13

Frequency and Intensity Cyber crimes in India: Technical Reasons and Legal Remedies

Dr. Ashish Verma[1], Dr. Shikha Dimri[2]

[1]Professor, School of Law and Justice, Adamas University, Kolkata.
[2]Sr.Associate, Professor, School of Law, UPES, Dehradun.

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."

Jürgen Stock, INTERPOL Secretary General

Whenever a new crisis emerges, different criminal actors are the first to jump on the occasion to exploit unsuspecting victims in times of fear, uncertainty and doubt. These exploits take multiple forms, from the physical to the digital world. History has taught us that the most efficient method to initially counter these threats is through prevention and awareness towards all levels of corporate and personal life.[1] Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we have not seen before. Complex criminal networks operate across the world, coordinating intricate attacks in a matter of minutes.[2] Cyber crime is a modern-day evil that's tems from our increasing reliance on computers. Communication technologies can be used to commit a wide variety of criminal offenses[3]. Cybercrimes are generally divided into two types: first, new offences committed

---

[1]Unodc.org. 2021. [online] Available at: <https://www.unodc.org/documents/middleeastandnorthafrica/2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf> [Accessed 24Augustr 2021].
[2]Interpol.int. 2021. *Cybercrime*. [online] Available at: <https://www.interpol.int/en/Crimes/Cybercrime> [Accessed 24August 2021].
[3]Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012

using new technologies, such as cybercrimes against computer networks and records, and second, old offences committed using new technology, such as using a computer network to enable the commission of a cybercrime.[4]

The Internet was argued to be a unique medium with the quickest level of diffusion in humanhistoryasearlyastheearly1990s[5]. There are very few people today who selives are unaffected by Internet-era technology, both positively and negatively.[6] In the plus side, the opportunity to instantly communicate and distribute information has brought unparalleled benefits to education, commerce, culture, and social networking. On the negative side, it has increased the opportunity for fraud to be committed. Information technology has enabled suspected criminals to commit large-scale offences with virtually no money and at a much lower chance of getting detected. In comparison to typical economic-motivated criminals (e.g., burglaries, larcenies, and bank robberies), online criminals are relatively unconcerned about meeting law enforcement and witnesses. Technology has changed the way adolescents engage and connect with their peers over the last decade; teens' increased dependence on technology has been well established.[7]

Defining cyber crime

Specific offences most commonly associated with cyber-dependent crimes, such as hacking and the creation or distribution of malware, are defined in the Computer Misuse Act 1990[8] Cyber crime is an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes. Use

---

[4]https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html [Accessed 21 August 2021].

[5]https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/ [Accessed 21 August 2021].

[6]https://www.pewresearch.org/internet/2018/07/03/the-positives-of-digital-life/ [Accessed 21 August 2021].

[7]https://www.sciencedirect.com/topics/computer-science/cybercriminals [Accessed 21 August 2021].

[8]As amended by the Police and Justice Act 2006

of 'cyber crime' refers to both forms of criminal activity, and we distinguish between them as outlined below:

Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other form of ICT.[9] These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks, i.e. the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud. [10]

Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber dependent crimes, they can still be committed without the use of ICT. For the purposes of this review the following types of cyber-enabled crimes are included: fraud (including mass-marketing frauds, 'phishing' e-mails and other scams; online banking and e-commerce frauds); theft (including theft of personal information and identification-related data); and sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery)[11]

Types of cyberattacks

Malicious domains

There are a considerable number of registered domains on the Internet that contain the terms: "coronavirus", "corona-virus", "covid19" and "covid-19". While some are legitimate websites, cybercriminals are creating thousands of new sites every day to carry out spam campaigns, phishing or to spread malware.

---

[9]Sleiman, M. B., & Gerdemann, S. (2021). Covid-19: a catalyst for cybercrime?. *International Cybersecurity Law Review*, *2*(1), 37-45.

[10]Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

[11]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf[Accessed 11 October 2021].

Malware

Cybercriminals are taking advantage of the widespread global communications on the coronavirus to mask their activities. Malware, spyware and Trojans have been found embedded in interactive coronavirus maps and websites. Spam emails are also tricking users into clicking on links which download malware to their computers or mobile devices.

Ransomware

Hospitals, medical centres and public institutions are being targeted by cybercriminals for ransomware attacks-since they are overwhelmed with the health crisis and cannot afford to be locked out of their systems, the criminals believe they are likely to pay the ransom.

The ransomware can enter their systems through emails containing infected links or attachments, compromised employee credentials, or by exploiting a vulnerability in the system.[12]

Covid 19 and cyber crimes

In late December 2019, the World Health Organization (WHO) noted initial media statements emanating from China's Wuhan Province about "viral pneumonia" cases.[13] Within weeks, researchers determined these cases were cause by a novel, rapidly spreading, and life-threatening coronavirus. Nations began assessing how they might protect their populations, with many instituting travel bans and the like, but the spread of the disease proved

---

[12]https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats [Accessed 11 October 2021].

[13]Chad R. Wells, etal., Impact of International Travel and Border Control Measures on the Global Spread of the Novel 2019 Coronavirus Outbreak, Proceedings of the National Academies of Sciences of the United States of America (March 31, 2020), https://www.pnas.org/content/117/13/7504. [Accessed 11 October 2021].

significantly hard to control,[14] particularly given the globalized economic environment and the existence of rapid, long-distance travel. On March 11, 2020, the WHO determined that the spread and severity of COVID-19 had reached pandemic levels,[15] and by early 2021, the virus had infected over 140 million individuals and killed over 3 million worldwide.[16] With vaccines now approved and in distribution,[17] some degree of relief appears on the horizon. Much depends however, among other things, on vaccine efficacy-particularly against new virus strains-and optimal vaccine distribution.[18] The COVID19 pandemic poses an unprecedented global challenge to all of society. Many have transferred their physical activities to online operations, as have criminals. As cybercrime increases in complexity and victims increase in quantity, law enforcers in some countries are moved to other duties. The economic impact of COVID19 adds a further layer of complexity for the public and for government. A perfect storm of potential cybercriminality emerges.[19]

---

[14]World Health Organization, Listings of WHO's Response to COVID-19, June 29. 2020, http://who.int/news/item/29- 06-2020-covidtimeline/[Accessed 11 October 2021].

[15]World Health Organization, Listings of WHO's Response to COVID-19

[16]World Health Organization. WHO Coronavirus Disease (COVID-19) Dashboard (February 24, 2021), reporting 111,762,965 cases of COVID-19 worldwide and 2,479,678 deaths, https://covid19.who.int/ [Accessed 11 October 2021].

[17]U.S. Food and Drug Administration, COVID-19 Frequently Asked Questions, (noting that "[o]n December 11, 2020, the FDA issued an Emergency Use Authorization (EUA) for the use of the Pfizer-BioNTech COVID-19 Vaccine...[and] [o]n December 18, 2020, the FDA issued an EUA for the use of the Moderna COVID-19 Vaccine."), https://www.fda.gov/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/covid-19-frequently-asked-questions#biologics[Accessed 11 October 2021].

[18]Alexander, K. B., & Jaffer, J. N. (2021). COVID-19 and the Cyber Challenge. *The Cyber Defense Review, 6*(2), 17-28. https://www.jstor.org/stable/27021373[Accessed 11 October 2021].

[19]https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBER CRIME_AND_COVID19_-[Accessed 12 October 2021]_Risks_and_Respon

"Cyber crimes have one up by almost 500% in India during the global pandemic. We need to consider the emerging threats from new technologies such as drones, ransomware, internet of things devices (IoT) and also the role of nation states in such cyber attacks. The lockdown, which witnessed adoption of inter-connected devices and hybrid work environment, has increased our dependence on technology. This renders us digitally more vulnerable than ever before"- Former Chief of Defence Staff (CDS) Late General Bipin Rawat[20].

With pandemic disrupting businesses and with remote working becoming reality, cyber criminals have been busy exploiting vulnerabilities. Year 2020 saw one of the largest numbers of data breaches and the numbers seem to be only rising.

According to Kaspersky's telemetry, when the world went into lockdown in March 2020, the total number of bruteforce attacks against remote desktop protocol (RDP) jumped from 93.1 million worldwide in February 2020 to 277.4 million 2020 in March—a 197 per cent increase. The numbers in India went from 1.3 million in February 2020 to 3.3 million in March 2020. From April 2020 onward, monthly attacks never dipped below 300 million, and they reached a new high of 409 million attacks worldwide in November 2020. In July 2020, India recorded its highest number of attacks at 4.5 million.

In February 2021—nearly one year from the start of the pandemic- there were 377.5 million brute-force attacks—a far cry from the 93.1 million witnessed at the beginning of 2020. India alone witnessed

---

ses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf

[20]https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece [Accessed 12 October 2021].

9.04 million attacks in February 2021. The total number of attacks recorded in India during Jan & Feb 2021 was around 15 million.[21]

Like most organisations, crime also went digital during the pandemic. As per the National Crime Records Bureau (NCRB) report for the year 2020, cyber crime surged 12% across the country, even as other crimes such as murder, theft and cheating witnessed a drop due to the national and regional lockdowns. Basically, cybercrime is on the rise because it is regarded to be the easiest method to commit a crime, and people who have a lot of computer expertise but are unable to find work or do not have a lot of money turn to this source and begin abusing the internet. It is simple for cyber criminals to gain access to data from here and then use it to withdraw money, blackmail, or do other crimes. Cyber thieves are on the rise because they don't see much of a threat and because they are so well-versed in the networking system that they believe they are safe. They are also the ones that create phoney accounts and then commit crimes.

As per NCRB report, A total of 50,035 cases were registered under Cyber Crimes, showing an increase of 11.8% in registration over 2019 (44,735 cases). Crime rate under this category increased from 3.3 in 2019 to 3.7 in 2020. During 2020, 60.2% of cyber-crime cases registered were for the motive of fraud (30,142 out of 50,035 cases) followed by sexual exploitation with 6.6% (3,293 cases) and Extortion with 4.9% (2,440 cases)[22] Most of the increase in cyber crimes came from states such as Telangana and Maharashtra while cases from the top 20 major cities rose by only 0.8%, suggesting more people were being targeted in smaller cities. The total rate of cyber crime per 100,000 people increased from 3.3 to 3.7 in

[21] https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html [Accessed 12 October 2021].

[22] https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf [Accessed 15 October 2021].

2020.[23]Cases of cyber crime recorded an 11.8% increase in 2020, a year when most rates of serious crimes fell, the Crime in India 2020 report shows. Cyber crime sections include several types of crimes that are either carried out using or primarily target computer systems or assets linked to the internet, such as internet banking and email accounts.[24] Hindustan Times has reported that overall, the number of cognizable cases rose by 28% but if Covid-related violations were removed, the number of new cases dropped compared to 2019. Some of the stark reductions were in cases of kidnapping and abduction, which fell by 19.3%, crime against women (down by 8.3%), crime against children (down by 13.2%) and crime against senior citizens (down by 10.8%). The murder cases increased by one percent.

But in case of complaints filed under sections dealing with cyber crime, the number of cases registered last year rose to 50,035 from 44,735 a year before. This ties in with trends seen across the world as more people moved to working and studying from home, spending more time with digital tools.

Most of the increase came from states such as Telangana, Assam, Bihar, Odisha, Jharkhand and Maharashtra while cases from the top 20 major cities rose by only 0.8%, suggesting more people were being targeted in smaller cities. The total rate of cyber crime per 100,000 people increased from 3.3 to 3.7 in 2020.

"The picture provided by NCRB on cyber crime is very limited," said Pawan Duggal, an independent expert in cyber security, who has been watching this space for more than two decades. He added that cyber frauds have increased in several countries during pandemic.

---

[23]Reuters; available at https://www.hindustantimes.com/india-news/cyber-crimes-registered-11-8-increase-last-year-ncrb-101631731021285.html [Accessed 21 October 2021]..

[24]Hindustan Times Report-"Cyber crimes registered 11.8% increase last year: NCRB; available at https://www.hindustantimes.com/india-news/cyber-crimes-registered-11-8-increase-last-year-ncrb-101631731021285.html visited on 17th November, 2021

"The ground reality is overwhelming. Every second person would have been targeted by a cyber fraudster. The actual cyber fraud is much higher. The Covid pandemic has turned cyber fraud as a cottage industry, which was once known to be run from Jamtara in Jharkhand, to several other parts of the country,"

To be sure, cyber crime sections include several types of crimes that are either carried out using or primarily target computer systems or assets linked to the internet, such as internet banking and email accounts.

Duggal's allusion was to financial frauds that target citizens by fooling them into sharing sensitive credentials like one-time password (OTP). State police departments have identified several hotbeds of including Bharatpur in Rajasthan, Deoghar in Jharkhand, Gwalior-Chambal region in Madhya Pradesh, Palgar in Maharashtra and Noida in Uttar Pradesh.

Officials in Rajasthan said police opened a dedicated cyber police post in Bharatpur on Rajasthan-Uttar Pradesh border, where police from at least 22 states have visited since January 2021. About 40% of cyber fraud cases reported from Hyderabad was traced to Bharatpur.

Steps Taken to Deal with Cyber Crime and Cyber Security

The COVID-19 pandemic has generated remarkable and unique societal and economic circumstances leveraged by cyber-criminals. The COVID-19 pandemic, and the increased rate of cyber-attacks it has invoked have wider implications, which stretch beyond the targets of such attacks. Changes to working practises and socialization, mean people are now spending increased periods of time online. In addition to this, rates of unemployment have also increased, meaning more people are sitting at home online- it is likely that some of these people will turn to cyber-crime to support themselves. The combination of increased levels of cyber-attacks and cyber-crime means there may be implications for policing

around the World- law enforcement must ensure it has the capacity to deal with cyber-crime.[25]

Central Government has taken steps to spread awareness about cyber crimes, issue of alerts/advisories, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities etc. to prevent such crimes and to speed up investigation. The Government has launched the online cybercrime reporting portal, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. The Central Government has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

'Police' and 'Public Order' are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against the cyber crime offenders.

Further, Government has taken several steps to prevent and mitigate cyber security incidents. These include:

(i) Establishment of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.

(ii) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(iii) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.

---

[25]Collier. B., Horgan. S., Jones, R., & Shepherd, L. (2020). The implications of the covid-19 pandemic for cybercrime policing in scotland: a rapid review of the evidence and future considerations. *Scottish Institute for Policing Research.*

(iv) Issue of alerts and advisories regarding cyber threats and counter-measures by CERT-In.

(v) Issue of guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(vi) Provision for audit of the government websites and applications prior to their hosting, and thereafter at regular intervals.

(vii) Empanelment of security auditing organisations to support and audit implementation of Information Security Best Practices.

(viii) Formulation of Crisis Management Plan for countering cyber attacks and cyber terrorism.

(ix) Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

(x) Conducting regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.[26]

Apart from the aforementioned, there needs to be a number of steps on the part of general public using computer systems. These steps would include first that the computer systems must be protected. Firewall and antivirus applications are vital security software. User must make sure all of your programmes are up to date and patched. Consumers only update their security software every 8.5 months, according to a Get Safe Online poll.

It should also be ensured that passwords are strong. Passwords of at least eight characters and a mix of upper and lower case letters, numbers, and symbols are considered strong. Keep your passwords safe and don't use the same one for all of your services and accounts.

---

[26] https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226 [Accessed 21 October 2021].

Passwords should be changed every 90 days.Wi-Fi in public places should be disregarded. When utilizing public Wi-Fi, never make online payments, email personal information, or introduce crucial account passwords. Cyber thieves establish networks that appear to be free internet but give them access to your personal information.Unsolicited emails and SMS communications should be avoided. A user should never click on a link, picture, or video sent to you by an unknown source. Check for spelling errors, bad language, unusual phrasing, and urgent requests for money or action to ensure that emails are authentic. Verify correspondence by personally contacting the sender. Also, be sure that the websites you're looking at are reputable. Malicious websites may appear to be identical to legal sites, however the URL is frequently misspelt or uses a different domain.

Protect personal information on social media- Cybercriminals utilise social media to gather personal information that they may subsequently exploit in phishing schemes. Before you provide personal information like your name, home address, phone number, or email address, think again. Limit physical access to critical information by turning off your computer while you're not using it. To keep private data safe, lock mobile devices and encrypt confidential data. Limit who in your workplace has access to certain network drives. All gadgets should be used with caution. Phones and other mobile devices are popular targets. Always be mindful of where your mobile devices are; they should never be left unattended and visible. Review your bank and credit card accounts on a regular basis. According to research, discovering identity theft and online crimes early reduces the effect. Do not amass a collection of computers or digital data- Keep digital data organized and up to date, and delete files on a regular basis. Dispose of old or unneeded computer hard drives in a secure manner at your office.

Legal Remedies

The Information Technology Act of 2000 subsequently revised in 2008, was enacted to set limitations for these types of attackers when it came to committing Cyber-crimes. For laypeople, this is known as

the Cyber-law. This Act establishes sanctions and compensation for offences involving technology. When a person is a victim of a cybercrime, he has the option of going to court to pursue legal action against the perpetrator.

The victim has the right to file an appeal in court for compensation for the wrong done to him under section 43A of the Information Technology Act of 2000, as this section covers the penalties and compensations for offences such as "damage to the computer, computer system, or computer networks, etc."Anybody corporate that deals with sensitive data, information, or maintains it on its own or on behalf of others and negligently compromises such data or information will be liable under this section and will be required to pay compensation according to the court's discretion.

Section 65 of the Act covers the punishment for the offences which involve "tampering with computer source documents", where according to the section, "Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both".

There are still some gaps in the IT Act of 2008 since there are new and unknown cyber-offenses for which the law needs to stretch its arms and tighten its grip.

Here are also offences that are not covered by the IT Act because they are already covered by other laws, such as "Cyber-defamation," which is governed by the Indian Penal Code, 1860. The term "Defamation" and its punishment are defined under this Act, so there is no need for a separate definition elsewhere because the impact of such an online offence is the same as it is offline.

We are living in the twenty-first century in a developing country, where technology is progressing and humans are being displaced

from their jobs. As a result of the increased use of the internet, the rate of online crime is growing as well, for which the victim has legal recourse.

However, we've seen that the number of cyber-crime case files is growing faster than the number of solved cases, which is attributable to people's negligence and a shortage of cyber professionals who can handle these situations. As a result, we require better training institutions as well as a mandatory branch of Cyber-security topics that will aid in the resolution of cyber-cases and increase trust in security; nonetheless, we can attempt to safeguard ourselves. No institution or anti-virus can totally safeguard someone, but by using the measures described above, we can secure our information, data, devices, and ourselves.

Prevention of Cyber Crime against Women and Children

Ministry of Home Affairs had constituted an Expert Group comprising of the official/ academicians from NSCS, Ministry of Home Affairs, CDAC Cert-In, Indian Institute of Technology, Indian Institute of Science and IT experts to study the gaps and challenges, prepare a roadmap for effectively taking of Cyber Crime in the country and give suitable recommendations to take effective measures to prevent crime against women and children and create awareness in the society about these issues.Accordingly, a scheme for Cyber Crime Prevention against Women and Children (CCWC) has been formulated by the Ministry of Home Affairs.The proposed scheme was examined by NCW.

Some of the inputs put forth by the Commission were as below:

- Online Women specific Crime Reporting Unit -Interlink with NCW should be made in such a manner that if a woman wants to make a complaint about cybercrime to NCW, it should be sent to MHA Crime Reporting Unit with acknowledgement to NCW and a copy to the complainant. It will encourage quick disposal of the complaints that too with the assistance of the IT professionals

- Monitoring Unit for Cyber Crimes-Monitoring unit should provide monthly reports on the complaints received through NCW
- National Forensic Laboratory-Investigations of crime against women are delayed due to pending reports from forensic laboratories so NCW agreed to it.[27]

The dramatic increase in the rates of cyber crime is also partly attributable to the inadequacy of the legal framework in delegitimizing such activities. The face of cyber crime has undergone transformational change in the last few years. Thus, a re-look at the ability of the Information Technology Act, 2000 to address the nuances of cyber security, as well as accommodate newer technologies like quantum computing and artificial intelligence, is the way forward.

[27]http://ncw.nic.in/ncw-cells/legal-cell/new-bills-laws-proposed/cyber-crime-prevention-against-women-and-children-ccpwc[Accessed 21 October 2021].