was track recorded as computer – oriented crime in Yahoo v. Akash Arora (1992), decided by the Delhi High Court. It was observed in the court that the first case of 'cyber-squatting' in the country, the Court held that domain names serve the same function as a trademark and are thus, entitled to equal protection under the trademark law. In this case the court also introduced the first polymorphic virus which was further disclosed and reported.

2000s: Proper punishment

As modernised was introduced and developments were taking place in science and technology field, the government try to slope down computer – oriented crimes by giving punishments against offences.

Indian government also took steps to reduce and to stop cybercrimes in India. For that purpose, India drafted 'Information Technology Act, 2000'. The act which lay down legislation, rules and regulations to deal with cybercrimes or computer – oriented crimes and to promote cyber security. This act provides legal remembrance for transactions carried out by mode of electronic devices, electronic data, computer system and other electronic or internet connected spheres.

2010s: Era of Major Breaches

Due to rapid development in IT sector, cybercrime increased and numbers of data breaches were elucidated in this era.

In 2015, India along with China, Russia and other members signed G20. Group of twenty is an international forum for the governments and central bank governors from 19 countries and the European Union. By signing this India undertake the norms at odds with conducting or assisting the cyber – enabled theft of Intellectual Property.

India is still trying her level best to take the edge off of cybercrimes by spreading awareness about preventive tips and cyber security as to safeguard privacy, personal information, dignity and nation from cybercrimes.

Various Modes of Cyber-Crime across World

Social Engineering and Phishing

a. Cyber-criminal ensures that to target or dig out those people who easily post their personal information on social media. In this type of cyber – crime criminals attack those users who have actually do not think and have a simple psychological and intellectual thought process as they can be easily be fool or get manipulate and can exploit them. The process is that they send messages from their friend's ID for urgent financial help and user does transaction in minutes being a foolish and stupid. This led to fraud and wrongful gain.
b. It is criminal offence using social engineering and technical subterfuge to break – in consumer's personal identity details and financial credentials.

Credit Card Fraud

It is an identity theft fraud where illicit or wildcat people uses credit card information of an individual and do purchases and withdraw cash from card. This is done by tracing or by unguarded and forbidden ways for acquiring confidential information from different sites.

Cyber – Crimes against women

a. Cyber Stalking

- It is done through social networking sites. Stalking further cause's mental and emotional torture to the person.
- Cyber Stalking is a heinous crime, which is to keep a close track on each step pf user and try to get intimidate by sending her sexual content and try to make out with her. This can only be stopped by a police complaint in cyber cell or department of police.

b. Cyber Hate Speech

This is giving a hate speech related to a famous personality, individual, political or religious organization or a company on social media platform. This causes defamation and disrespect to the user. This further led to the contempt and discourtesy to the user on the social media platform.

c. Cyber Bullying

It includes directions of communication network to harass and mental torture the person. It later gives rise to distribution or sending of nasty images, call recordings or videos of cyber bashing to mock the person and lampoon the individual.

d. Cyber Stalking

- It is done through social networking sites. Stalking further causes mental and emotional torture to the person.
- Cyber Stalking is a heinous crime, which is to keep a close track on each step pf user and try to get intimidate by sending her sexual content and try to make out with her. This can only be stopped by a police complaint in cyber cell or department of police.

e. Cyber Grooming

This is a mechanism which pedophile a relationship between person and attacker which foster to sexual molestation or blackmailing. This can be avoided by not interacting and chatting with strangers on social media platforms.

1. Cyber extortion

Attackers nag and oppress victim and victim in order to avoid cybercrime he has to fulfill his demand or pay him in cash or kind. As to remove cyber – threat or stop cyber – attack the attacker also indulge individual in high – risk and dangerous task.

2. Cyber Intrusion and Data Breaches

- Cyber intrusion is done by stealing someone's personal data and attachments from social media platforms and other networking sites and using that information for their dangerous and corrupt plans.
- Data breach is a commotion wherein information is stolen or misappropriation from a system without the knowledge and endorsement of the owner. Stolen data is sensitive, confidential and of national security.

3. Malware Attack

- Venomous and nasty software that is installed by various fraudulent ways. The various sub – categories of malware –
  a. Virus – Treacherous code that recreate itself and require execution in a way to destroy the system.
  b. Worm – Self – reproducing code that transmits through network without any interference and information of owner.
  c. Trojan Horse – This gets conceal within a valid application and gets activated within a few seconds of its installation and create backdoors, delete files and disable the internet service from the system.
  d. Ransom ware – Shakedown malware that hide and bolt users' information in order to blackmail and earn money.
- Virus is a malware that spread by injecting its copy to become and intrinsic of another part. There is transmission of virus from system to system. Worms also cause a similar damage. They recreate their functional copies and damage the system.
- A 'bot' is a type of malware which hackers bring into play to operate and administer an infected or

contaminated system or networks connected and is managed under a single hacker.

- Social media accommodate an excellent platform for spreading viruses and malware. Producers of adware, malware and viruses conceal their death – dealing programs in links, attachments and messages which are an easy go task in any of the networking sites. Once the costumer replies to it, the virus enters the system and start ruining the system without any information to user.

4. Hacking

- Hacking is reconstructing, violating and invading a hardware and software of a digital device which is not his personal property and he is not his creator. Hackers are individual who cater in such programming skills which provide them high level knowledge and can have command in handling the entire set up.
- Hacking – Hacking is to get hands on knowledge of computer and security or 'self – expounding' about computers and security. People who are held responsible for attacking and destroying computers or any digital device are known as "hackers".

Various categories and sub – groups of Hacking are:

- White Hats – individuals who work under restrictions and guidelines of 'hacker ethic' as not to cause harm or for security purposes.
- Gray Hats – the phrase was profound by Lopht. These hackers are best acknowledged as old school hacking groups. They work as security consultants.
- Black Hats – hackers are provoked by anger, power and hatred. They do not give a second thought or hesitate before stealing or dismantling a network in which they trespass or invade.

Sub – groups of Hacking

- Elite – they have information, knowledge and skills of top most grade of hacking. This status is gained by popular hackers, maneuvers and endured phase.
- Script Kiddies – this is most disdain group within the hacking community. As they are youngest and most unskilled hackers and serve those cat paws which are established by elite hackers.
- Cyber – Terrorist – They use stenography and cryptology for swapping details, documents and directions. They are motivated by social and political groups as to disrupt the security system or grasp the information of other nation's security or other national policies. This operation is done to target or bull's eye on a specific military operation of a nation to cause threat or damage to defense system of a country and further relates to cyber – terrorism.
- Disgruntled (ex) Employees – One of the most threatening and publicized groups. These people lose their corporate sector jobs or work, and take retaliation or do tit for tat by hacking their system and entering viruses or worms in their systems.
- Virus Writers – These hackers' enterprise the weakness of other hackers and then code or phrase these methods to do foible in their systems.
- Hacktivist – These people attack political, social or religious agendas of groups as to deficit their website and establish a denial of services feature to disgruntle the functions of website.
- Suicide Hackers – Individuals motivate to slope down the deprecatory infrastructure for radical causes who are afraid for going jail. They have links with suicide bombers and can lead to cyber – terrorism.
- Spy Hackers – These hackers' contract for stealing or capturing trade secrets of a company and to become a part of corporate world and for gain of cash, these hackers do these odd jobs.

Cyber – attacks

- Advanced Persistent Threats (APT) – APT is a combatant process that possesses worldly – wise and knowledgeable levels of expertise and consequential resources to grant opportunities to target its objectives by using variant attack vectors. Its main objective is to reduce an elongated time - span and to adapt efforts or skills for grade of conformity with the costumers. The attack cycle aims at target discovery, data, research and intelligence trumpet.
- Remote Code Execution – This is the procedure to execute malware remotely in order to deceive and take or hold on the system.
- ARP poisoning – Address Resolution Protocol misguide inter – related gadgets of the original MAC machine. It enters the system by popping up a request and create a reply encase which take the piss off and trick a game which make a hole for poison.
- Bluejacking – A message is sent via Bluetooth device without permission of owner, which can also contain sound effect. This prey the control of device in a no – disclosure mode.
- Cookies and Attachments – Cookies can engulf web – browsing history and malicious secretive data. This led to an attack of session hijacking which target main attachments and cause virus and worms' attack.
- Cross – site Request Forgery - This is to create misleading HTML links and redirecting the users to perform some specific instructions.
- DNS poisoning – Domain Name System poisoning is attack to change or reshape the cached DNS results. The major threat is the reproduction of DNS information to Internet Service Provider and cached in the system.
- Evil twin – Rouge access point attack which structure and aligned a new WAP (Wireless Access Point) with same SSID (Service Set Identifier), or free Wi – Fi. This led to theft of confidential data which is done by using public Wi Fi services.
- Spoofing – This attack is done to change IP address and email address as to cancel and secure the attackers identity, through which they can easily delete some important files by taking control of the device.

Cross countries legislations to stop cyber crime

Cambodia

Under direction and guidance of Kingdom of Cambodia, Cyber Crime Laws is drafted. The main objective of this legislation is to govern and shape education, safety measures and concise all kinds of offences carried out by computer system. The aim of law is to ensure safety and prevent all licit and sanctioned interest in using and developing technology.

Article 7: Duties of National Anti – Cybercrime Committee (NACC) The NACC has following duties –

- Construct strategies, action – plans and programs to shield cyber community and information gauze for government and general public.
- Instruct and suggest course of operation to General Secretariat of the NACC.
- Administer work – flow and tack action – plans execution.

Article 16: Investigation power of the NACC

1. Officers or dignitaries of NACC has nominated and designated by judicial police officials who are given patronage or supervision to inspect cybercrime offence.
2. During investigation of a cybercrime, another offence is founded who has same facts and circumstances which are associated or has a link with previous crime, then the crimes must be scrutinize by NACC and a complaint must be filed to the expertise authority.
3. With the command of court NACC can endeavor forensic department inquiry in stipulation to speed up and lubricate the work of court and lessen the burden of court also.
4. Article 17: Preservation of Computer Data and Data Trafficking:

Cases of top – priority and dully legitimate, have given rationalize instructions relating to arrangements or basis of a criminal offence by use of a computer system as for the backbone of evidence or for identifying the executor of commission of counterfeit data or doing data trafficking which is subject to destruction, risk of alteration.

Steps stated in sub – clause (1) should be command in period not more than 90 days and if period outstrip it should be not more than 30 days.

For execution and preservation of data a service provider is appointed and subsequent steps are taken for criminal inspection of data by the court.

Article 27: Child Pornography

Any person by malicious act or unintentionally, commits the following acts –

- Construct child pornography for reason of spreading sexual videos of child by computer system.
- Provide or make it accessible through a digital device
- Circulate or handout via a system
- Acquire or get hands on child pornography by system for oneself or someone else.
- Store or horde in a system shall be imprisoned for 1 year which may exceed to 3 years and fine 2 million Riel to 10 million Riel.

Explanation of 'child pornography' for clause (1) –

- A minor captivates in sexually explicit deal
- Realistic images showing to a minor captured in a sexually explicit conduct.

Riyadh, Saudi Arabia

The Saudi Anti – Cyber Crime Law purpose is to firm and procure the cautious exchange of data, protection of rights of users and to safeguard public interest, morals and most important is to protect their privacy. According to law cybercrime means "offences that are perpetrated against individual or an organization or group with an unlawful intention which led to cause harm to prestige of victim and cause mental harm and torture either directly or indirectly by using modern telecommunication networks.

Article 2: Purpose of Cyber laws

Laws target to put to an end or at least try to control crimes by identifying such crimes and their criminals and ensuring their end results and punishments to certify the following:

- Strengthen and reinforce information security
- Safeguarding rights concerning to legal and licit uses of computers
- Preserving public interest, morals, nation security and economy.

Article 3: Illegitimate control of system through networking sites

- Counter – spy, blocking or unlawful swapping of data via networking sites or a system without justifiable approval of the owner.
- Unguarded access to computers with desire to threaten or blackmail an individual to oblige him to lay hold on or forbear him from taking an action.
- Criminal use of a website or hacking a website with the intention to reconstruct its blueprint or pattern as to dismantle, change or seize its URL.
- Conquering privacy through the maltreatment of camera – equipped digital devices.

shall be subject to imprisonment for a term of year which shall not increase 3 years or a fine which shall not extent five thousand riyals, or both.

Article 4: Financial loss and its punishment

1. Procurement of movable property or bonds for personal use or other motive or signing such bonds across fraud or serve as false identity or name.
2. Illicit access of bank or credit data, or data pertaining to possession of securities with goal to procure data, documents, information or credential data.

Provided that such person shall be punished for a term of imprisonment not more than 3 years or fine not more than two million riyals or both.

Article 6: Causing threat to public at large

1. Person who commits the following cybercrimes shall be punished for five years imprisonment and fine i.e., three million riyals or either of punishment.
2. The cybercrimes that are threat for whole of society are as follows

- Presenting, building, constructing, circulating or hoarding the material on a website for porn videos or gambling sites on a public order.
- Framing or casting information on a website via computer which stimulate human trafficking or

exemplify method of use or accelerate transactions of narcotic and psychotropic drugs.

Article 7: Cybercrimes against nation's security

1. Building or printing of a website on networking sites for terrorist organizations to lubricate communication with heads or associates of such organizations and provide them weapons or bombs or get indulge in other technique used in terrorist activities-
2. Unsanctioned approach to a website or an information directly or via networking sites or any through any digital device with the aim of pursuing data jeopardy the national security of the nation or nation's economy.

Provided that such person who execute aforesaid crimes shall be subject to imprisonment which may extend to 10 years and fine not more than five million riyals or either of one punishment.

UAE (United Arab Emirates)

The National Electronic Security Authority (NESA) formulates Cybercrime law which modulates the protection of communication networks and information system. The law barred any unguarded access to website or digital device.
Article 35: Cybercrimes against religion or religious values

A person whoever commits cybercrime to provisions of Islamic sharia, shall be punished by imprisonment of 7 years or fine not exceeding one million dirhams, or both.

Underneath is cybercrimes carryout by computer network or any other digital device which are against any religion or religious practices –

1. Offend any of the Islamic customs or sacredness
2. Abuse any of customs or solemnity of any other religion whether those practices are absolute and inalienable.
3. Humiliate or offend any of acknowledged and divine astronomical religious propagandas.
4. If crime include insult to Divinity (Allah or God) and prophets Islam or disciples of
5. Hindu or any other religion and principles of its origin.

Bangladesh

The Information and Communication Technology Act, 2006 has formulated cybercrimes law.

According to this act cybercrime means "any criminal activity that serves a computer either as a device and has goal for immortalize crimes, all these activities came under umbrella of cyber-crime."

The genus of cybercrime is the illegal and unauthorized conduct of computer. Section 66: Punishment for tempering with computer source documents: -

A person by his ambition or forethought hide, destruct or modify any computer source, data, network site is confidential and required protection by law for time being in force, that person shall be punished with imprisonment fir a term which shall not more than 3 years and fine.

Section 67: Hacking with computer system: -

Whoever with intention to conviction or perceive that he is likely to cause wrongful lose or destruction to public or a person, does any act for destruction deletes or change any information inhabit in a system or diminishes its value or efforts its detrimental means, that conduct of offence is called "Hacking".

Section 68: Punishment for hacking: -
Whoever commits hacking will be punished for imprisonment which may not extend three years or fine which may extent to 2 lakhs or both.

Ghana

The Parliament of Ghana in December, 2008 passed the Electronic Transactions act (ETA), 2008. Its main objective is to save the cyber space as a method to pacify crimes that may affect the capability of citizens to being it valued. The Data Protection Act, 2012 commission potential and power.

Clause 3: Cyber Crime against Data Breach

A person dies following illegal activities that will be considered as Data Breach: -

1. Enactment and examine compliance by individuals who employ the electronic industry.
2. Make directorial arrangements it consider absolute for dismissal of the duties.
3. Inspect any complaint under this Act and ascertain in the manner as commission think fit as fair & reasonable.
4. Keep and sustain the
5. Data Protection Register

Provide that data breach is a bailable offence and punishment is imprisonment not more than 3 years.

South Africa

The cybercrimes and cyber security bill are designed to inflict penalties to abide cybercrime and synchronize jurisdiction in respect of cybercrimes and establish a framework to promote cyber security.

Section 4: Unlawful acts in respect of software and hardware tool

1. Whoever does illegal or purposefully produce, sells, buys, take over, fabricate, acquire, access or advertise any software or hardware tool for goal or target for contravening the computer data or storage is guilty of an offence.
2. Explanation – 'software or hardware tool' means any electric, machine – like, tool, instrument or equipment or a notable component of a digital device. This is shaped or framed for the following purposes –

- Acquiring access as scrutinized
- Examining data as foreseen
- Intercession with data or system
- Changing, reproducing, accessing or dispensing a password or code.

Section 5: Unlawful interference with data or computer program

Any person who by illicit and voluntarily impinge with –

- Computer program
- Data is a culpable offence.

For this section "interference with data or computer program

means to permanent or temporary –

a. Eradicate data or computer program
b. Modifying data or computer program
c. Furnish, destruct or valuable data or computer program
Section 8: Cyber Fraud

A person who unguarded or with objective deceive or does misinterpret –

- By mode of data or computer program
- Through any intervene with data or program of a system which causes definite or prospective prejudice to another person has conducted culpable offence of cyber fraud.

Section 10: Cyber extortion

Whoever by illegitimate and voluntarily –

- Pressurize to conduct a crime
- Execute any offence, and,

Does interception acquire any data or use any data, program or software is found guilty of offence for purpose of –

- Taking benefit from another person
- Constrain another person from doing any act is guilty of an offence of cyber extortion.

Nepal

The Cybercrime act is drafted as a bill on stakeholder consultations and conducts. This act is applicable to whole of Nepal and to a person who does or perpetrates any act against this act.

Section 5: Illegal remaining in an electronic system

Whoever voluntarily and by unlawful manner remain logged in a digital device or any part of that device and continues to remain in the system shall be punishable for imprisonment and fine based on the magnitude of the offence.

Section 6: Illegal interception

A person voluntarily and unguarded way excess a lawful manner or intercession by mechanical and electric means –

- Any private transferable to, form or within a digital device
- Removal of radiations and energy wave ionizing from electronic system

Such person is liable for punishment of imprisonment and fine depending upon the grade of degree of the crime.
Section 16: Solicitation of women and children

A person voluntarily, via a digital device or gadget forces a women or child to indulge in and meet the requirements of illicit relationship or sexual exploit of the person, aid or abets the connection or conduct of sexual exploit shall be liable for imprisonment and fine based on the magnitude of offence.

Philippines

The Cybercrime Prevention Act, 2012 is drafted to address legal issues relating to online interactions and networking sites. The unlawful acts done through internet were denounce by criminalizing libel and to retrench freedom of expression and speech which cause defamation to another person.

Section 15: Search, seizure and examination of computer data–

The search and seizure are required to done by warrant from court or by appropriate authority which fulfill following duties and power imposed –

- Assure a computer system, data and information storage system
- To reprint or construct copy of those data
- To stable the coherence of relevant data
- To regulate or deport forensic analysis or inspect the computer data
- To exhibit abstruse or delete those computer data
- Provided that steps are taken to safeguard the data and necessary information on documents to ensure the search and seizure. The period for examination must be conducted within 30 days from the date approved by the court

Cyber Laws of India

As Cyberspace is a spectral and bodiless dimension that is impossible to regulate and safeguard using conventional law. The chief or foremost source of cyber law in India is the Information Technology Act, 2000. Most of cyber-crime cases are committed by educated person. So, it is required the deep knowledge about the cyber –crime and its prevention. Also, in India most of the cases found where, crimes are committed due to lack of knowledge or by mistake.

Information Technology Act, 2000

This act lays down legislation and rules and regulations to deal with cybercrimes or computer– oriented crimes and to promote cyber security. This act provides legal remembrance for transactions carried out by mode of electronic devices, electronic data, computer system and other electronic or internet connected spheres.

Section 43: - [Penalty & Compensation] for damage to computer, computer system etc.: -

Whoso ever without the authority of owner, or who possess the system, extract or get hold of computer, computer system or network: -

a. Acquire or affiliation approach such computer, computer system or network and resource.
b. Reproduce, duplicate or distillate any data, database, information from such computer, computer system and network consisting of information or data stored in a detachable storage mode.
c. Detroit or genesis to be dismantling any computer, computer system, network, data computer data base or any programmers repose in such computer, computer system or network.
d. Institute or launch or convict to be introduced in any computer contaminated or computer virus into computer, computer system or network.
e. Disorganize or cause deranges such computer, computer system or network.
f. Dissent or cause rebuttal of outpouring to any person command or such computer, computer system or network by any medium.
g. Grant any support to any person to expedite outburst to a computer, computer system or network in contrast of provisions of this Act, rules and regulation stated.
h. Tariff the services 'aid ed' by a person to account of another person by tinkering or exploiting any computer,

computer system or network.

i. Destruct, remove, modify any information inhabit in a computer resource or shrink its value or use or affects it dangerous by any means.
j. Theft, hide, destruct or modify or causes any person hide, steal or destruct any computer source, code served by a computer resource with an aim to dismantle the system.

Shall be punishable to pay damages by way of reimbursement to person so work on. Explanation: - For the requirement of this section: -

1. Computer contaminant means any set of computer directions that are framed: -
   a. To change, destruct, transfer or document program residing within a computer, computer system or network.
   b. By any means to seize the normal conduct of computer, computer system or network.
2. 'Computer database' means a depiction of information facts, concepts or directions in text, image, audio, video that are being put together in a standardize method it gave been generated by a computer, computer system or network and motive for use in computer, computer system or network.
3. 'Computer Viruses' means computer specification, data, programme or manual that destruct, breakdown, deface or adversely affect the performance of a computer resource or attract itself to another computer resource and set off when a programme data or instruction is contemplated or some other events of computer resource.
4. 'Damage' means to change, destruct, regroup, any computer resource by any medium.
5. 'Computer Source Code' means jotting down list of programmers, computer commands, design and framework of programme inspection of computer resource in any form.

Section 43A: Compensation for failure to protect data – Where a body corporate own, covenant or grasp any sensitive and confidential personal data or information in a computer resource which it utilize, acknowledge or handle, is neglected by executing and sustaining reasonable security practices and procure and there by wrongful loss or gain to any person, such corporate body must be liable to fine to compensate the injury caused.

Section 66 F: Punishment for cyber terrorism – A person who–

With aim to menace the unity integrity security or sovereignty of India or to bash terror in people –

1. Contradict or cause the contradiction of access to any person authority to acquire computer resource.
2. Procure hand to acquire a computer resource without permission of owner. (iii)Direct or cause to direct any computer contaminant.

And by any mode work on or is likely to cause bruise or demise to person or destruct of property, services to the community or censorious information.

Voluntarily creep into a computer resource without knowledge or authority of owner, and acquire data or information that is restrained to use for security reasons in relation to state, public morality, decency, foreign relations, contempt of court, defamation or incitement to an offence of cyber terrorism

Section 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: - Whoever –

a. Communicate, print or broadcast or cause to print or broadcast material in any electronic form which show children seize in sexually explicit act or work.
b. Compose, text or digital images, store, swap, reproduce, search, spread material in an electronic form depict children in sexual nasty, outrageous exploit manner.
c. Refine, persuade children to online relationship with one or more children for sexually explicit act or a work that is improper and is a crime and not just.
d. Ease abusing children online, or,
e. Store in any electronic mode from own abuse or that of others perpetuates to sexually exploit conduct with children.

Shall be punishable for not more than 5 years and fine not more than 10 lakh rupees for first attempt and for subsequent attempts imprisonment for a term which may increase to 7 years and fine not more than 10 lakh rupees.

Provided that under provision of section 67, section 67A if printing, documenting in a book, newspaper or pamphlet is to be justified and for good faith and used for bona fide heritage or religious purpose is not an offence.

Section 72: Penalty for breach of confidentiality and privacy-

If any person as provided in the Act, or for law being in force for the time, discharge the powers stated under this act, rules and regulation thereunder, has utilized the access or acquired to any electric mode of record, register, information, correspondence, document or other material without the permission of the owner shall be liable for punishment, i.e., imprisonment for a term not more than 2 years or fine not more than one lakh rupees or both.

The Information Technology Act, 2000 also target to provide the legal shell so that legal sanctity is harmonised to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be manifest by electronic means of communication and the same shall have legal validity and enforceability.

Hybrid model of laws for cybercrime and Cyber Security in India

As there is rapid development in the field of internet and technology; there is also speedy elevation of cybercrime in India. The government of India has drafted an act 'Information Technology Act, 2000 which lay down lays down legislation and rules and regulations to deal with cybercrimes or computer – oriented crimes and to promote cyber security. This act provides legal remembrance for transactions carried out by mode of electronic devices, electronic data, computer system and other electronic or internet connected spheres.

There is a gap and requirement of some improvisation in the act. This is an attempt to state some rules and regulations regarding various modes of cybercrimes and their cyber security.

Future Scope of Research

In this research paper, the focus is primarily on various modes of cybercrimes in world and drafted bill of cyber security and also included cybercrimes against women and children as cyber stalking, cyber bullying, child pornography and many more. Our research is limited to cyber – terrorism.

and regulations are stated to fill this gap and provide cyber security against cybercrimes.

S.no.	Domain of cybercrime	Legislations
1.	Drafting a bill for cybercrime and cyber security	The cybercrimes and cyber security bill are designed to inflict penalties to abide cybercrime and synchronize jurisdiction in respect of cybercrimes and establish a framework to promote cyber security.
2.	Information Technology	This act must be applicable to whole of India and to a person who does or perpetrate any act against this act.
3.	National Anti – Cybercrime Committee (NACC)	There must be a committee to deal with cybercrime as to lessen the burden of courts and tribunals. The NACC has following duties - Construct strategies, action – plans and programs to shield cyber community and information gauze for government and general public. Instruct and suggest course of operation to General Secretariat of the NACC. Administer work – flow and tack action – plans execution.
4.	National Electronic Security Authority (NESA)	An authority is formulated for cyber security of computer and computer systems. It formulates Cybercrime law which modulate the protection of communication networks and information system. The law barred any unguarded access to website or digital device.
5.	Child pornography	Explanation of 'child pornography' for section 67B of Information Act, 2000 – A minor captivates in sexually explicit deal Realistic images showing to a minor captured in a sexually explicit conduct.
6.	Cybercrime intended to harm society at large	Framing or casting information on a website via computer which stimulate human trafficking or exemplify method of use or accelerate transactions of narcotic and psychotropic drugs.
7.	Cybercrimes religious values against religion or	A person whoever commits cybercrime to provisions of Islamic sharia, shall be punished by imprisonment of 7 years or fine not exceeding one million dirhams, or both. Underneath are cybercrimes carryout by computer network or any other digital device which are against any religion or religious practices – Offend any of the religion customs or sacredness Abuse any of customs or solemnity of any religion whether those practices are absolute and inalienable. Humiliate or offend any of acknowledged and divine astronomical religious propagandas. If crime include insult to Divinity (Allah or God) and prophets Islam or disciples of Hindu or any other religion and principles of its origin.
8.	Hacking with computer and its punishment	Whoever with intention to conviction or perceive that he is likely to cause wrongful lose or destruction to public or a person, does any act for destruction deletes or change any information inhabit in a system or diminishes its value or efforts its detrimental means, that conduct of offence is called "Hacking". Person will be punished for imprisonment which may not extend three years or fine which may extent to take 2 lakh rupees or both.
9.	Hacking a URL and its punishment	Criminal use of a website or hacking a website with the intention to reconstruct its blueprint or pattern as to dismantle, change or seize its URL. Person shall be subject to imprisonment for a term of year which shall not increase 3 years or a fine which shall not extent to 1 lakh rupees, or both.
10.	Cyber Extortion	Whoever by illegitimate and voluntarily – Pressurize to conduct a crime Execute any offence, and, Does interception acquire any data or use any data, program or software is found guilty of offence for purpose of – Taking benefit from another person Constrain another person from doing any act is guilty of an offence of cyber extortion.
11.	Illegal Interception	A person voluntarily and unguarded way excess a lawful manner or intercession by mechanical and electric means – Any private transferable to, form or within a digital device Removal of radiations and energy wave ionizing from electronic system Such person is liable for punishment of imprisonment and fine depending upon the grade of degree of the crime.

We can also further research on cybercrimes for firearm weapons, cybercrime for trafficking in arms and weapons. There is scope for research on cybercrimes related to foreign relation of India with other countries that is also a very vast and interesting topic to research on. The research work is very vast and as it is done to grasp more and more knowledge.

CONCLUSION

Cybercrimes and cyber security are connected to each other. India has drafted Information Technology Act, 2000 which lays down legislations against cybercrimes and have also stated its punishments. There is gap in the act and some rules

References

1. Kumar, S., Koley, S., & Kuamr, U. (2015). Present Scenrio of Cyber Crime in INDIA and its Preventions. *IJSER*, *6*(4), 1972-1976.
2. Schjølberg, S. (2017). *The History of Cybercrime: 1976-2016*. BoD--Books on Demand
3. Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: trends and challenges. *International Journal of Innovations & Advancement in Computer Science*, *6*(12), 187-196.
4. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief

study on cyber crime and cyber laws of India. *International Research Journal of Engineering and Technology (IRJET)*, *4*(6), 1633-1640.

5. Adamski, A. Cybercrime Legislation in Poland Cybercrime Legislation in Poland.
6. Giri, S. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. *Pramana Research Journal*, *9*(3), 662-672.
7. Ennin, D., & Mensah, R. O. (2019). Cybercrime in Ghana and the Reaction of the Law. *JL Pol'y & Globalization*, *84*, 36.
8. Jayasekara, A. D., & Rupasinghe, W. (2015). Cyber-Crime in Sri Lanka. *Journal of US-China Public Administration*, *12*(10), 759-763.

How to cite this article:

Ananta Aggarwal and Kajal Mittal (2021) 'Developing Hybrid Model of Laws for Cybercrime & Cyber Security in India Through Cross Countries Study', *International Journal of Current Advanced Research,* 10(05), pp. 24509-24518.
DOI: http://dx.doi.org/10.24327/ijcar.2021.24518.4863

****