Reviewing Status of Cyber crime in India- Expanding Horizons

Banreet Singh Kler[1], Dr. Arpana Bansal[2]
[1,2]*Guru Kashi University, Talwandi Sabo*
doi.org/10.64643/IJIRTV12I6-191363-459

Abstract- The purpose of the paper to analyse the increasing cases of cyber violations, the urgency for more robust and comprehensive cyber security measures, among other issues. Between March and April 2020, India has witnessed a staggering 86% increase in cyber-attacks. According to the UN Special Reporter, women are both disproportionately targeted by online violence and suffer disproportionately serious consequences as a result. Cybercrime has real consequences and costs. It undermines women's wellbeing, their rights, and their progress in all aspects of life. Cyber violence results in psychological, physical, sexual or economic harm to women. Given the push towards digitisation, amongst the ongoing pandemic, more women and girls are using the internet for varied purposes including education, work, and financial transactions, amongst others. Many of these women and girls could be first-time users and/or may have a limited understanding of good practices when interacting with others in cyberspace and could be subjected to cybercrimes. No doubt the crime rate has subsided as people are staying back but online frauds have seen an upsurge. Apart from being interaction/communication interfaces, sometimes these also serve as platforms for criminal elements and eventually end up being the epicentres of immeasurable security concerns. This working from home has now become an opportunity for cybercriminals to exploit the people through e-mail scams, hacking passwords, phishing, ransom attacks, online sexual harassment, etc.

Keywords - Cyber Crime, Covid-19, Phishing, Computer Crime, Cyberspace, Online Violence

I. INTRODUCTION

Ever since the lockdown, people are accessing social media websites such as Instagram, Facebook, Twitter, etc., more frequently in addition to watching movies and series by subscribing to web channels like Netflix, Amazon, HotStar, Zee etc. and also indulging in online games by installing various applications. All these activities are supported by the internet. People tend to provide and/or give permissions to access their personal information readily available on their phones, laptops and/or social media accounts in order to use the services provided by the applications. Many a times, in order to purchase apps or access online services, financial information too is shared by the users. Additionally, in view of the 'stay home, stay safe' government notification, people have become more dependent on various payment gateways to pay their utility bills, premiums, recharge their mobile phones, buy medicines and essential commodities online and indulge in various such online activities. All these activities have opened the door for spyware and ransom ware attacks. A spyware steals sensitive personal data of the user while, ransom ware takes control over the login and other vital credentials of a person. These attacks may result into huge losses to people not only financially but also otherwise. All these crimes are caused by computers. Computer crime alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individuals private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files. Computer crime describes a very broad category of offenses. Some of them are the same as noncomputer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like hacking, are uniquely related to computers. Read on to find out what kinds of activities are considered computer crimes and how to protect yourself from them.

II. MEANING AND DEFINITION OF COMPUTER CRIMES

Much of the literature on computer crime focuses on computer-related fraud. "Fraud is the intentional or

deliberate perversion of truth in order to gain an unfair advantage". This is certainly a large part of computer crime but is perhaps a bit too narrow for our purposes. Many others, when they think of computer crime, only think of those who break into computers to steal or destroy information. We can get a slightly larger definition by examining what is actually investigated by law enforcement agencies. The FBI National Computer Crime Squad (NCCS) concerns itself with all crime involving computers in two or more states ["FBI Computer" 1]. It considers the following to be important computer crimes:

Intrusions of the Public Switched Network (the telephone company)
Major computer network intrusions
Network integrity violations
Privacy violations
Industrial espionage
Pirated computer software
Other crimes where the computer is a major factor in committing the criminal offense".

Examples of Cyber Crimes

Following are examples of prevalent Cyber Crimes:

Child pornography- Making or distributing child pornography.
Copyright violation - Stealing or using another person's Copyrighted material without permission.
Cracking - Breaking or deciphering codes designed to protect data.
Cyber terrorism - Hacking, threats, and blackmailing towards a business or person.
Cyberbully or Cyberstalking - Harassing or stalking others online.
Cybersquatting - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
Creating Malware - Writing, creating, or distributing malware (e.g., viruses and spyware.)
Denial of Service attack - Overloading a system with so many requests it cannot serve normal requests.
Doxing - Releasing another person's personal information without their permission.
Espionage - Spying on a person or business.
Fraud - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
Harvesting - Collect account or account-related information on other people.
Human trafficking - Participating in the illegal act of buying or selling other humans.
Identity theft - Pretending to be someone you are not
Illegal sales - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
Intellectual property theft - Stealing practical or conceptual information developed by another person or company.
IPR violation - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.
Phishing - Deceiving individuals to gain private or personal information about that person.
Salami slicing - Stealing tiny amounts of money from each transaction.
Scam - Tricking people into believing something that is not true.
Slander - Posting libel or slander against another person or company.
Software piracy - Copying, distributing, or using software that is Copyrighted that you did not purchase.
Spamming - Distributed unsolicited e-mail to dozens or hundreds of different addresses.
Spoofing - Deceiving a system into thinking you're someone you are not.
Typo squatting - Setting up a domain that is a misspelling of another domain.
Unauthorized access - Gaining access to systems you have no permission to access.
Wiretapping - Connecting a device to a phone line to listen to conversations.

NCRB Data Analysis on Cyber Crime

As per the cyber crime data maintained by the National Crime Records Bureau (NCRB), a total of 217, 288, 420 and 966 Cyber Crime cases were registered under the Information Technology Act, 2000 during 2007, 2008, 2009 and 2010 respectively. Also, a total of 328, 176, 276 and 356 cases were registered under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007, 2008, 2009 and 2010 respectively. A total of 154, 178, 288 and 799 persons were arrested under Information Technology Act 2000 during 2007-2010. A total number of 429, 195, 263 and 294 persons were arrested under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007-2010. As per

2011 NCRB figures, there were 1,791 cases registered under the IT Act during the year 2011 as compared to 966 cases during the previous year (2010) thereby reporting an increase of 85.4% in 2011 over 2010. Of this, 19.5% cases (349 out of 1,791 cases) were reported from Andhra Pradesh followed by Maharashtra (306), Kerala (227), Karnataka (151) and Rajasthan (122). And 46.1% (826 cases) of the total 1,791 cases registered under IT Act, 2000 were related to loss/damage to computer resource/utility reported under hacking with computer systems.

According to NCRB, the police have recorded less than 5,000—only 4,829 cases and made fewer arrests (3,187) between 2007 and 2011, under both the Information Technology (IT) Act as well as the Indian Penal Code (IPC). And convictions remain in single digits, according to lawyers. Only 487 persons were arrested for committing such offences during the year 8 2011. There were 496 cases of obscene publications/transmission in electronic form during the year 2011 wherein 443 persons were arrested. Out of total 157 cases relating to hacking under Sec. 66(2), most of the cases (23 cases) were reported from Karnataka followed by Kerala (22) and Andhra Pradesh (20 cases). And 20.4% of the 1184 persons arrested in cases relating to IT Act, 2000 were from Andhra Pradesh (242) followed by Maharashtra (226). The age-wise profile of persons arrested in cyber crime cases under the IT Act, 2000 showed that 58.6% of the offenders were in the age group 18–30 years (695 out of 1184) and 31.7% of the offenders were in the age group 30-45 years (376 out of 1184). Madhya Pradesh (10), Maharashtra (4), Kerala (3) and Delhi (2) reported offenders whose age was below 18 years.

Meanwhile, a total of 422 cases were registered under the Indian Penal Code or IPC Sections during the year 2011 as compared to 356 such cases during 2010 thereby reporting an increase of 18.5%.

Maharashtra reported maximum number of such cases (87 out of 422 cases i.e. 20.6%) followed by Chhattisgarh 18.0% (76 cases) and Delhi 11.6% (49 Cases). Majority of the crimes out of total 422 cases registered under IPC fall under 2 categories--forgery (259) and Criminal Breach of Trust or fraud (118). Although such offences fall under the traditional IPC crimes, these cases had the cyber overtones wherein computer, Internet or its enabled services were present in the crime and hence they were categorised as Cyber Crimes under IPC. Age-wise profile of the offenders arrested under Cyber Crimes reveals that offenders involved in 9 forgery cases were more in the age-group of 18-30 (46.5%) and 50.4% of the persons arrested under Criminal Breach of Trust/Cyber Fraud offences were in the age group 30-45 years.

Meanwhile 9 out of 88 mega cities did not report any case of cyber crime i.e., neither under the IT Act nor under IPC Sections during the year 2011. And 53 mega cities have reported 858 cases under IT Act and 200 cases under various sections of IPC. A total of 44,546 cases were registered under Cyber Crimes, showing a huge increase of 63.5% in registration over 2018 (27,248 cases). Crime rate under this category increased from 2.0 in 2018 to 3.3 in 2019. During 2019, 60.4% of cyber-crime cases registered were for the motive of fraud (26,891 out of 44,546 cases) followed by sexual exploitation with 5.1% (2,266 cases) and causing disrepute with 4.2% (1,874 cases).

Table 1: Cyber crimes against women (2019-2021)

Cyber crimes against women			
State/ Year	2019	2020	2021
Andhra Pradesh	356	375	471
Karnataka	2,698	2,859	2,243
Kerala	139	246	353
Tamil Nadu	124	306	248
Telangana	288	649	883

III. RECENT TREND

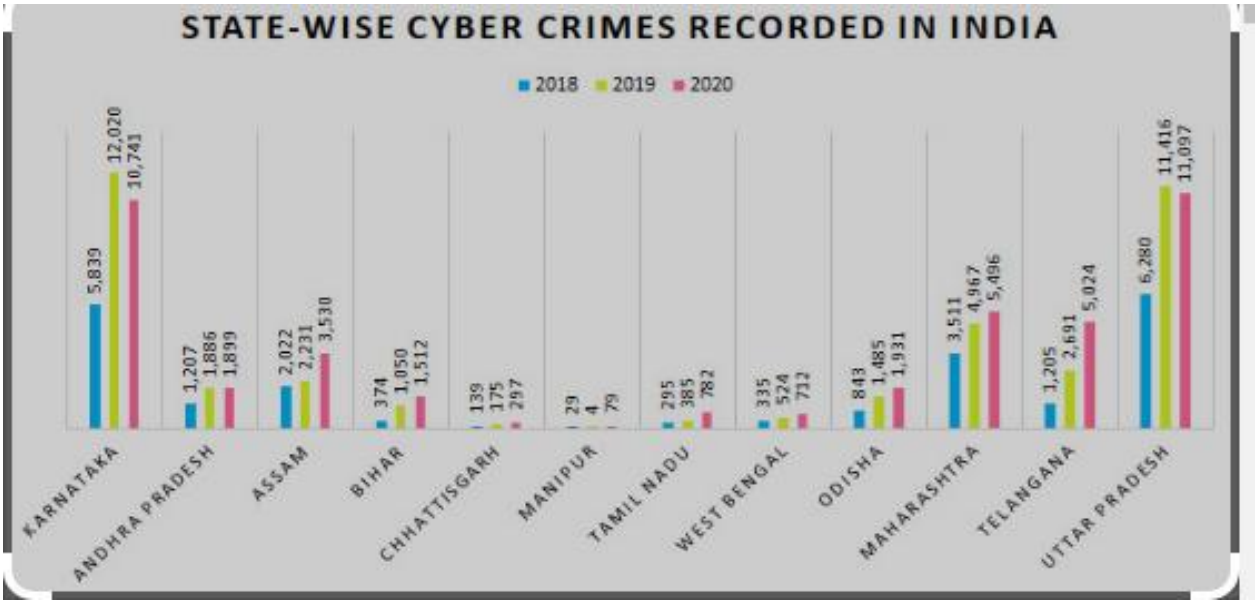
The pandemic of COVID-19 and the imposed lockdown, has led to more people to be confined at home with many more hours to spend online each day and increasingly relying on the Internet to access services, they normally obtain offline. The dangers of cyber-crime have been there for many years, but the increase in the percentage of the population connected to the Internet and the time spent online, combined with the sense of confinement and the anxiety and fear generated from the lockdown, have provided more opportunities for cybercriminals to take advantage of the situation and make more money or create disruption. It is important to note that some more vulnerable segments of the population, such as children need to spend more time online for services such as schooling. This seismic change in how we live our lives and use the Internet has prompted a proliferation of e-crimes. Common cybercrime techniques, such as phishing, have seen a spike. Phishing is the fraudulent practice of inducing individuals to reveal personal information, such as passwords and credit card numbers through fake websites or emails.

Table 1. Cyber Crimes - IT Act Cases

Sr. No.	Type of Offence	No. of Cases				
		2017	2018	2019	2020	2021
1	Tampering Computer Source Document	233	257	173	338	55
2	Computer Related Offences	10108	14141	23612	21926	19915
3	Cyber Terrorism	13	21	12	26	15
4	Publication/ transmission of obscene/sexually explicit act in electronic form	1768	3076	4187	6308	6598
5	Interception or Monitoring or decryption of Information	4	6	9	7	2
6	Un-authorized access/attempt to access to protected computer system	2	0	2	2	3
7	Abetment to Commit Offences	0	1	0	1	7
8	Attempt to Commit Offences	4	13	14	18	5
9	Other Sections of IT Act	1503	980	2720	1017	827
	Total Cyber Crimes under IT Act	**13635**	**18495**	**30729**	**29643**	**27427**

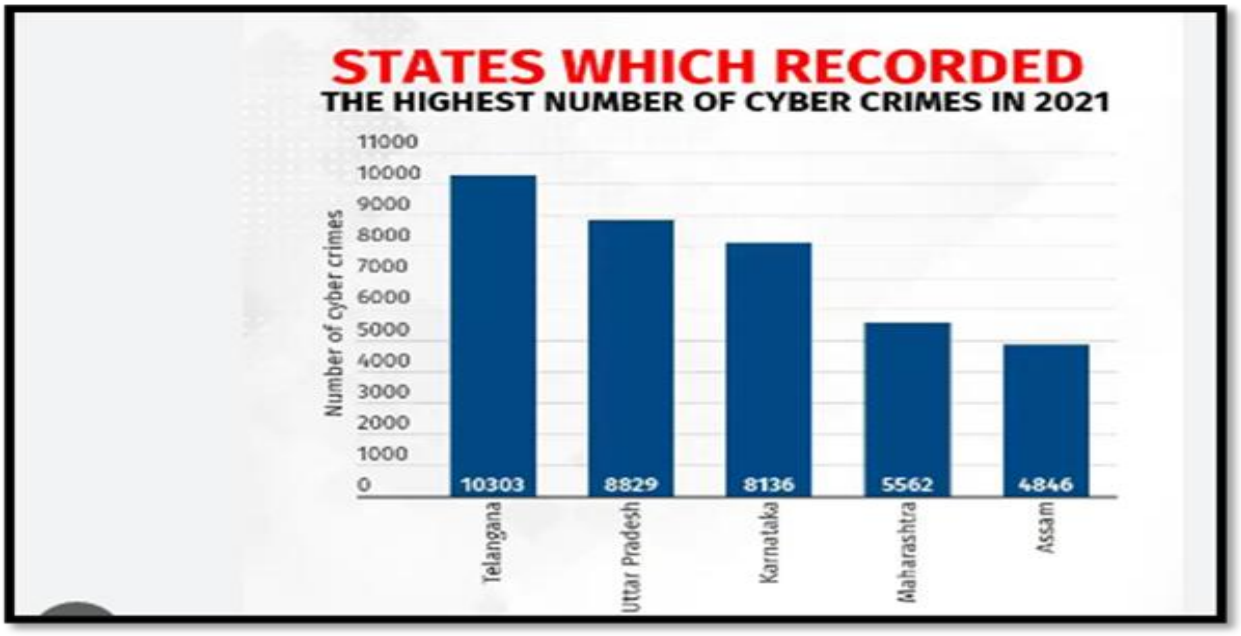
The Kaspersky Security Network (KSN) report showed that its products detected and blocked 52,820,874 local cyber threats in India between January to March this year. The data also shows that India now ranks 27th globally in the number of web-threats detected by the company in Q1 2020 as compared to when it ranked on the 32nd position globally in Q4 2019."There has been a significant increase in the number of attacks in 2020 Q1 that may continue to rise further in Q2 as well, especially in the current scenario where we notice an increase in cybercriminal activities, especially in the Asia Pacific region," said Saurabh Sharma, Senior Security Researcher, GReAT Asia Pacific at Kaspersky. The number of local threats in Q1 2020 in India (52,820,874) shows how frequently users are attacked by malware spread via removable USB drives, CDs and DVDs, and other "offline" methods. Protection against such attacks not only requires an antivirus solution capable of treating infected objects but also a firewall, anti-rootkit functionality and control over removable devices. According to the firm, the number of local threats detected in Q4 2019 was 40,700,057. Lt. Gen. Rajesh Pant, India's National Cyber Security Coordinator (NCSC), told the Economic Times that cyber criminals had launched thousands of "fraud portals" related to the coronavirus. These sites have lured thousands of Indians eager to contribute to the fight against coronavirus into making donations. Many of these phony sites are quite sophisticated, virtually indistinguishable from their genuine counterparts.

Figure 1: State wise cyber crime recorded for year 2018,2019 and 2020



India also ranks 11th worldwide in the number of attacks caused by servers that were hosted in the country, which accounts of 2,299,682 incidents in Q1 2020 as compared to 854,782 incidents detected in Q4 2019, said the report. According to National Commission for Women (NCW) data, 54 cybercrime complaints were received online in April in comparison to 37 complaints received online and by post -- in March, and 21 complaints in February. The panel is taking complaints online due to the lockdown. Cyber experts, however, said the numbers are just the 'tip of the iceberg'." total of 412 genuine complaints of cyber abuse from March 25 till April 25. Out of these, as many as 396 complaints were serious ones from women, (and these) ranged from abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail and more.

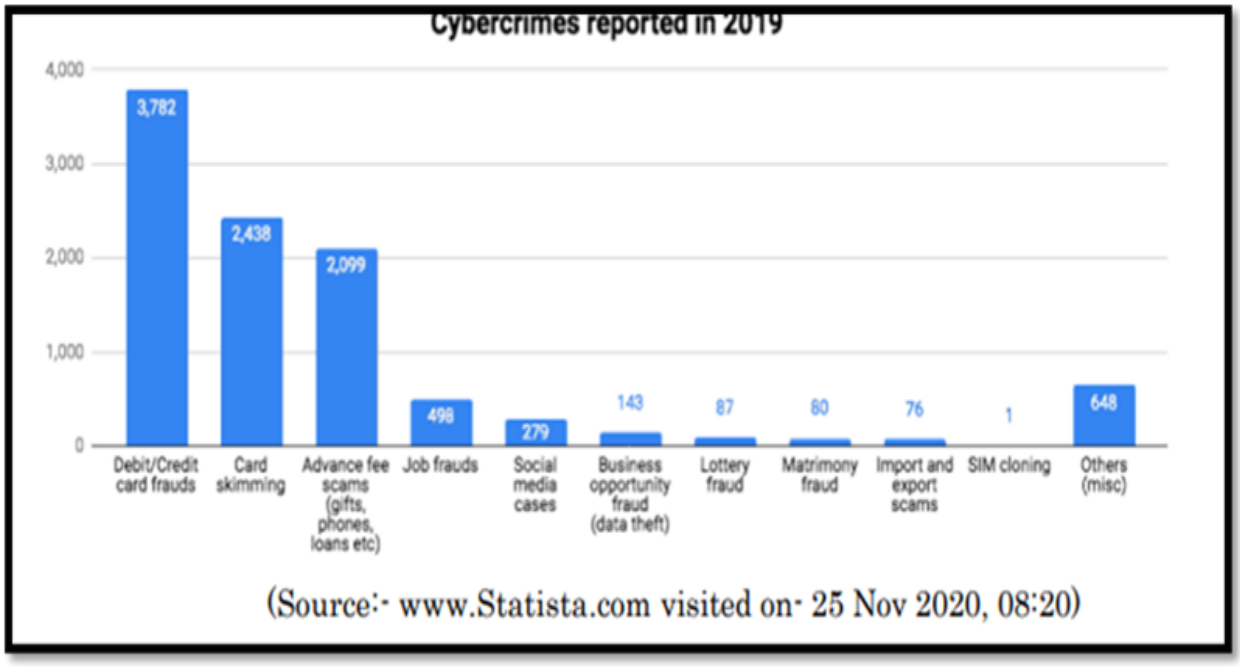
Figure 2: State recorded highest number of cyber crime cases in 2021



Reasons for increasing Cyber Attacks in India

Increasing dependency on technology: In India, cybercrime is increasing with the increased use of information and communication technology (ICT). Growing digital reliance in the post-COVID era has exposed digital disparities.

Figure 3: Cybercrimes reported in 2019



Limited capacity enforcement agencies: the capacity of the enforcement agencies to investigate cybercrime remains limited. India's approach to cyber security has so far been ad hoc and unsystematic.

With 'police' and 'public order' being in the State List, the primary obligation to check crime and create the necessary cyber infrastructure lies with States. At the same time, with the IT Act and major laws being central legislations, the central government is no less responsible to evolve uniform statutory procedures for the enforcement agencies.

Lack of International Coordination: International cooperation and consensus is missing in this field.

No procedural code: There is no separate procedural code for the investigation of cyber or computer-related offences.

Shortage of technical staff: There have been half-hearted efforts by the States to recruit technical staff for the investigation of cybercrime. A regular police officer, with an academic background in the arts, commerce, literature, or management may be unable to understand the nuances of the working of a computer or the Internet.

Low digital literacy among the general public and digital gaps amongst nations create an unsustainable environment in the cyber domain.

Penalty and compensation for damage to Computer, Computer System etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, or computer resource —

1. Accesses or secures access to such computer, computer system or computer network;
2. Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
3. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. Or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5. Disrupts or causes disruption of any computer, computer system or computer network;

6. Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this act, rules or regulations made thereunder;
7. Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
8. Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
9. Steel, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

Government Initiatives to Tackle Cyber Crime in India
Government of India has organized several initiatives to combat cybercrime. These can be listed as follows:
(i) Banning of unsafe apps: India had banned apps that posed a threat to security.
- India had banned many apps (mostly of Chinese origin), which were found to be unsafe for usage by Indian citizens.

(ii) The Indian Computer Emergency Response Team (CERT-In):
- It operates as the national agency for tackling the country's cybersecurity, and has helped in lowering the rate of cyber attacks on government networks.

(iii) Indian Cyber Crime Coordination Centre (I4C)
- To act as a nodal point in the fight against cybercrime
- To prevent misuse of cyber space for furthering the cause of extremist and terrorist groups

(iv) National Critical Information Infrastructure Protection Centre (NCIIPC)
- It is a central government establishment, formed to protect critical information of India, which has an enormous impact on national security, economic growth, or public healthcare.

(v) Cyber Swachhta Kendra: Cyber Swachhta Kendra helps users to analyse and keep their systems free of various viruses, bots/ malware, Trojans, etc.
- Launched in early 2017.

(vi) Cyber Surakshit Bharat: It was launched by the Ministry of Electronics and Information Technology (MEITy) in 2018 with an aim to
- spread awareness about cybercrime and
- building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.

(vii) The Cyber Warrior Police Force: It was organised on the lines of the Central Armed Police Force in 2018.
(viii) Information Technology Act, 2000 (Amended in 2008): It is the main law for dealing with cybercrime and digital commerce in India.
(ix) National Critical Information Infrastructure Protection Centre (NCIIPC) was created under Section 70A of IT Act 2000 to protect Cyberinfrastructure.
(x) BIS guidelines: The broad guidelines for the identification, collection, acquisition and preservation of digital evidence issued by the Bureau of Indian Standards (BIS) is fairly comprehensive and easy to comprehend for both the first responder (who could be an authorised and trained police officer of a police station) as well as the specialist (who has specialised knowledge, skills and the abilities to handle a wide range of technical issues). The guidelines, if followed meticulously, may ensure that electronic evidence is neither tampered with nor subject to spoliation during investigation.
(xi) Judicial Intervention: A five-judge committee was constituted in July 2018 to frame the draft rules which could serve as a model for the reception of digital evidence by courts.
The committee suggested Draft Rules for the Reception, Retrieval, Authentication and Preservation of Electronic Records are yet to be given a statutory force.

IV. CONCLUSION

Thus, it is clear that the cybercrime today has come to describes a very broad category of offenses. Some of them are the same as non-computer offenses, such as larceny or fraud, except that a computer or the Internet is used in the commission of the crime. Others, like hacking, are uniquely related to computers. The government must make sure the safety of the state digital network & systems which store important public information and must take concrete steps during this regard. The lockdown has exposed the weak

cyber-laws and after a couple of 5 percent increase in cybercrimes, the govt. has shifted some focus to the current side and also the cyber-centres and cyberpolice became active. The govt. is issuing an advisory to the general public to to not fall prey to those only crimes and take precautions while filling their details and passwords on online sites. But the govt also must come up with some stronger laws, procedures, and methods to catch the hackers. Besides, there's a necessity to introduce some security applications to forestall the companies' systems and hospital computers from hacking. These are a number of the short-term solutions during the lockdown but there also needs some reform within the current Information Technology Act, 2000 because it could be a comprehensive act and doesn't include much of the opposite aspects which are littered with the cyber-crimes.

REFERENCES

[1] Available on https://www.lexology.com/library/detail.aspx?g=f33f6b37-6b62-425a-852b0be29cbe46a7

[2] What is Computer Crime ?'- Computer Hope available at: - https://www.computerhope.com(Last visited on- 27 Nov 2020, 12:07).

[3] Computer Crime'- Find Law available at: - https://criminal.findlaw.com(visited on- 27 Nov 2020, 12:20).

[4] Working Definition of Computer Crimes'- Stanford Computer Science available at: - https://cs.stanford.edu> projects (visited on- 2 Dec 2020, 15:00).

[5] Ibid

[6] Ibid1

[7] Supra note 2.

[8] Supra note 1.

[9] Available at: https://ncrb.gov.in/en (visited on- 28 Nov 2020, 11:20).

[10] Available at: http://f3magazine.unicri.it/?p=2085(visited on- 27 Nov 2020, 12:20).

[11] Available at: https://www.forbes.com/sites/ronakdesai/2020/05/14/cybercrime-in-indiasurges-amidst-coronavirus-lockdown/?sh=603a4f31392e(visited on- 27 Nov 2020, 12:20).

[12] Available at: https://ciso.economictimes.indiatimes.com/news/37-increase-in-cyberattacksin-india-in-q1-2020-report/75962696(visited on- 27 Nov 2020, 12:20).

[13] Available at: https://www.newindianexpress.com/nation/2020/may/01/significant-increasein-cybercrime-against-women-during-lockdown-experts-2137987.html(visited on- 27 Nov 2020, 12:20).

[14] S. 43 of the Information Technology Act, 2000- Indian Kanoon available at: - https://indiankanoon.org> doc (visited on- 27 Dec 2020, 14:40).

[15] S. 43 of the Information Technology Act, 2000- The Center for Internet and Society available at: https://cis-India.org> resources> (visited on- 27 Dec 2020, 14:57).