European Economic Letters
ISSN 2323-5233
Vol 14, Issue 1 (2024)
https://doi.org/10.52783/eel.v14i1.1220
http://eelet.org.uk

Combating Cybercrime: A Study on Problems, Preventions and Cyber Laws of India

Dr. Megha Ojha[1] & Dr. Rakhi Raturi [2]

1. Dr. Megha Ojha, Associate Dean (Research), IILM Law School, IILM University, Gurugram, India e-mail: megha.ojha@iilm.edu; medhasango@gmail.com
2. Dr. Rakhi Raturi, Assistant Professor, School of Commerce, NMIMS (Deemed-to-be University), Navi Mumbai, India, e-mail; rakhi.raturi@nmims.edu; rakhi2808@gmail.com

Abstract

Cyberspace is a complex and dynamic network of people, software, and service interactions. The significant rise in the internet users around the world has brought with it a peculiar set of problems. Evidence of illegal digital activity is frequently trapped in large volumes of data all of which are challenging to detect or to report evidences of crimes. In the majority of nations, cybercrime has become a global epidemic and a difficult social problem. Cybercriminals are technically adept and employ a range of deceptive techniques to dupe individuals, corporations, and even the government. As the frequency and severity of cyberattacks continue to rise on an annual basis, states and international organizations are attempting to mitigate the resulting damage and to also enhance cyber security. In the light of the preceding facts, this chapter focuses on the understanding of cybercrimes, the global and Indian cybercrime scenario, and the legislative measures implemented so far. It would also highlight the empirical evidence of the various cybercrimes reported by the government in India. The chapter strives to build an understanding of the issue from the global and national perspective and put forth some insights for combating cybercrimes.

Keywords: Technology, Cyber-crimes, Statistical analysis, Global and Indian trends, Motives of cyber-crime, Cyber laws, International and national agencies

1. Introduction

There is a massive amount of data which is shared and created in the digital space. However, information on the Internet is not immune to unauthorized access or harm. The technological revolution has expanded the internet users' capabilities and reach, but it has also given birth to a high-tech cybercrime scenario on a global scale. Cybercrimes pertain to illegal activities against individual or groups of individuals with a criminal intent to cause bodily or mental harm, or a financial theft, to the victim directly through the use of the Internet (Saroha, 2014). Cybercriminals are similar to the terrorists who also create unfair economic and social impact on nations through their criminal operations. Internet is comparatively a safer bet for criminals to conduct their activities and launch assaults while keeping a certain degree of anonymity. Due to this internet anonymity, criminal minds can indulge in various criminal incidents. These cybercriminals target social and professional networks, and mobile platforms such as smartphones and tablets and bring harm personally or financially (Chouhan, 2014). These criminals may not belong to a single city or a nation, and it is difficult for authorities to conduct investigations and bring justice. Cybercrime is universal in nature whereas traditional crimes such as theft and robbery are local and their legal controls could be handled by the established book of law. It is recommended that greater resources be allocated to cybercrime response, or the process of finding and incarcerating cybercriminals, rather than less resources being allocated to cybercrime prevention like antispyware or firewall (Ross Anderson, 2013).

1.1. Covid and the surge in cybercrime

During Covid-19, as corporations were allowing the work from home options, cybercriminals used this as an opportunity of excessive use of internet to steal sensitive information, make money, and create issues. According to an INTERPOL assessment on global cybercrime during COVID-19, hackers shifted their focus from individuals and targeted small and medium enterprises, government, and key infrastructure businesses. Their investigations found around nine lakhs spam messages, malware occurrences, and approximately fifty thousand harmful URLs linked with COVID-19. In African countries, as the cashless payments increased in pandemic and their public awareness was low about payment gateways, there were incidences of various financial frauds. The charity scams and sextortion were also reported. In United States, hackers tried to get remote access to corporate network to steal sensitive data. In several locations, a ransomware campaign led primarily by LOCKBIT virus targeted medium-sized businesses. The trade trafficking of images involving child sexual exploitation increased. In Asian countries, cybercriminals exploited flaws in the security of teleconference technologies to steal data. There have also been reports of an increase in the cloning of official government websites to acquire sensitive user data that can be utilized in future hacks. Europe reported a considerable spike in the number of fraudulent sites created with the keywords 'COVID' or 'Corona' in an attempt to earn from the increasing number of people seeking online help for COVID-19. Major crimes related to technology as reported by INTERPOL in 2019 were as follows:

- Fraudsters used COVID-19-themed phishing emails to trick victims into giving personal information and downloading malware.
- Malware targeted critical healthcare facilities
- Cybercriminals used COVID-19-related material as bait to breach systems, attack networks, steal data, and build botnets.
- Domain name registrations containing "coronavirus" or "COVID" spiked. Such fraudulent websites facilitated malware dissemination and phishing. (INTERPOL Cybercrime: COVID-19 Impact, 2020)

2. Background

2.1 Definition of Cybercrime and its types

Cybercrime is in its infancy, and with each passing day, new forms of illegal conduct in cyberspace acquire significance. Cybercrime and cyberattacks are not defined internationally. According to the United Nations, transgressions frequently fall into the following categories:

a) Violating the privacy, availability, and integrity of computer data and systems;
b) breaking laws about computers; c) breaking laws related to content; and d) breaking laws about copyright and related rights.

Even though we cannot arrive at a unifying definition of cybercrime, the term is used to explain a number of crimes and destructive actions. David Wall defined cybercrime as "harmful behaviour associated to a computer (Wall, 2001)." Cybercrime can be judged as the "illegal or illicit computer-mediated actions undertaken across worldwide electronic networks (Barrett, 2001)." It is important to distinguish between 'cyber-enabled' and 'cyber-dependent' crimes. Hacking and spyware attacks are examples of cyber-dependent crimes. These are crimes that started with technology and cannot happen outside of the digital world. Cyber-enabled crimes are not new, but technology makes them easier (Kirsty Phillips, 2022).

According to (Biswal & Pani, 2021), following are some of the technical cybercrime attacks which criminals are indulging in:

1. **Credit card hacking & skimming:** Usually, hackers call random individuals pretending to be bank employees or authorized credit card agents in order to obtain their personal information. They warn the victims that their bank account or credit card would be revoked, if they fail to provide the details about their account or card. With financial information such as Card number and CVV number, a hacker is able to quickly make any online purchase. Typically, thieves install skimming devices at posh retail centres and ATMs.
2. **Juice Jacking:** As part of "juice jacking," a sort of cyberattack, USB cables are used to send data and install malware on victims' phones. This is possible if you swap out your phone while using public charging stations in restaurants, public transport areas, utility places etc. There are USB charging ports in these public locations that can steal information, duplicate phone's data, and discreetly install malware on devices. Any computer or Mac can access the data clone of the phone. Photographs, films, and other media would also be accessible to the hacker.
3. **MITM (man in the middle):** It is an attack that occurs when a hacker or third-party hijacks communication between two parties. Instead of client and server communicating directly, a third-party element disrupts the connection.
4. **Vishing:** In Vishing, hackers and spammers usually contact potentially susceptible individuals while pretending as authorized representatives of legitimate businesses. In the telephonic conversation, they seek to gather private user information.

5. **Session Hijacking:** Session hijacking is when an anonymous hacker takes control of a legitimate session between a client (user) and server (often a Webserver).
6. **DOS attack:** A hacker attempts to get access to a server, or any other internet device by and generates a massive strain on the server until its resources are drained, hence making the server or service unusable to actual users.

The cybercrime can be the crime targeted against an individual, or against property or against Government:

Table 1. Types of Cybercrime

cybercrimes against person	• Computer-based harassment, impersonation, privacy invasion, online victimization, and cyberstalking. • Selling illicit goods online or via emails, such as selling illegal drugs, guns, or wildlife. • Email spoofing, job fraud, matrimonial fraud, etc. • Cyber-defamation, and cyber-pornography (obscene material being transmitted via pornographic websites and pornographic websites). • Hacking
Cybercrimes against property	• Credit card fraud or laundering of money, etc. • Unauthorized computer access • Computer vandalism • Forgery • Transmission of malicious programs • Intellectual Property related Crimes **-** piracy, copyright related infringement, trademark infringement, and stealing of computer source code.
Cybercrimes against government	• Hacking into official websites • Cyber extortion • Cyber terrorism • Computer malware
Other cybercrimes	• Logic bombs • Computer viruses; spam; email abuse; email bombing etc.

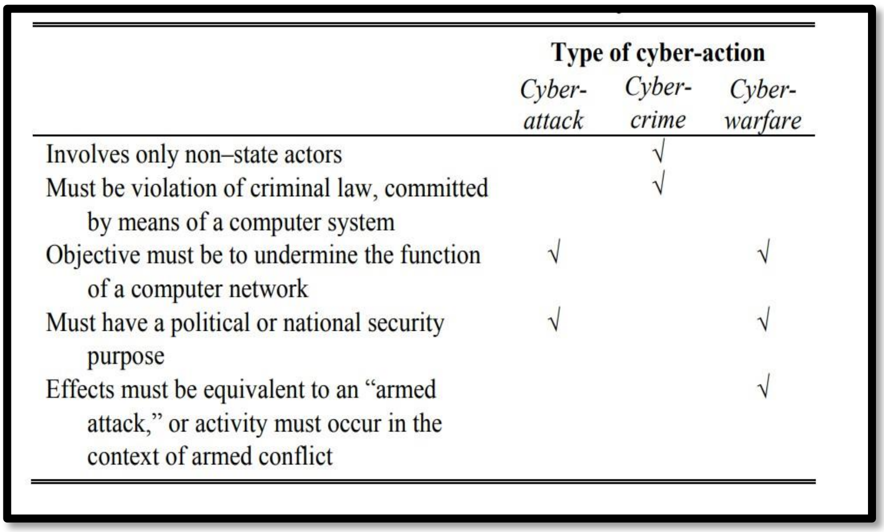
Source: Author's compilation

2.2. Dynamics of cyber threats with respect to international policy

The majority of important infrastructures and processes are connected to the Internet, which makes cyberattacks a threat to national security. As a result, cyber threat is increasingly seen as a severe security concern for industry and business. Criminologists have emphasized the need to study the causes and motives behind frauds against clients if it needs to be controlled. In many economies, inadequately punitive sanctions, inadequate & weak legislation have further fuelled cybercrime. Apparently, unknowingly sometimes, even prominent businesses have either sponsored or promoted the growth of cybercrimes. It might be said with remorse that commercial sectors have no incentive to prevent spam because doing so would diminish their profits. Two major hubs of cyber-crime activities are related to the regions of Russia and Europe. Both these regions are high on criminal linkages. Secondly, cybercriminals in these economies seek those illicit internet models that allow quick monetization. Cybercrimes involving fictitious social networking profiles are also monetized. In Armenia, criminals use Social Networking profiles to transmit pornographic information. Later on, they charge the victims or blackmail them to broadcast the pages. There is a different trend for Indian and Middle Eastern cybercriminals who build false social media profiles more to defame the victims and less on monetary levels (Kshetri, 2016).

There are some old incidents of fraud which highlights how nations were easily succumbed to cyber operations. In 2010, the FBI's cybercrime operations, busted a multinational gang that stole big amount of money from small businesses and local governments using Zeus. Arrests were made in multiple countries, including few operating from the United States. The bulk of those sentenced were international students who acted as "cyber-mules." These pupils performed well in math and computer science. If the countries are too small to absorb the present talent, then educated young may be attracted to participate in illegal internet businesses that provide rapid riches. There were other instances in which lawfully employed persons saw cybercrime as an attractive way to make extra money. Similarly leading technology company, Microsoft reported that their former employee of an antivirus software company was suspected of writing or creating the 'Kelihos' botnet in 2012 (related to bitcoin theft). However, now countries like Russia are implementing stricter rules with internet. Businesses seeking to register the domain must provide copies of their passports or legal registration documents, according to the new restrictions. Prior to the implementation of this regulation, domains were created without any scrutiny (Kshetri, 2013). The international banking operations are also hampered by an increase in online frauds. By bypassing bank safeguards, fraudsters manipulate and compel clients into making payments to them (Global Banking Fraud Survey, 2019). Although a decade has passed, the incidents of cybercrimes are increasing rapidly. Leaders and policymakers should be relentless in ensuring that technology should be used for development and not for crimes.

Table 2. The extent of cyber-crime with respect to national security



	Type of cyber-action		
	Cyber-attack	*Cyber-crime*	*Cyber-warfare*
Involves only non–state actors		√	
Must be violation of criminal law, committed by means of a computer system		√	
Objective must be to undermine the function of a computer network	√		√
Must have a political or national security purpose	√		√
Effects must be equivalent to an "armed attack," or activity must occur in the context of armed conflict			√

Source: (Oona A. Hathaway, 2012)

Although there are no physical boundaries on the Internet, certain information may be prohibited. Both the website host and the access provider have the power to prohibit access to specific websites and IP addresses, respectively. Controlling information has, for instance, always been vital in military battles since it may have an impact on both the civilian population and the enemy nation. Information control over the Internet becomes increasingly important in such a situation.

2.3. Need of collaboration by international and regional organizations in the fight against cybercrime

Cybersecurity must thus be integrated into all of our efforts. This also has national and global security ramifications. Cisco estimated that there were around 200 million Internet-connected devices in the year 2000, with this figure expected to increase to 10 billion by the year 2013. In present scenario, the Internet of Everything, a mix of machine-to-machine (M2M), person-to-machine (P2M), and person-to-person (P2P), will fuel the next wave of Internet development (IoE). With this technical development comes an equivalent amount of cyber risk (Parasol, 2018). Thus, cybercrime investigations require the international cooperation when perpetrators and victims reside in different nations. National sovereignty prohibits conducting investigations in other nations without the authorization of local authorities. In nations with inadequate cybercrime rules, criminals may target victims outside of their own country. Consequently, all relevant countries must assist Cybercrime investigations (White, 2020). Cyber security regulations require businesses and organizations to secure their systems and data against cyber-attacks viruses, phishing or illegal access etc.

According to the Global Cybersecurity Index 2020 recent reports, the United States is the most secure and equipped to tackle hackers and followed by the United Kingdom and Saudi Arabia. Germany ranks thirteenth while Russia ranks sixth (Cyber Crime & Security, 2022). With the exception of the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection, international law does not govern cyberspace. Most governments and global entities, like the United Nations General Assembly's First Committee on Disarmament and International Security, the G20, the EU, ASEAN, and the OAS, feel that how states use ICTs is governed by international law (ICTs). Even in terms of punishment, there is a significant disparity: cybercrime in the United States can result in up to twenty years' prison, life prison, or the death penalty, but in Germany it is penalised by regular detention and/or a fine.

In 2020, cybercrime against British businesses increased by twenty percent despite the Computer Misuse Act and the revised Data Protection Act. In response to cyberattacks, Russian insurers frequently educate workers or modify policies. In Russia, cybercrime can have a punishment of maximum ten years' jail, community service, or a penalty fee. Germany has the least severe cybercrime punishments, whereas the United States has the most severe legal enforcements. The United States' cyber security laws and privacy system is considered the most robust in the world. The State's privacy regime relies mostly on ad hoc government enforcement and private litigation. Information technology and computer systems are now secured by directives from the Executive Branch and cyber security regulations from Congress. As early as 2003, California enacted the Notice of Security Breach Act, which requires companies that keep the individual data of residents and if there are chances of breach, it had to be notified with due diligence. The security breach regulations penalize businesses for cyber security failures while allowing them to determine how to defend their systems. This rule incentivizes organizations to invest proactively in cyber security in order to avoid future reputational and economic loss (Yuriy Timofeyev, 2022).

Even in the most liberal nations, restrictions and laws govern the application of principles of free speech, notwithstanding the significance of safeguarding it. There are certain hate groups against certain entities or person who use email and social media post to spread social unrest through malicious messages. Such activities can also be posted as video content on platforms such as YouTube. Not all countries have criminalized these actions or are capable to control such public activities on internet. Sometimes such control questions the extent of the freedom of expression principle. It is advisable for countries to resolve such issues through their diplomatic efforts and to create discussions in the Convention and make it truly worldwide. The safe and secure development of Smart Cities and related technologies depends on the Cyber Security Law. According to estimates from the Chinese government from 2017, the country has almost seven hundred million internet users. Additionally, six hundred million people use mobile devices to access the internet. They depend on China's internet, e-commerce, payment, and shipping infrastructure and seldom ever use cash. In countries that provide safe havens yet lack or have inadequate cybercrime laws to abide with extradition demands, cybercriminals often seek asylum. Additionally, since many extradition agreements have a "double criminality" provision, a suspect may only be sent from country A to country B to receive justice for breaking its laws if the country extraditing him or her also has a law that punishes the same behaviour. If cybercrimes are not criminalized in certain nations or if the applicable laws do not correspond with the investigating governments, cybercriminals are free to roam and spread malice (Hakmeh, 2017).

There are different points of view on the present balance between national and international cybercrime enforcement. Despite the existence of a number of international treaties to combat cybercrime, these treaties do not meet the needs of all governments. The Budapest Convention on Cybercrime is the primary international law treaty governing government-to-government contacts in cyberspace. Their agreement states that governments must go above and above to punish cybercrime in line with their own national laws (Kittichaisaree, 2017). China, India, and Russia all rejected the declaration because they were not involved in its preparation and because certain of its wording posed a threat to national sovereignty in terms of transnational access to information and data (Yuriy Timofeyev, 2022).

2.4. Eminent International Cyber Law enforcement authorities

Since cybercrime transcends international borders, and it is a worldwide danger. The security of digital data and information systems and the prevention of the negative use of information and communication technology by cybercriminals, terrorist organizations, or state actors are the two most important issues facing the information society. The term "cyber security" was created as a consequence of efforts made to remedy these security flaws in the information society. In accordance with Resolution 65/230 of the General Assembly and Resolutions 22/7 and 22/8 of the Commission on Crime Prevention and Criminal Justice, the Global Programme on Cybercrime is intended to support Member States in addressing cyber-related crimes through capacity development and technical support. In 2002, the Commonwealth of Nations produced a model cybercrime legislation to unify regulation and stimulate international collaboration. The sample law is modelled by the Convention on Cybercrime. The group in charge of China's anti-spam program is developing standards and better techniques to combat cybercrime. ISPs must engage consumers successfully in order to decrease spam. Many regulatory agencies have failed to properly combat cybercrime, and even in the most technologically advanced countries, hackers are becoming stronger (Nweze-Iloekwe, 2022).

The Council of Europe's Cybercrime Convention is made for a specific goal, and even though it is a regional process, it affects the whole world. The United Nations (UN) Convention against transnational organized crime has a global scope and indirectly encompasses cybercrime when it is done by criminal networks in connection with serious crimes. At the 58th session of the General Assembly (GA) in 2003, Argentina, Bulgaria, Canada, Ethiopia, and the United States co-sponsored a UN resolution called "Cybersecurity and the protection of critical information infrastructures." This resolution encouraged Member States and other relevant international organizations to consider the need to safeguard crucial information systems against potential abuse, including tracking assaults and, where necessary, information dissemination. Terrorists use computers to plan, coordinate, and talk, and counter-terrorism officials have often found high-tech tools like cell phones, satellite phones, and the Internet being used by terrorists. Also, hackers, thieves, and corrupt officials have gotten their hands on important information about law enforcement. The fact that terrorism can happen anywhere in the world led the United Nations General Assembly to emphasize in resolution 51/210 that terrorists could use electronic or wired communication networks to commit crimes (Broadhurst, 2006). Other international organizations concerned with cyber security:

a) The UNODC Global Programme fights cybercrime in Central America, Eastern Africa, MENA, and Southeast Asia.
b) ENISA: it is EU-backed and helps with cyber policies and certification.
c) European Cybercrime Centre (Hague): aids EU nations with international crime and terrorism.
d) National Cyber Security Centre: guidelines to respond to UK cyber events.
e) Cyber Security & Infrastructure Security Agency (US): reduces cyber violence and terrorism.
f) INTERPOL (Singapore): worldwide cybercrime body. Uses law enforcement and private cyber-expertise.
g) NATO Cooperative Cyber Defence Centre: Cybersecurity teaching, counselling, research, and development.

156 countries, according to the UN, have cybercrime legislation in place; Europe has the highest adoption rate while Africa has the lowest (Cybercrime Legislation Worldwide, 2021). Law enforcement and prosecutors are concerned about the changing nature of cybercrime and the resulting skills shortages, particularly when enforcing laws across borders (Global Programme on Cybercrime).

2.5. Cybercrime control mechanisms in India

In the recent decade, cybercrime in India has grown significantly. In the first three months of 2020, India was the target of 3.3 million cyberattacks (Shivani Shinde, 2021) Indian government cyberattacks cost the government Rs. 1.25 lakh crore yearly, according to the Economic Times (PTI, The Econimic Times, 2020). With more than five hundred million Internet users, Indians are the second-largest online population in the world. By 2023, it is predicted that there will be more than six hundred million internet users in the nation (Mandavia, 2019). By 2020, India will have recorded more than fifty thousand incidences of cybercrime, according to the most current NCRB statistics (PTI, The Hindu, 2021). To satisfy international cyber security standards, India requires a robust system, a solid legal framework, and real policy initiatives. Without this, India is unable to combat cybercrime.

It is part of the Indian Government's Ministry of Home Affairs. With a projected budget of 415.86 crore, the plan was approved in October 2018. In India, owing to effort/initiative of the government, a website/web portal (*https://cybercrime.gov.in*) is accessible for the victims and complainants to report cybercrimes online. Though the webpage/portal is for reporting cybercrime complaints only, and should not be considered a FIR. Complaints filed using the website are the responsibility of the appropriate State or UT authority. Customers are encouraged to ensure the veracity of any information they put on the site before submitting a complaint. It is made mandatory for the police department of each State and Union Territories to investigate complaint using the information provided by the complainant on the portal/website. Cyber-crime complaints are exclusively accepted here, with an emphasis on offenses against women and minors. Reports made on this site are handled by police and other law enforcement organizations depending on the information provided in the reports. Correct and precise information must be provided when making a complaint in order for it to be handled quickly. According to the National Cyber Crime Reporting Portal, the cybercrimes rates in India is increasing in its reach as well as number of incidents reported *(National Cyber Crime Reporting Portal)*

3. Methodology & Data Source

Since IT and technology-dependent industries are so diverse, finding a clear and unified view of cyber-crime has become imperative because of this. CERT-In, the National Informatics Centre, the National Critical Information Infrastructure Protection Centre (CERT- In); the Ministry of Home Affairs, and the National Crime Records Bureau all contributed important insights in this area. Researchers used data from the National Crime Records Bureau (NCRB) on different features and incidences of digital-based crimes in India for statistical research. We chose India's most susceptible States and five major urban areas based on cybercrime cases registered under the Indian Penal Code, the Information Technology Act, and other SLL. As new risks and best practices arise in India's cyberspace, this chapter is expected to evolve and be amended accordingly. We studied and analysed the existing cyber security framework and reinforce how a centralized law enforcement approach is the only tactic to combat the internet black market of cybercrime.

3.1 Statistical Information on Cybercrime Offences in India

Table 3 reflects the alarming rate at which the cybercrimes are increasing in India. Also, many of the cases remain unreported because of the lack of awareness among the cyber victims.

Table 3. Number of cybercrimes registered in India (Year 2012 to 2020)

YEAR	2012	2013	2014	2015	2016	2017	2018	2019	2020
CASES REGISTERED	3,377	5,693	9,622	11,592	12,317	21,796	27,248	44,735	50,035

Source: Compiled by authors from NCRB Reports (Year 2012-2020) (Bureau, 2021)

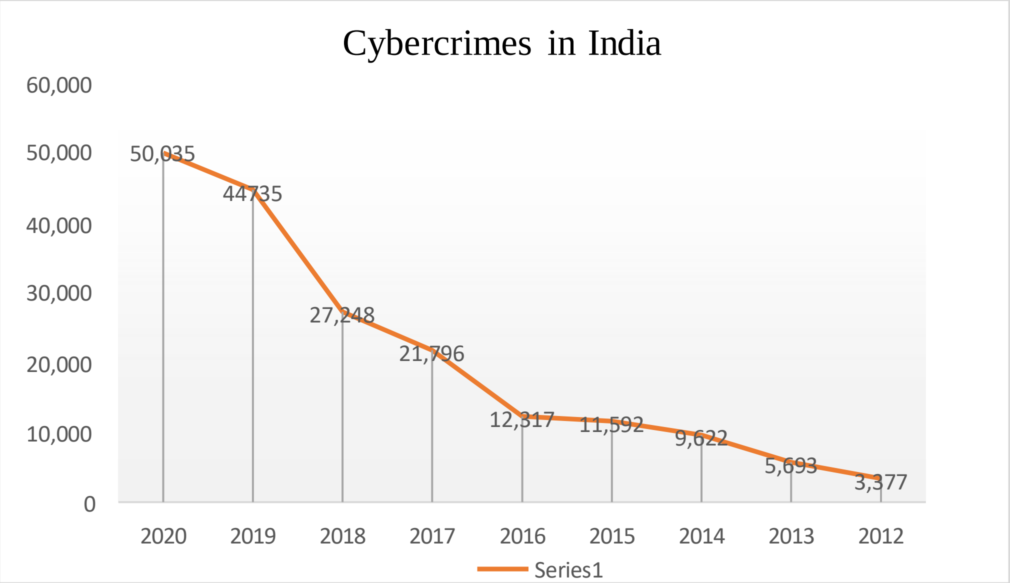


Fig. 1 Rise of cyber-crimes in India. *Source***:** author's graphical representation based on NCRB Reports (Bureau, 2021)

3.1.1 Cybercrime reported under the Information Technology Act, 2000

The most common types of crimes, in terms of frequency, are fraud and cheating. This reveals that people require adequate supervision to protect their privacy and financial transactions since they are too naive and uninformed of certain activities.

Table 4. Cases registered under Information Technology Act 2000 (Year 2018-2020)

Sr.	Crime Heads under I.T. Act 2000	Cases Registered (Year)		
		2018	2019	2020
1	Altering electronic source documents (Sec. 65)	257	173	338
2	Crimes involving computers (Sec. 66)	3969	4447	4557
3	Stolen computer or communication equipment (Sec.66B)	391	558	288
4	Identity Theft (Sec.66C)	6688	12255	5148
5	Cheating by personation by using computer resources (Sec.66D)	2704	5520	11191
6	Breach of privacy (Sec.66E)	389	812	742
7	Cyber Terror (Sec. 66F)	21	12	26
8	Electronic publication/transmission of obscene /sexual content (Sec. 67)	3067	4187	6308
9	Interception or Monitoring or decryption of Information (Sec.69)	6	9	7
10	Unauthorized access/attempt to access protect-ed computer system (Sec.70)	0	2	2
11	Abetment to Commit Offences (Sec.84 B)	1	0	1
12	Attempt to Commit Offences (Sec.84C)	13	14	18
13	Other Sections of IT Act	980	2720	1017
	Total Offences under I.T. Act	**18495**	**30729**	**29643**

*Source***:** Compiled by authors from NCRB Reports (Year 2018-2020) (Bureau, 2021)

3.1.2 Cybercrime reported under the Indian Penal Code

Table 5. Cases registered under the Indian Penal Code (Year 2018-2020)

Sr.	Crime heads under the Indian Penal Code	Cases Registered (Year)		
		2018	2019	2020
1	Incitement to Commit Suicide online (Sec.305/ 306 IPC)	7	8	10
2	Cyberstalking, cyberbullying, and the victimiza-tion of women and children (Sec.354D IPC)	739	777	872
3	Data stealing (Sec.379 to 381)	106	285	98
4	Fraud (Sec.420 r/w Sec.465, 468- 471 IPC)	3353	6233	10395
5	Cheating (Sec.420)	2051	3393	4480
6	Forgery (Sec.465, 468 & 471)	260	512	582
7	Defamation/morphing (Sec.469 IPC r/w IPC and IRWA)	18	19	51
8	Fake Profile (with SLL and IPC)	78	87	149
9	Counterfeiting	2	5	9
10	Cyber threats and Blackmail (Sec.506,503,384 IPC)	223	372	303
11	Misinformation on social media (Sec.505)	97	190	578

12	Others crimes (r/w I.T. Act)	1713	1849	2674
	Total Offences under IPC	**8647**	**13730**	**20201**

Source: Compiled by authors from NCRB Reports (Year 2018-2020) (Bureau, 2021)

3.1.3 Cybercrime reported under SLL

The Gambling Act need revalidation especially with the advent of 5G technology. The users are sure to lose money if these gambling platforms are not scrutinised as per law.

Table 6. Offences under SLL *(Involving Communication Devices as Medium/Target) r/w IT) (Year 2018-2020)*

Sr.	Offences under SLL (Involving Communication Devices as M edium/Target) r/w I.T.	Cases Registered (Year)		
		2018	2019	2020
1	Gambling Act (Online Gambling)	20	22	63
2	Lotteries Act (Online Lotteries)	2	9	26
3	Copy Right Act, 1957	62	34	49
4	The Trade Marks Act of 1999.	0	0	5
5	Other Crimes	22	22	48
	Total	**106**	**87**	**191**

Source: Compiled by authors from NCRB Reports (Year 2018-2020) (Bureau, 2021)

3.1.4 Motives for Cybercrimes

Hacking, child pornography, cyberstalking, denial of service, malware, phishing, and information warfare are among the many cybercrimes that have been recorded. The motives range from monetary gain, personal gain, victim harassment etc. to the system sabotage, data theft and information warfare. The majority of fraud cases in this country involve money.

Table 7. Cybercrime Motives (2017-2020)

Sr.	Cybercrime Motives	Cases Registered (Year)			
		2017	2018	2019	2020
1	Personal Revenge	628	794	1207	1470
2	Anger	714	461	581	822
3	Fraud	12213	15051	26891	30142
4	Extortion	906	1050	1842	2440
5	Disrepute	1002	1212	1874	1706
6	Prank	321	296	1385	254
7	Abuse or Exploitation	1460	2030	2266	3293
8	Political Motive	139	218	316	356
9	Terror Activity	110	44	199	113
10	Inciting hatred against nation	206	218	49	106
11	Disrupt Public dealing or service	55	21	28	165
12	Sale of illegal Drugs	8	6	10	92
13	Creating one's own business	156	198	181	21
14	Spreading Piracy	90	671	45	210
15	Psychopath or Deviant activity	17	4	1	0
16	Stealing Information	10	16	93	62
17	Abetment to Suicide	5	2	0	0

18	Others	3756	4956	7578	8814
	Total	**21796**	**27248**	**44546**	**50035**

Source: Compiled by authors from NCRB Reports (Year 2017-2020) (Bureau, 2021)

3.1.5. State -wise and city-wise Cybercrimes reported in India

Table 8. State-wise statistics of Cybercrimes reported cases *(Top 10 Indian States*)

Indian States	Cases Registered (Year 2017-2020)			
	2017	2018	2019	2020
Karnataka	3174	5839	12020	10741
Uttar Pradesh	4971	6280	11416	11097
Maharashtra	3604	3511	4967	5496
Telangana	1209	1205	2691	5024
Rajasthan	1304	1104	1762	1354
Assam	1120	2022	2231	3530
Odisha	824	843	1485	1931
Jharkhand	720	930	1095	1204
Bihar	433	374	1050	1512
Madhya Pradesh	490	740	602	699

Source: Compiled by authors from NCRB Reports (Year 2017-2020) (Bureau, 2021)

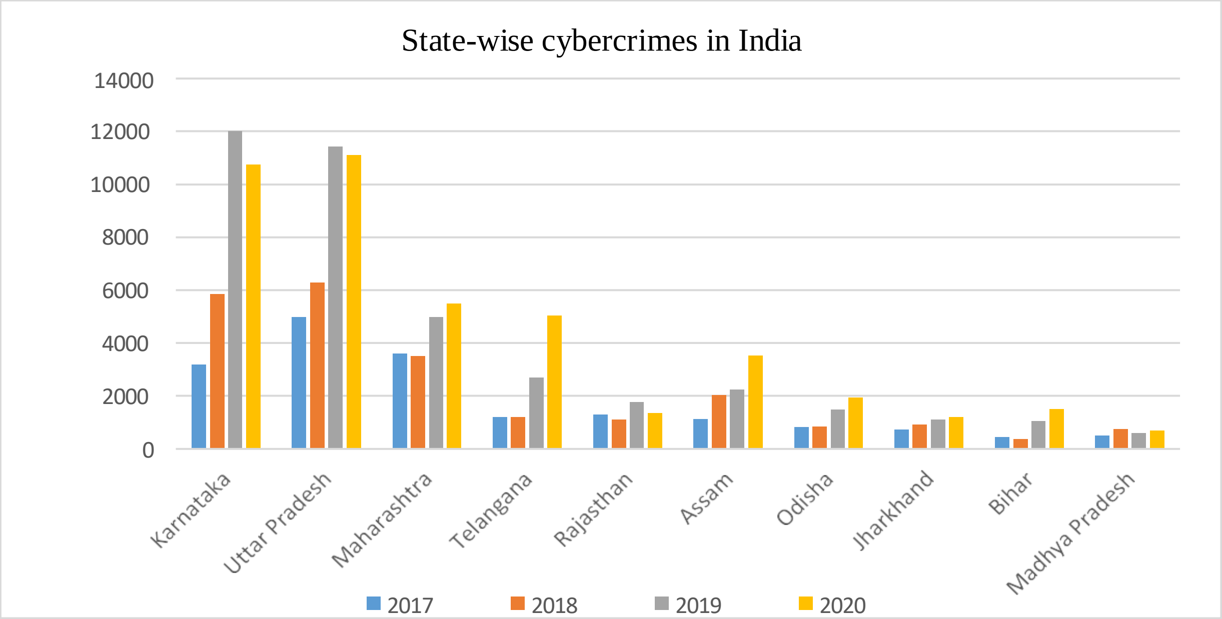


Fig. 2. State-wise incidents of cybercrime in India. *Source*: Author's graphical representation based on NCRB Report (Bureau, 2021)

Table 9. Cybercrimes in Metropolitan Cities (*Top 5 Cites of India)*

Indian States	Cases Registered (Year 2017-2020)			
	2017	2018	2019	2020
Bengaluru	2743	5253	10555	8892
Mumbai	1362	1482	2527	2433
Hyderabad	328	428	1379	2553
Lucknow	608	962	1262	1465
Jaipur	685	415	544	192

*Source***:** Compiled by authors from NCRB Reports (Year 2017-2020) (Bureau, 2021)

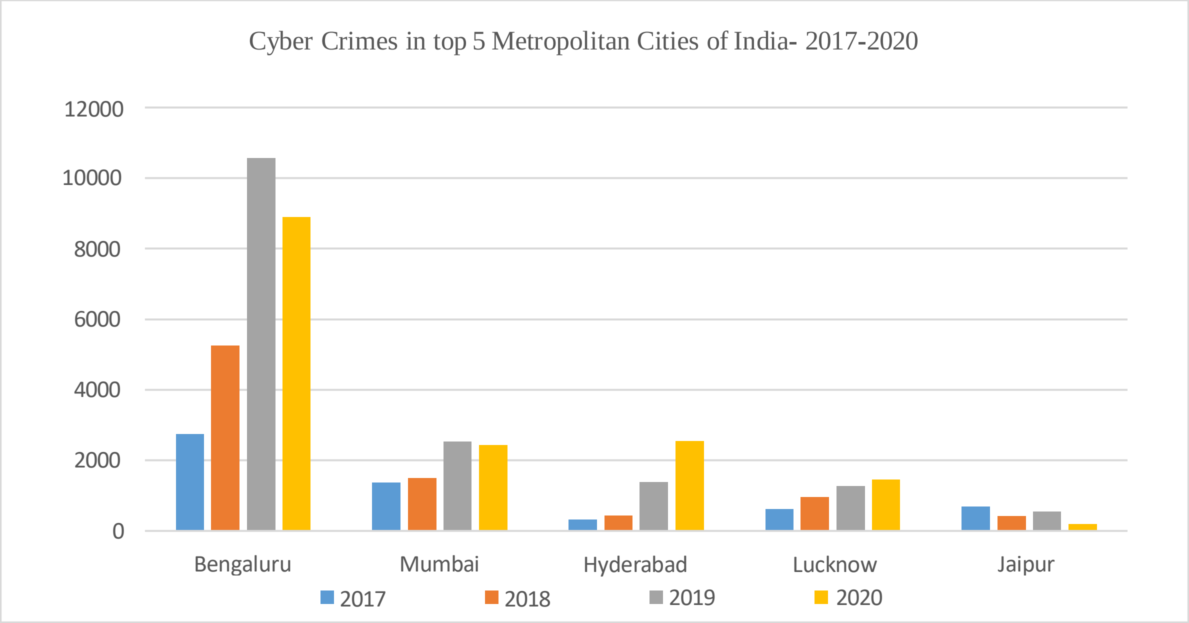


Fig. 3. Cybercrimes reported in Top 5 Metropolitan cities of India. *Source*: Author's graphical representation based on NCRB Report (Bureau, 2021)

3.2. Prosecution of cybercrimes in India

All Internet users must adhere to cyber law. India's capacity to battle cybercriminals has been enhanced by cyber legislation. Information Technology Act was enacted in 2000. (indiacode.nic.in). The Information Technology Act of 2000 legitimizes electronic documents and signatures. The Act controls certifying companies for digital signatures. The Act creates civil and criminal punishments for violations. It also permits the Central Government to select an Adjudicating Authority to determine whether a person has violated the law. The I.T. Act of 2000 has three objectives. First, the legalization of electronic commerce. Second, to facilitate electronic filing with the government. Third, modify the Indian Penal Code from 1860 and the Indian Evidence Act from 1872. However, this Act was the topic of numerous disputes, reviews, and complaints, with one side of the business alleging that certain sections are very stringent and the other claiming that it was too lenient.

Amendment Act 2008**:** Industry organizations were approached to analyze the I.T. Act’s claimed shortcomings, compare it to comparable legislation in other countries, and recommend revisions. The I.T. Act 2000 up to certain extent failed to combat cybercrime in India and thus the Information Technology (Amendment) Act 2008 was passed on October 27, 2009. The amendment included all modern communication devices. The Information Technology (Amendment) Act of 2008 protects e-governance, e-banking, and e-commerce.

Table 10. Cyber offences under the I.T. Act 2000 and the respective punishments.

Sections	Offences	Punishment & Penalties
Section 43	Computer or computer system damage	Damages to the victim.
Section 65	Tampering with the computer source	3 years in jail, a Rs 2 lakh fine, or both
Section 66	Other offences	3 years in jail, a Rs 5 lakh fine, or both
Section 66A	Sending insulting texts, etc.	3 years in jail, fine
Section 66B	Receiving stolen computer resource or communication device	3 years in jail, Rs 1 lakh fine, or both
Section 66C	Using a person's passwords, digital signatures, biometric thumb imprints, or other identifying attributes for fraud.	-do-
Section 66D	Computer-aided impersonation.	3 years in jail, Rs. 1 lakh fine, or both
Section 66E	Privacy infringement	3 years in jail, Rs. 2 lakh fine, or both
Section 66F	Cyber terrorism	Possibility of life imprisonment.
Section 67	Electronically distributing obscene material.	Three years in jail and a Rs. 5 lakhs fine. Second conviction: 5 years in jail, Rs.10 lakh fine
Section 67A	Publishing or transmitting of material containing sexually explicit act, etc., in electronic form	Five years in prison and a fine of up to 10 lakh rupees; seven years and 10 lakh rupees for a second conviction.
Section 67B	Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.	-do-
Section 72	Breach of Confidentiality and Privacy	Two years or a Rs 1 lakh fine, or both.
Section 72A	Any individual, including an intermediary, who breaches a legal contract	Three years or a Rs 5 lakh fine, or both.
Section 73	Publish forged electronic signature Certificates	Two years or a Rs 1 lakh fine, or both.

Table 11. Cybercrimes in India and their punishment under Indian Penal Code

IPC Sections	Offences	Punishment & Penalties
Section 292	Sale of indecent literature, etc.	Two years in jail, Rs. 2,000 fine. Second conviction: 5 years in jail, Rs 5,000 fine
Section 379	utilizing stolen mobiles/computers or stolen data	Three years in jail, fine, or both.
Section 383	Extortion – It may include web-jacking	-do-
Section 420	Cheating and dishonestly inducing delivery of property. - cybercrimes like creating bogus websites, cyber frauds are punishable under this section	Seven years in jail, fine
Section 463	Forgery of electronic records - crimes such as making false documents or false electronic records are punishable under this section.	Imprisonment up to two years or fine or both
Section 468	Forgery for purpose of cheating - email spoofing is one such cybercrime punishable under this section.	Imprisonment up to seven years and fine.
Section 499	Sending defamatory messages by email	Imprisonment up to two years or fine or both.
Section 503	Email criminal intimidation	-do-

Source: Author's compilation based on the provisions of Indian Penal Code, 1860

4. Results & Discussion on cybercrimes as reported in India

NCRB reported 50,035 cybercrimes in India in 2020. Data interpretation shows that 2020 will have more cybercrime instances than 2019, 2018, and 2017. India's States and cities are seeing more cybercrime, according to data. Karnataka, Uttar Pradesh, Maharashtra, and Bengaluru, Mumbai, and Hyderabad are India's most vulnerable states and cities. In 2019, the Central Government developed a web portal (cybercrime.gov.in) to facilitate online cybercrime reporting, and after that several complaints were filed at portal. In three years, 11 lakh cybercrimes were reported to the national cybercrime reporting portal, including 2 lakh social media crimes (FBI Report, 2022). According to PURPLESEC cyber security data, cybercrimes will cost $10.5 trillion annually by 2025 and $6 trillion annually. According to reports, the US is the top cyberattack target, followed by India (Purplesec, 2022). India ranks third in cybercrime according to the FBI (FBI Report, 2022). In India, people also attempt unauthorised network access for enjoyment, as a challenge, or to test network security. It may not be accurate in all circumstances as there are cyber-criminals who can access the Internet unlawfully with evil intentions. Hence, cyber laws are required to be flexible with the quick deviations/changes. Cyberattacks can mess up things like electric grids, air defence systems, and nuclear centrifuges. Several scholars argue for a collaborative public private model cyber policy and cybersecurity technology ecosystem to give cyber users more power in a tech enabled smart city environment (Md Iman Ali, 2021). Existing laws do not cover all kinds of cyberattacks. The law of war sets up rules for the very few cyberattacks that are armed attacks or happen during a war (Oona A. Hathaway, 2012).

5. Conclusion & Policy Recommendation

The I.T. Act of 2000 was last updated in 2008. The Amendment Act has loopholes. Due to underreporting, jurisdictional limits, public apathy, and escalating technology costs, police struggle to investigate cybercrimes. In India, cybercrime is rising. Cybercrime is always changing owing to digital technology advancements. Cybercrime must continually be fought with new ideas and tactics. All stakeholders, including court personnel, legal experts, litigants, and the general public or users, must learn cybercrime technology. Many people, including investigators, are uninformed of restrictions like the adjudication procedure's extent. Jurisdiction is another issue not sufficiently addressed by the I.T. Act or I.T. (Amendment) Act. All key players in the region need training on cybercrime in the "cloud" or "space." Cybercrime is international, territory-free, and devoid of jurisdiction and borders; hence investigators often dismiss these claims. Sometimes judges are reluctant to handle them. Often, nothing can be seen as a scene in cybercrime, thus evidence-related difficulties are also a worry. If authorities don't act promptly to seize equipment and collect evidence, evidence may be wiped. So, set a firm deadline. Cybersquatting is one of the internet crimes committed to extort money, although the Act does not address it. I.T. Act does not address spam emails, ISP accountability for copyright violations, or data privacy. The government also created the online cybercrime reporting portal www.cybercrime.gov.in to submit child pornography/child sexual abuse material or sexually graphic information. The government will build the Indian Cyber Crime Coordination Centre to combat cybercrime (I4C). The "Bill" regulates kid data. "Data localization" would be restricted, especially "sensitive personal data." Cross-border data transfers require consent and authorisation. Data Principal will pay dearly for any leaks (the owner of such data). The Data Protection framework will create a DPA Adjudication and Appellate Tribunal to oversee data processing, storage, and transfer. AII must appoint a DPO to enforce privacy regulations and report breaches. The government has also taken steps to combat cybercrime. Some initiatives are given below:

1. "*National Critical Information Infrastructure Protection Centre*": 2000 IT Act Section 70A (amended 2008). It's part of NTRO and falls under the PM's office (PMO) (PMO). Protect and advise against cyber terrorism, cyber warfare, and other threats to key information infrastructure.
2. "*Centre for Excellence for Internet of Things* (COE-IT)": As part of the Digital India Initiative, it was announced to stimulate the IOT ecosystem using India's IT assets and assist the country become a leader in hardware and software.
3. "*CERT-IN*": Incident Prevention and Response. Cyber-incident data collection, analysis, and distribution • Cyber security forecasts and alerts • Emergency response measures
4. "*Cyber Swachhta Kendra* (Botnet Cleaning and Malware Analysis Centre)": It's based on the 'National Cyber Security Policy,' which aims to protect the country's cyber eco-system. This centre helps ISPs and antivirus/product companies.
5. http://cybercrime.gov.in: India's Ministry of Home Affairs handle which deals with cyber safety and cybersecurity.

6. Suggestions and Recommendations

Despite cyber laws and government rules, user awareness and alertness is essential to control criminals by preventing cybercrime. Some precautions which any individual/business can take are as follows:

For Individuals

Since online fraud is among the most prevalent forms of cybercrime. It entails exploiting phishing websites to acquire a person's personal information, such as banking passwords, and then taking money from the victim's account. Individuals should be more careful with sharing passwords, email addresses, passwords, and phone numbers with third parties. Posting photos and personal content on social media should be done with caution. Avoid opening or replying to mysterious emails or users. Using a strong password for all accounts. Using an updated antivirus software to protect the machine and data. Many people don't realize their mobile devices are vulnerable to viruses and hackers. The software to be downloaded should always be from reputable sources. We must also update our operating systems on regular basis and anti-virus software should be used. Even a small mechanism of locking screen can avoid certain mishaps.

At the Supervisory level/Business Level

Every district court should set up a special Cyber Court to hear cases and issue orders when the legal system cannot wait to respond. Mandatory provisions to certify digital evidence with digital evidence authenticators. Services and websites that are based in India must follow their own set of regulations. Personal data of Indian citizens should be kept on Indian servers. Cybersecurity frameworks, standards, and/or best practices should be mandatorily implemented by enterprises and government agencies. Focusing on cybercrime threat response, cybercrime operations, and the development of cyber capabilities, governments must aim to lessen the global impact of cybercrime and protect communities for a safer world. Cybercriminals must be treated like theft, rape, and murder. India has various laws and regulations to fight cybercrime, but they need to be updated as technology improves and criminals discover new tactics. To effectively combat cybercrime in India, national and international law enforcement must coordinate. India is doing a good thing by making a National Cyber Security Strategy to fight this growing problem. But as the country works on its policy and eventually puts it into place, it must also look to international law. This is because international law already provides strong protection against cyberattacks, is a good addition to any future domestic cybersecurity policy or law because the cyber world is inherently global, and can teach India lessons that it can use in its own upcoming cybersecurity policy. The connecting qualities of the Internet, in particular how it connects people, social spaces, and infrastructure across multiple countries, frequently conflict with the structure of sovereignty and jurisdiction that governs surveillance (Ben Collier, 2022). Cyber laws are formed in the context of the Internet to ensure that netizens use cyberspace responsibly. Internet users are clueless of cyber laws and the rise in cybercrime cases (Asma Md. Isa et al., 2020). Combating cybercriminals and cyberterrorists will create unanticipated complicated issues that may be avoided with effective individual and government cooperation. Technical analysis should determine cause, impact, and attacker method. All workers, external entities, and consumer groups should get Cybersecurity training and awareness initiatives.

References

(n.d.). Retrieved from indiacode.nic.in: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

(n.d.). Retrieved from https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=

(n.d.). Retrieved from https://cybercrime.gov.in/Default.aspx

(n.d.). Retrieved April 12, 2022, from https://www.cert-in.org.in/

(2019). Ministry of Home Affairs, Government of India. Delhi: PIB Delhi. Retrieved May 17, 2022, from https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226

Barrett, D. (2001). Cybercrime: law enforcement, security and surveillance in the information age. (D. T. Loader, Ed.) *Journal of Social Policy*, 149-188. doi:DOI: https://doi.org/10.1017/S0047279400376218

Ben Collier, D. R. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services,Policing and Society. *Taylor & Francis*, DOI: 10.1080/10439463.2021.1883608.

Broadhurst, R. (2006, July 1). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal, 29*(3), 408-433. doi:Policing: An International Journal

Bureau, T. N. (2021). Ministry of Home Affairs, Government of India. Retrieved from https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.2.pdf

Chouhan, R. (2014, September 19). Cyber Crimes: Evolution, Detection and Future Challenges. *The IUP Journal of Information Technology, X*(1), 48-55. Retrieved May 13, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498348

(2022). *Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2020.* Statista Research Department. Retrieved April 27, 2022, from https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/

(2021). *Cybercrime Legislation Worldwide.* Geneva: UNCTAD. Retrieved May 16, 2022, from https://unctad.org/page/cybercrime-legislation-worldwide

FBI Report. (2022, May 20). *India among top five victims of cybercrime: FBI report*. The Hindu . Retrieved June 2, 2022, from https://www.thehindubusinessline.com/info-tech/india-among-top-five-victims-of-cybercrime-fbi-report/article65475805.ece

Global Programme on Cybercrime. (n.d.). United Nations : Office on Drugs & Crime. Retrieved from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

Hakmeh, J. (2017, June 6). *Building a Stronger International Legal Framework on Cybercrime*. Retrieved May 22, 2022, from https://www.chathamhouse.org: https://www.chathamhouse.org/2017/06/building-stronger-international-legal-framework-cybercrime

(2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19.* France: INTERPOL Secretary General. Retrieved 22 May, 2022, from https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Kirsty Phillips, J. C. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, 379-398. doi:https://doi.org/10.3390/forensicsci2020028

Kittichaisaree, K. (2017). *Public international law of cyberspace.* Cham: Springer, 2017. Retrieved May 2022, 27, from https://www.springerprofessional.de/public-international-law-of-cyberspace/12108792

Kshetri, N. (2013, April). Cyber-victimization and cybersecurity in China. *Communications of the ACM, 56*(4). doi:doi:10.1145/2436256.2436267

Kshetri, N. (2016, September 10). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, 313-338. doi:doi:10.1007/s10611-016-9629-3

Mandavia, M. (2019, September 26). *The India has highest number of Internet users after China: Report*. India: The Econimic Times. Retrieved from https://m.economictimes.com/tech/internet/india-has-second-highest-number-of-internet-users-after-china-report/articleshow/71311705.cms

Md Iman Ali, S. K. (2021). The Impact of India's Cyber Security Law and Cyber Forensic On Building Techno-Centric Smartcity IoT Environment. *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS).* Greater Noida, India: IEEE. doi:https://doi.org/10.1109/ICCCIS51004.2021.9397243

National Cyber Crime Reporting Portal. (n.d.). Ministry of Home Affairs, Government of India. Retrieved July 2, 22, from https://cybercrime.gov.in/

National Cyber Crime Reporting Portal, https://cybercrime.gov.in/. (2022). Retrieved June 12 , 2022, from cybercrime.gov.in: https://cybercrime.gov.in/

Nweze-Iloekwe, N. (2022). The Legal and Regulatory Aspect of International Cybercrime and Cybersecurity: Limits and Challenges. *Golden Gate University School of Law.*

Oona A. Hathaway, R. C. (2012, August). The Law of Cyber-Attack. *CALIFORNIA LAW REVIEW, 100*(4). Retrieved May 2022, 16, from https://www.californialawreview.org/print/2the-law-of-cyber-attack/

Parasol, M. (2018, February). The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. *Computer Law & Security Review, 34*(1), 67-98. doi:https://doi.org/10.1016/j.clsr.2017.05.022

PTI. (2020, Oct 20). The Econimic Times. *Cyber crimes in India caused Rs 1.25 lakh crores loss last year: : Official*. The Economic Times. Retrieved from economictimes.indiatimes.com: https://economictimes.indiatimes.com/tech/tech-bytes/cyber-crimes-in-india-caused-rs-1-25-lakh-cr-loss-last-year-official/articleshow/78773214.cms

PTI. (2021, September 15). The Hindu. *India reported 11.8% rise in cyber crime in 2020; 578 incidents of 'fake news on social media': Data*. The Hindu. Retrieved from https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece

Purplesec. (2022). *Cyber Security Statistics The Ultimate List Of Stats Data, & Trends for 2022.* Purplesec. Retrieved June 17, 2022, from https://purplesec.us/resources/cyber-security-statistics/

Report. (2022, June 21). *India ready to face cyber threat: Amit Shah*. The Times of India. Retrieved June 24, 2022, from https://timesofindia.indiatimes.com/india/india-ready-to-face-cyber-threat-amit-shah/articleshow/92347344.cms

Ross Anderson, C. B. (2013). Measuring the Cost of Cybercrime. *The Economics of Information Security and Privacy*, 265-300. doi:https://doi.org/10.1007/978-3-642-39498-0_12

Saroha, R. (2014). Profiling a Cyber Criminal. *International Journal of Information and Computation Technology, 4*(3), 253-258. Retrieved May 2022, 12, from https://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf

Shivani Shinde, N. A. (2021, April 6). India becomes favourite destination for cyber criminals amid Covid-19. *Report*. Mumbai, New Delhi: Business Standard. Retrieved April 25, 2022, from business-standard.com: https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html

Shivani Shinde, N. A. (2021, April 6). India becomes favourite destination for cyber criminals amid Covid-19. . Mumbai: Business Standard. Retrieved May 25, 2022, from https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-crimin

(2019). *The multi-faceted threat of fraud: Are banks up to the challenge?* Austrelia: KPMG International Coporative. Retrieved April 27, 2022, from https://assets.kpmg/content/dam/kpmg/au/pdf/2019/global-banking-fraud-survey-2019-au.pdf

Wall, D. (2001). Crime and the Internet. In D. Wall (Ed.), *Crime and the Internet* (Ist ed.). London: Routledge. doi:https://doi.org/10.4324/9780203299180

White, G. (2020, May 3). Love Bug's creator tracked down to repair shop in Manila. BBC News. Retrieved May 4, 2022, from https://www.bbc.com/news/technology-52458765

Yuriy Timofeyev, O. D. (2022, March). Insurers' responses to cyber crime: Evidence from Russia. *International Journal of Law, Crime and Justice, 68*. doi:https://doi.org/10.1016/j.ijlcj.2021.100520