HISTORICAL GENESIS AND EVOLUTION OF CYBER CRIME AND CYBER SECURITY LAWS IN INDIA

Dr. Sanjeev Kumar[1], [2]

[1]M.Phil and PhD in International Relation and Politics & NTS from JNU, New Delhi
[2] Assistant Professor in Legal, Department of History, Chanakaya Law College, Maniharan, Saharanpur, UP Affiliated Chaudhary Charan Singh University Meerut, UP-India

---***---

Abstract - *Crime has also been associated with the history of Human life. Along with a civil society, crime has also been continuously associated. The crimes have also changed with the time and circumstances. In modern time, a word like cyber crime comes to the forefront. Almost all nation-state of the world have constituted laws to deal with cyber crime. The development of the technology and electronic information has led to the beginning of computer related crimes commonly known as cyber crime. In this article we are presenting the very important information which explains cyber crime. As well as studying what is the history of cyber crime in India and what laws have been constituted related to cyber security.*

Keywords: ***Acts and Regulations, Cyber Crime, Cyber Security, Cyber laws, Cyberspace, Cold War, Information Technology, Model Law, Netizens, National Security, Worldwide, etc.***

1. INTRODUCTION

The emergence of cybercrime is a significant step in human history. That had an impact on the crime's social and financial aspects. In the age of information technology, cybercrime may seem to have a recent past, although there has always been evidence of it. Numerous ancient texts, dating back to prehistoric times, as well as legendary tales, have discussed crimes done by individuals, whether they were against another person, like common theft and burglary, or against the nation, such espionage and treason. Kautilya's Arthashastra, acknowledged to have been a realistic administrative treatise in India and published around 350 BC, discusses a variety of crimes, proper security measures for rulers to implement, dangerous crimes within a state, etc. Additionally, it suggests punishment for the list of predetermined offences. The Arthashastra further analyses the notion of compensating victims for their losses and lists the numerous punishments that have been handed out for the specified offences. All members of society are negatively impacted by crime, regardless of its form. Due to the Internet's fast spread and the digitalisation of commercial activity, cyber crime has risen sharply in developing nations.

Today, the world community started making cybercrime laws according to the way, the number of crimes in cyberspace increased in the virtual world. If we throw light on history of cybercrime laws, then its beginning is associated with the beginning of the internet world. The laws governing this area are known as Cyber laws and all the netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet. The concept of security is a core concept in the study of international relations. Traditionally, and until relatively recently, security analysis focused on state security, viewing it as a function of the levels of threats which states face from other states, as well as the manner and effectiveness of state responses to such threats (Rather and Jose 2014)[1]. In reality, the phrase 'cybercrime' is mostly used in knowledge society of the 21st century, and is created by combining two terms cyber and crime. The continually increasing cyber crimes not only threaten national security but also pose a direct threat to international security. Cybercrime is 'transnational or international' there is no border in cyber world. What such laws have been made by world governments and how will they control such crimes, those subjects have been highlighted in this research article.

2. SIGNIFICANCE OF THE STUDY

The entire world is moving towards development and simultaneously towards technological advancement and the rapid development of internet and computer technology globally has led to the growth of new forms of transnational crime especially. The problems and crimes brought by or in sector of information technology/ internet have virtually no boundaries. The researcher believes that the final paper will provide the readers with knowledge of cyber-crimes, cyber laws of India especially Information Technology Act of India.

3. OBJECTIVES OF THE STUDY

The objectives of the study are some following:

1. To investigate the history of cyber crime in the world.
2. To examine the concept of cyber crime and constituted cyber laws in India.

3. To highlight the cyber crime impact on national and international security.

4. To discuss the cybercrime breach of confidentiality and privacy of National Security.

4. RESEARCH METHODOLOGY

This article is focused on both histories of cyber crime and cyber laws in India. I have taken account both primary and secondary sources of data information's. The primary sources of information are constitution, Acts and regulations of India while secondary sources of information are articles, journals, commentaries and book. In this research, I have also followed Bluebook rules of citation.

5. SCOPE OF THE STUDY

In this research paper, I have tried to focus on cyber-crime, its types, Information Technology Act of India and compare analysis with other countries. This article may touch any other laws, rules or regulations of the countries but will not deal with them deeply. It will contain some cases of India but there is no any time period limit for the cases.

6. CONCEPT OF CYBER SECURITY

The word 'cyber security' is yet to be defined in a comprehensive manner because of the complex and fact changing nature of information and communication technology at global and national level. This device allowed a series of steps that was continual within the weaving of special fabrics or materials.[2] One of the most concise ones can be found on the Techtarget website and it states: 'Cyber security is the body of technologies, processes and practices designed to protect networks, computer, programs and data from attack, damage or unauthorized access. The term cyber security incorporates both the physical security of devices as well as the information stored therein. It covers "protection from unauthorized access, use, disclosure, disruption, modification and destruction".[3] According to the Information Technology Act, 2000 cyber security means "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction." Advocate Prashant Mali trying to define the cyber security as "cyber security means the processes & technologies designed & implemented to protect devices, networks and data from unauthorized access, vulnerabilities and incursion into IT infrastructure via any network or the cyber space (internet) by a malefactor with any intent".[4] Cyber security is strategy against unauthorized access or threats to computers, programs, networks, personal data, etc.

7. HISTORICAL GENESIS AND EVOLUTION OF CYBER CRIME

The historian Kumar and others idea about historical genesis and evolution of cyber crime is that "The primitive type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom".[5] According to Chaubey stated that "during the period of 1950's, it would be an astonished feeling for everyone who uses palmtops and microchips today, to know that the first successful computer was built and the size of the computer was so big that it takes the space of entire room and they were too expensive to operate. The Personal computers become cheaper and become household item at the start of 21st century in India. The Internet was first started by the US department of defence, after World War II with the idea to have a network which could work in the event of disaster or war and securely transmit information".[6]

Abraham and Seymour described in his book "However at that point nobody anticipated the opportunities' the internet is going to provide the technology savvy criminals. In India the internet services started by the state-owned Videsh Sanchar Nigam Limited in year 1995 and in 1998 the government has ended the monopoly of VSNL and market is opened to private operators. At that point, the internet users in India are 0.1% of total population, and now India has become the 2nd largest country in terms of internet users after china with 33.22% people using internet.[7] The process of criminalization of human behaviour judged to be harmful the public is typically one that builds slowly in common law jurisdictions. Momentum gained through problem identification and pressures exerted mg special interest groups can easily span decades before undesirable actions are classified as "crime". In some instances, this process is accelerated through the occurrence of certain "catalyst events" that capture attention of the public and the attention of lawmakers".[8]

According to Abraham and Seymour explanation "In the case of computer crime, legislators grew increasingly attentive is the 1980s as businesses became more dependent upon computerization and as catalyst event cases exposed significant vulnerabilities to computer crime violations. Criminals can now easily encrypt information representing evidence of their criminal acts, store the information and even transmit it with little fear of detection by law enforcement".[9] "Due to the extraordinary impact of the Internet, a computer crime scene can now span from the geographical point of the victimization to any other point on the planet, further complicating criminal investigative efforts. A commonality among these types of crimes is that the offender, to a great degree, depends upon the lack of technological skills of law enforcement to successfully commit the offenses and escape undetected. Based upon what empirical evidence has been available on self-assessed skills of investigators in this area, computer criminals would have good reason to feel some confidence in their chances to evade detection of their crimes”. [10] As we advance towards the 21st century, it can be observed that “the technological innovations have laid the way for the entire population using computer technology today, to experience new and wonderful conveniences in their daily life ranging from how to educated, shops, entertain, to availing the understanding of the business strategies and work flow”.[11] But it's fair to say that the technological marvels that have enhanced our quality of life also have certain risks. While computer technology has given many people access to improved conveniences, it has also given thieves new entry points.

8. TYPES OF CYBER CRIME

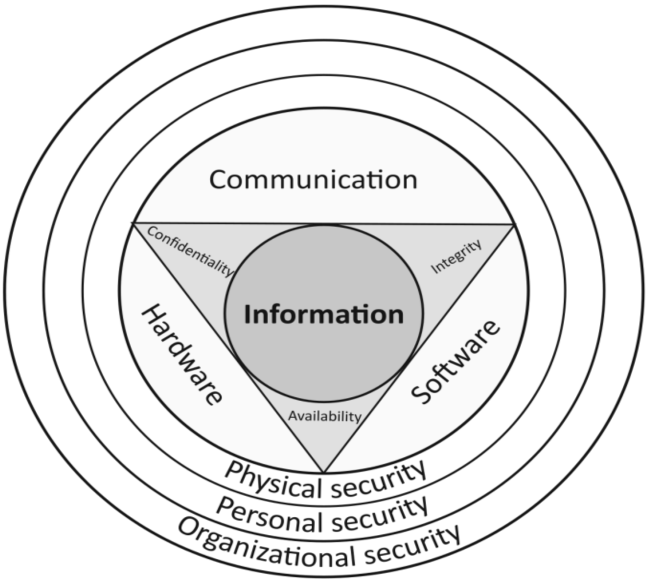
This article examines the acts wherein computer or technology is tool for an unlawful act. The kind of activities usually involves a modification of conventional crime by using informational technology. Here is the list of prevalent cyber crimes, some of them widely spread and some are not prevalent on larger scale. Cybercrime is classified on the basis of the subject of the crime. The cyber crimes are discussed below-

1. Cybercrime against Individuals
2. Crime against Organizations
3. Crime against society

8.1. Cybercrime against Individuals

These types of crime such crimes are committed against a person or his property. Following are the examples of the main offenses covered under it.

A. Unauthorized Access
B. Online fraud
C. Cyber Stalking
D. Hacking
E. Plastic Card Fraud
F. Spoofing
G. Identity theft



8.2. Cyber Crime against Organizations

In contemporary era, almost all big companies and organizations are more back on their online growth. In such a situation, they also have to deal with cybercrime. Some examples of the main cybercrimes committed against institutions or organizations are:

A. Data breach
B. Cyber terrorism
C. Warez distribution
D. Denial of service (DoS) attack

8.3. Cyber Crime against Society

These types of cybercrimes that effect of the entire society, in which the number of young men & women and children are more affected. Also, which are banned websites and products in the society and illegal materials are made available to the people through the internet. Following are the examples of the cybercrimes against society.

A. Child pornography
B. Online gambling
C. Selling illegal article
D. Forgery
E. Spamming

9. HISTORY OF CYBER CRIME

The cyber crime is evolved from Morris Worm to the ransom ware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation. The historical evolution of cybercrime threats are given in chronological order.

S.No.	Country	Year	Cyber Crime threats
1.	France	1834	The first cyberattack ever is effectively carried out when two bandits breach the French Telegraph System and steal stock market data.
2.	USA	1878	Near the beginning Mobile Calls-Two years after Alexander Graham Bell created the device, the Bell Telephone Company disconnects a group of young boys from the New York telephone network for regularly and purposefully misdirecting and disconnecting consumer calls.
3.	Davy Crockett Cat	1955	In order to test a theory regarding how phone networks function, Phone Hacker-David Condon whistles his phone while playing his "Davy Crockett Cat" and "Canary Bird Call Flute." The computer accepts the secret message, assumes he is an employee and links him to a long-distance operator
4.	USA	1957	Joe Engressia, a blind, 7-year-old boy with perfect pitch, hears a high-pitched whistle on a phone line and begins to whistle along to it at a 2600Hz speed, helping him communicate with phone lines and becoming the United States' first phone hacker or "phone phreak."
5.	USA	1969	RABBITS Virus-The University of Washington Data Center downloads a program on a computer from an unknown user. The inconspicuous machine creates copies of itself before the machine overloads and ceases running (breeding like a rabbit). It is known to be the first virus on a computer.
6.	Nederland	1970-1995	Kevin Mitnick-Kevin Mitnick penetrates some of the highest-guarded networks in the world, including Nokia and Motorola, leveraging specialized social engineering systems, tricking insiders into handing codes and passwords over and using codes to breach internal operating systems.
7.	USA	1973	Embezzlement-A local New York bank teller uses a machine to embezzle more than $2 million.
8.	UK	1981	Ian Murphy, also known as "Captain Zap," was found guilty of cybercrime after breaking into AT&T's network and changing the internal clock to charge off-hour rates during times of high network traffic.
9.	Siberian	1982	The Logic Bomb The CIA blows up a Siberian gas pipeline by injecting a code into the network and the operating system to monitor the gas pipeline without using a bomb or a missile.
10.	USA	1984	US Secret Service-The United States Comprehensive Crime Prevention Act grants authority over electronic theft to the Secret Service.
11.	USA	1988	The Morris Worm-Robert Morris releases what on the Internet will be considered the first worm. To show that the author is a student there, the worm is released from a computer at MIT.
12.	UK	1989	Trojan Horse Program A diskette that appears to be an AIDS information archive is mailed to a UK electronic journal to thousands of AIDS researchers and subscribers.
13.	USA	1994	Managers of Datastream Cowboy and Kuji at the Rome Air Production Centre, a U.S. Over 100 user profiles have been compromised thanks to a "sniffer" password installed on the Air Force testing facility's network. Investigators discovered two hackers who went by the names Datastream Cowboy and Kuji were responsible for the attack.
14.	Russian	1995	Vladimir Levin—Russian software developer Vladimir Levin hacks from his apartment in Saint Petersburg into Citibank's New York IT machine and authorizes a number of illegal transfers, ultimately wiring worldwide accounts for an estimated $10 million.
15.	USA	1999	The Melissa Virus-A virus infects Microsoft Word records, transmitting itself via email as an attachment automatically. It mails out to the first 50 names mentioned in the Outlook email address box of an infected device.
16.	Russis	2000	Barry Schlossberg, alias Lou Cipher, successfully extort $1.4 million from CD Universe for services given to the Russian hacker in an effort to apprehend him.
17.	DNS	2002	Online Attack-A DDoS targets the entire Internet for an hour by attacking the 13 root servers of the Domain Name System (DNS). Users are generally unchanged.
18.	Nigeria	2004	Choice Point-A 41-year-old Nigerian citizen breaches Choice Point's consumer records, but the company only notifies 35,000 citizens of the abuse.

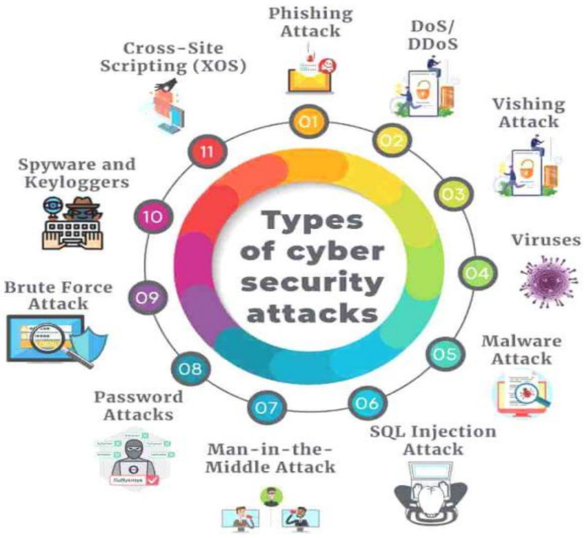
19.	**USA**	**2006**	TJX-A cybercriminal group captures TJX, a Massachusetts-based retailing company, 45 million credit, and debit card numbers. It uses a majority of the stolen cards to fund a Wal-Mart internet shopping spree.
20.	**Russia**	**2008**	Heartland Payment Systems-134 million credit cards are exposed to spyware on Heartland's computer systems via SQL injection.
21.	**The Church of Scientology**	**2008**	A hacker group known as Anonymous targets the Church of Scientology website. The DDoS attack is part of a political activist movement against the church called "Project Chanology." In one week, the Scientology website is hit with 500 DDoS attacks.
22.	**Stuxnet Worm**	**2010**	The Stuxnet Worm-The world's first software bomb is a destructive computer virus that can attack control systems used for controlling manufacturing facilities.
23.	**USA**	**2010**	An Eastern European cybercrime ring steals $70 million from U.S. banks using the Zeus Trojan virus to crack open bank accounts and divert money to Eastern Europe. Dozens of individuals are charged.
24.	**Sony Pictures**	**2011**	A hack of Sony's data storage exposes the records of over 100 million customers using their PlayStation's online services. Hackers gain access to all the credit card information of users. The breach costs Sony more than $171 million.
25.	**Epsilon**	**2011**	Epsilon-A cyberattack on Epsilon that provides consumers, including Best Buy and JPMorgan Chase, with email handling and marketing facilities results in millions of email addresses being hacked.
26.	**RSA SAFETY**	**2011**	Sophisticated hackers steal information about RSA's SecurID authentication tokens, used by millions of people, including government and bank employees. This puts customers relying on them to secure their networks at risk.
27.	**ESTsoft China**	**2011**	Hackers expose the personal information of 35 million South Koreans. Attackers with Chinese IP addresses accomplish this by uploading malware to a server used to update ESTsoft'sALZip compression application and steal the names, user IDs, hashed passwords, birthdates, genders, telephone numbers, and street and email addresses contained in a database connected to the same network.
28.	**Lulzsec**	**2011-2012**	Lulz Security, or LulzSec, a break-off group from hacking collective Anonymous, attacks Fox.com and then targets more than 250 public and private entities, including an attack on Sony's PlayStation Network. They then publicize their hacks though Twitter to embarrass website owners and make fun of insufficient security measures.
29.	**USA**	**2009-2013**	Roman Seleznev hacks into more than 500 businesses and 3,700 financial institutions in the U.S., stealing card details and selling them online, making tens of millions of dollars. He is eventually caught and convicted for 38 charges, including hacking and wire fraud.
30.	**Russian**	**2013-2015**	Global Bank Hack-More than 100 organizations around the world have access to secure information from a community of Russian-based hackers.
31.	**eBay**	**2014**	A cyberattack exposes names, addresses, dates of birth, and encrypted passwords of all of eBay's 145 million users.
32	**Crypto Wall**	**2014**	Crypto Wall ransomware, the predecessor of Crypto Defense, is heavily distributed, producing an estimated revenue of $325 million.
33.	**Anthem**	**2015**	Anthem reports theft of personal information on up to 78.8 million current and former customers.
34.	**Locker Pin**	**2015**	Locker Pin resets the pin code on Android phones and demands $500 from victims to unlock the device.
35.	**Android Phones**	**2015**	With the claim that up to 78.8 million current and former customers' personal information has been compromised, Locker Pin resets the pin code on Android phones and demands $500 from victims to unlock the system.
36.	**Wikileaks**	**2016**	Leaks of DNC Emails: Ahead of the 2016 US presidential election, WikiLeaks received and published emails that had been stolen from the Democratic National Committee.

37.	**Equifax**	**2017**	Equifax-Equifax is compromised, revealing 143 million customer accounts, one of the biggest US credit bureaus. Social Security numbers, birth dates, addresses, driver's license numbers, and certain credit card numbers are part of the confidential leaked info.
38.	**Chilpotle**	**2017**	Millions of Chipotle patrons had their credit card information stolen by an Eastern European criminal organisation that targeted eateries.
39.	**WannaCry**	**2017**	Wanna Cry, the first known example of ransomware operating via a worm (viral software that replicates and distributes itself), targets a vulnerability in older versions of Windows OS. Within days, tens of thousands of businesses and organizations across 150 countries are locked out of their own systems by WannaCry's encryption. The attackers demand $300 per computer to unlock the code.
40.	**Starwood**	**2018**	Using stolen credentials, a threat actor was able to breach Marriott Hotels systems through a Remote Access Trojan (RAT). Data from over 500 million guests, including sensitive data like credit card and passport information, was stolen.
41.	**Dubsmash**	**2018**	The well-known video streaming platform discovered that 161.5 million user details were up for sale on the dark web. The data contained information such as names, email addresses, and encrypted passwords.
42.	**Alibaba**	**2019**	A telemarketing employee privately obtained 1.1 million pieces of data including Alibaba client contact information and leaked it to a distributor's staff member during the November 11 Singles' Day shopping festival.
43.	**Facebookk**	**2019**	An unidentified hacker published phone numbers, account names, and Facebook IDs belonging to more than 530 million Facebook members.
44.	**Sina Weibo** **China**	**2020**	Sina Weibo, the Chinese version of Twitter, has 538 million users, and information on them was stolen and spread online.
45.	**Solar Winds**	**2020**	A well-known cyber security company, Fire Eye, declared they had been the target of a nation-state attack. Security personnel stated that their Red Team toolbox, which contained programmes used by ethical hackers in penetration examinations, had been destroyed. While looking into the nation-state attack against its own Red Team toolset, Fire Eye came into a distribution network attack. The researchers stumbled across evidence that attackers entered a backdoor in the Solar Winds software "trojanizing" Solar Winds Orion business software updates to distribute malware.
46.	**Colonial Pipeline** **USA**	**2021**	An energy firm in the United States, Colonial Network, was forced to shut down its entire fuel distribution pipeline as a result of a ransomware assault, endangering the supply of gasoline and jet fuel throughout the east coast of the country. The largest fuel pipeline in the nation was restored with the assistance of Eastern European hackers after Colonial Pipeline paid them roughly $5 million.
47.	**Accenture**	**2021**	The Lock Bit ransom ware gang breached Accenture's networks, encrypted files and demanded $50 million to avoid having their encrypted files sold on the dark web.

Note- *Data Sources has been collected from Various Cyber Security Reports, 2022.*

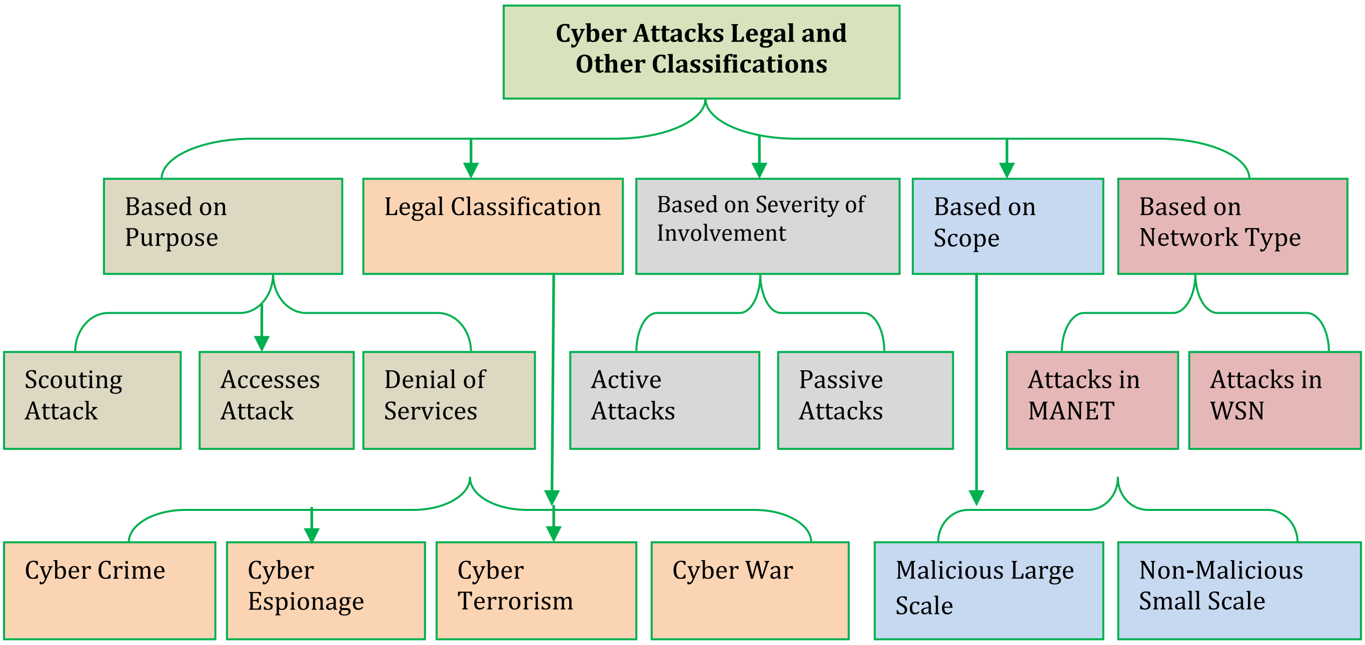
10. NATURE OF CYBER SECURITY ATTACKS

In the time of cyberspace, today human beings are completely interconnected with each other of the world through the internet. The way of information technology has limited the distance, in the same way cybercrimes are increasing day by day in different ways. Cyber security knows no borders and is not limited to any one geography or culture. The challenges and opportunities facing cyber security experts, policymakers and the public are global in nature and require globally-minded solutions at all levels. At the same time, rapid changes in technology have a direct impact on societies around the world and the changing threat environment. The Hewlett Foundation's 2019 Cyber Initiative Grantee Convening will focus on two pillars: (1) the global nature of cyberspace and (2) emerging technology challenges and solutions. These cybercrimes attack the security in the following way.



11. CYBER ATTACKS LEGAL AND OTHERS CLASIFICATIONS

The cyber Attack due to increasing technology can be classified as different types. In this classification, the basic five types of cyber attacks are described. In which legal classification is the subject of our study. The legal classification of cyber attacks as a major threat to national security and international politics in various counties in the world.



This is increasing threat to the nation state as well as humanity. In this diagram the legal classification is divided into the following four parts which are analyzed as cyber crime, cyber espionage, cyber terrorism and cyber war. The technology has increased the number of cyber crimes leading to changes in the world order which is seeing threat as a non-traditional security dimension.

12. REQUIREMENT FOR CYBER LAW IN INDIA

Firstly, India's legal system is quite comprehensive and well-defined. The most important of the many laws that have been passed and put into effect is The Constitution of India. The Indian Penal Code, the Indian Evidence Act of 1872, the Banker's Book Evidence Act of 1891, the Reserve Bank of India Act of 1934, the Companies Act, and others are among the laws they have that we also have. As a result, the advent of the Internet brought about a number of delicate legal difficulties and challenges, necessitating the adoption of Cyber laws.

Secondly, "the existing laws of India, even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgment found that it shall not be without major perils and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace"[12] without enacting new cyber laws.

Thirdly, "none of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email is not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament"[13] As such the need has arisen for Cyber law.

Fourthly, "Internet requires an enabling and supportive legal infrastructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of Internet, can only be possible if necessary legal infrastructure compliments the same to enable its vibrant growth"[14]

Other cyber historian and cyber security expert analysis that "Cyber laws in India or cybercrime law in India are important because of the prime reason that cybercrime act in India encompasses and covers all the aspects which occur on or with the internet -_transactions, and activities which concern the internet and cyberspace. The rise of the 21st century marked the evolution of cyber law in India with the Information Technology Act, 2000 (popularly known as the IT Act). The first-ever cybercrime was recorded in the year

1820. The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic 17 Commerce on International Trade Law".[15] This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations, applicable to alternatives to paper based methods of communication and storage of information.

13. HISTORY OF CYBER SECURITY LAW IN INDIA

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. "It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft. After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members".[16] "The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to 18 be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000".[17] Department of electronic and information technology policy explain that "With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000. This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts".[18]

14. CYBER LAWS

Cyber crimes are a new class of crimes which are increasingly day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes.

14.1. CYBER SECURITY LAW IN INDIA

In India, cyber laws are contained in the Information Technology Act, 2000 (IT Act) which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The following Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001
5. National Policy on Information Technology 2012
6. National Cyber security Policy, 2013
7. National Cyber Security Coordination Centre (NCCC), 2017
8. Cyber Swachhta Kendra (2017)
9. Cyber Surakshit Bharat (2018)
10. Cyber Warrior Police Force (2018)
11. Indian Cyber Crime Coordination Centre (I4C), 2020
12. National Cyber Security Policy Mission 2020
13.
    (CERT-In) 2022

The various offences related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

A- Cyber Crimes under the IT Act

1. Tampering with computer source documents-Section 65

2. Hacking with Computer systems, Data alteration-Section-66
3. Publishing obscene information-Section-67
4. Un-authorised access to protected system Section-70
5. Breach of Confidentiality and Privacy-Section-72
6. Publishing false digital signature certificates-Section-73

B- Cyber Crimes under IPC and Special Laws

1. Sending threatening messages by Email- Section 503 IPC
2. Sending defamatory messages by Email- Section 499 IPC
3. Forgery of electronic records- Section 463 IPC
4. Bogus websites, cyber frauds- Section 420 IPC
5. Email spoofing- Section 463 IPC
6. Web-Jacking- Section 383 IPC
7. E-mail Abuse- Section 500 IPC

C- Cyber Crimes under the Special Acts

1. Online sale of Drug under Narcotics Drugs and Psychotropic Substance Act
2. Online sale of arms- Arms Act

15. NATIONAL CYBER SECURITY POLICY

The Department of Electronics and Information Technology has a policy framework called the National Cyber Security Policy (DeitY). It tries to defend both private and public infrastructure from online threats. Additionally, the policy aims to protect "information, including personal information (of site users), financial and banking information, and sovereign data."

15.1. National Cyber Security Policy Mission

1. To safeguard data and online information infrastructure.

2. To develop the skills necessary to stop and address online dangers.

3. To use institutional structures, people, processes, technology, and collaboration to limit vulnerabilities and lessen harm from cyber events.

15.2. National Policy on Information Technology 2012

The National Policy on Information Technology 2012 was recently adopted by the Union Cabinet in September 2012. In order to meet the nation's economic and developmental issues, the Policy strives to make use of information and communication technology (ICT).

15.3. National Cyber security Policy, 2013

The National Cyber Security Policy was created in 2013 as a response to the 2013 NSA eavesdropping scandal, which made India aware of the need for cyber security. Information may be divided into two categories: that which can be shared freely and that which has to be protected.

15.4. National Cyber Security Policy Vision, 2013

The goal of this policy is to create a resilient and secure cyberspace for individuals, organisations, and the government.

15.5. National Cyber Security Coordination Centre (NCCC), 2017

It was put into operation in 2017 and given the responsibility of doing real-time threat assessments and developing situational awareness of possible cyber threats to the nation.

15.6. National Critical Information Infrastructure Protection Centre (NCIIPC):

According to section 70A of the IT Act, the organisation was established. It is a national nodal agency for critical information infrastructure protection, and its mission is to defend critical information infrastructure (CII) from threats including cyber terrorism and cyber warfare. Power and energy, banking, financial services, insurance, communication, transportation, government, strategic, and public companies are all parts of the essential infrastructure.

15.7. Cyber Forensic Laboratory

The Cyber Forensic Laboratory and Digital Imaging Center aids law enforcement authorities in the gathering and forensic examination of electronic evidence in cases of cybercrime

15.8. Cyber Swachhta Kendra (2017)

It was released at the beginning of 2017 and offers a platform where users may analyse and purge malware, viruses, and other threats from their computers.

15.9. Cyber Surakshit Bharat (2018)

“Cyber Surakshit Bharat initiative was launched by the Ministry of Electronics and Information Technology (MeitY),in association with National e-Governance Division (NeGD) in 2018.It was launched with the objective of creating awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments”.[19]

15.10. The Cyber Warrior Police Force (2018)

In 2018, the government launched the plan to establish a cyber warrior police force. The idea is to model it after the Central Armed Police Force.

15.11. Indian Cyber Crime Coordination Centre (I4C), 2020

"The centre was inaugurated in 2020 by the Union Home Minister along with the National Cyber Crime Reporting Portal.I4C has seven major components National Cybercrime Threat Analytics Unit (TAU),National Cybercrime Reporting, Platform for Joint Cybercrime Investigation Team, National Cybercrime Forensic Laboratory (NCFL) Ecosystem, National Cybercrime Training Centre (NCTC),Cybercrime Ecosystem Management Unit, National Cyber Research and Innovation Centre".[20] National Cyber Crime Reporting Portal is a citizen-centric initiative that will enable citizens to report cyber crimes online.

16. NATIONAL CYBER SECURITY POLICY MISSION 2020

In order to reduce vulnerabilities and minimize damage from cyber incidents, this policy's mission is to protect information and information infrastructure in cyberspace. To achieve this, it combines institutional structures, people, processes, technology, and cooperation to build capabilities to prevent and respond to cyber threats. A new cyber security policy will be developed by the government in 2020 in response to the necessity for modifying the current policy due to changes in the ICT environment.

17. INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-In) 2022

The document outlines the scope of the Cyber Security Directions of April 28, 2022, issued by CERT-In pursuant to subsection (6) of Section 70B of the Information Technology Act, 2000, in order to improve understanding among various stakeholders and to advance the development of an open, safe, trusted, and accountable Internet in the nation. The Government is putting together a larger cyber security infrastructure to combat rising threats, and recently published Cyber Security Directions are just one component of that architecture. "Cyber Security Rules were already in place but they are around eleven years old. Over this period, size, shape & dimension of Internet has changed significantly. The nature of user harms and risks in 2022 are different from what it used to be a decade back. The perpetrators of cyber crime are both state and non state actors with sinister designs. Rapid & Mandatory reporting of incidents is a must and a primary requirement for remedial action for ensuring stability and resilience of Cyber Space".[21]

"The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area"[22] of cyber security:-

A. gathering, analysing, and disseminating data on cyber events;
B. forecasting and warnings of cyber security issues;
C. taking immediate action to address cyber security problems;
D. Coordination of the activities involved in responding to cyber incidents;
E. Publishing guidelines, advisories, vulnerability notes, and whitepapers about information security practises, procedures, and the prevention, response, and reporting of cyber incidents;
F. Any additional cyber security-related duties that may be required.

18. CONCLUDING REMARKS

It is cleared from the previous studies and records that with the increment in technology, cyber crime increases. Qualified people commit crime mores; there is a need to know about principles and computer ethics for their use in proper manner. Today in the technology age, where human civilization has achieved unlimited facilities and security in every field, it has provided more ease in the development of cyber technology. But anti humanitarian and anti-nationalist people gave birth to cyber crimes. Both human security and national are being threatened through cyber-crimes. The socio-economic, political and cultural spheres are being directly harmed by cyber criminals. Track the number of cyber crimes through the National Crime Records Bureau and other security agencies. These crime reports show that the numbers of cyber crimes are increasing day by day. Today India has become the second largest internet users' country in the world. The government of India is also making new laws from time to time prevent cyber crimes and punish cyber criminals. The government also agreed to cooperation on the international convention for the prevention of cyber crimes. The government's Ministry of Information Technology and Ministry of Law together made laws and policies to crack down on cyber criminals. In which the following important laws were passed like- Information Technology Act, 2000, National policy on information Technology 2012, National Cyber Security Policy 2013, Indian Computer Emergency Response Team (CERT-In) 2022 etc. The whole world stands together against cyber terrorism. There also a campaign against such criminals in which women and children are also harassed. The civil society and government need to work together to stop all such cyber crimes. The government should make some more laws and modify the sections of IPC and make new laws. So that criminals can be stopped cyber crimes. In the age of modern technology, the society of the nation is intertwined with cyber security. Therefore, without it the national security of any nation is not possible.

19. SUGGESTIONS

The following suggestions can be given that may be useful for dealing the cyber security challenges in India:

1. The people's participation can be of great help in combating cyber crime and cyber security.
2. A special cyber security Cell Station should be developed to handle cases dealing with computer offences.
3. A "Cyber Forensic Laboratory with all updated technologies should be endorsed to detect computer related crimes".[23]
4. Public Awareness Programmes should be carried out to sensitized public and particularly police officers about the "*National Cyber security Policy, 2013, National Cyber Security Policy Mission 2020,* Indian Computer Emergency Response Team (CERT-In) 2022".[24]
5. The security expert in educational institutions to spread awareness about computer abuse among students.

ACKNOWLEDGEMENT

I am expressing our sincere gratitude and thanks to Cyber security agencies and expert of this area for his valuable guidance, and support and kind co-operation during preparation of this research article and helping us in writing this review article successfully. I am also thankful to various Universities library like DU, JNU, NLU, NCRB resources and online reports to help for this article.

REFERENCES

1 Rather, M. A. & K. Jose (2014). "Human Security: Evolution and Conceptualization." European Academic Research, 2 (5): 6766–6797.

2 Kasture, Jyoti Pralhad, (2018), Cyber crime and related laws in India, *International Journal of Pharmacy and Analytical Research (IJPAR),* Vol-7(3) July – Sep

3 Badruddin and Anis Ahmad (*2017),* Cyber Security Challenges: Some Reflections on Law and Policy in India, *The Haryana Police Journal*,Volume 1 No. 1, October

4 Mali, Prashant, (2015), *Cyber Law & Cyber Crimes 2nd Edition*, Snow White Publication, Mumbai.

5 http://cybercrime.planetindia.net/intro.htm (Accessed on 4th February, 2016)

6 Chaubey, R.K. (2012) "An Introduction to Cyber Crime and Cyber law", Kamal Law House,

7https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users (Accessed on 3rd February, 2016)

8 Abraham D. Sofaer, Seymour E, (2001), The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press,

9 Abraham D. Sofaer, Seymour E, (2001), The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press

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

11 Cyber crime and it Classification, (2020) www.bbau.ac.in/dept/Law/TM/1.pdf

12 Indian Cyber Security, (2022), Cyber Laws in India, http://www.indiancybersecurity.com/ cyber_law_in_india.php

13 Indian Cyber Security, (2022), Cyber Laws in India, http://www.indiancybersecurity.com/ cyber_law_in_india.php

14 Indian Cyber Security, (2022), Cyber Laws in India, http://www.indiancybersecurity.com/ cyber_law_in_india.php

15 History of cyber Security law in India, 2022, http://www.indiancybersecurity.com/ cyber_law_history_india.php

16 Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, http://deity.gov.in

17 Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, http://deity.gov.in

18 Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, http://deity.gov.in

19 *Krishnan, Dolly & Mohit Verma,* (2020), Cyber security And Cyber Laws around the World and India: Major Thrust Highlighting Jharkhand for Concerns, *Indian Politics & Law Review Journal*, The Law Bridge Publishers, 20th July

20 *Krishnan, Dolly & Mohit Verma,* (2020), Cyber security And Cyber Laws around the World and India: Major Thrust Highlighting Jharkhand for Concerns, *Indian Politics & Law Review Journal*, The Law Bridge Publishers, 20th July

21 Ministry of Electronic and Information Technology, (2022), *Indian Computer Emergency Response Team (CERT-In) 2022*, Government of India, 18 MAY, PIB Delhi

22 Ministry of Electronic and Information Technology, (2022), *Indian Computer Emergency Response Team (CERT-In) 2022*, Government of India, 18 MAY, PIB Delhi

23 Badruddin and Anis Ahmad (2017),Cyber Security Challenges: Some Reflections on Law and Policy in India, *The Haryana Police Journal*, Volume 1 No. 1, October

24 Ministry of Electronic and Information Technology, (2022), *Indian Computer Emergency Response Team (CERT-In) 2022*, Government of India, 18 MAY, PIB Delhi

BIOGRAPHY

Dr. Sanjeev Kumar has completed his M.Phil and PhD in Central Asian Studies, School of International Studies, Jawaharlal Nehru University, New Delhi. Dr. Kumar's area of specialization in Non-Traditional Security like drug trafficking, terrorism, cyber security, Environment and National Security etc. He has more than 25 research papers and articles, 4 chapters contribute in edited book, 3 books, published in national and International publications from India and Abroad.