SUPREMO AMICUS

VOLUME 29 | MARCH, 2022 ISSN 2456-9704

CYBER CRIMES DURING COVID - 19 PANDEMIC IN INDIA AND WORLD

By Arushi Sharma
LLM from SLS Noida

By Shivanshi Gupta
LLM from O.P. Jindal

ABSTRACT

The Coronavirus epidemic has resulted in increased online communication, business, and personal relationships. But cybercrime affects both the public and law enforcement. The COVID-19 epidemic threatens both individuals and society. We all rely on computers, mobile devices, and the Internet to deal with the repercussions of social estrangement during a crisis. Malicious actors have exploited these weaknesses. Financial cybercrime is on the rise as the country fights with the COVID-19 pandemic. Increased internet activity due to remote schooling and Work from Home is increasing security failures. For example, phishing (false websites posing as COVID-19 resources or leads for hospital beds/oxygen cylinders), online sales of counterfeit pharmaceuticals, and bank fraud through sham versions of the 'PM CARES Fund' have all occurred during the second COVID-19 wave. It's a national issue. Around 330 million people in ten countries, including India, had been victims of cybercrime in the last year, and over 55 million had been victims of identity theft. These shocking statistics underline the need for a global effort to limit the growth of cybercrime. However, India, which is gradually becoming one of the main hubs for such operations, must first take critical legal, technological, and policy safeguards. To hold individuals who use the COVID-19 pandemic for criminal benefit accountable, the criminal justice system must work together to identify, investigate, attribute, and prosecute the above offences. Legitimate crowd-funding campaigns for hospitals have been misdirected to alternate criminal pockets via fake websites in recent weeks. However, there are steps that consumers and businesses can take to assist reduce the danger of assault. To avoid using the same password on several websites, users should be wary of phishing emails and websites, practise good cyber hygiene, only use trusted wi-fi networks, and consider using a password manager. It is also vital to use two-way communication before sending or downloading any files from an email that may include malware. Verify the sender's identity by texting, calling, or sending a WhatsApp message. Instead of clicking on email links, go to reliable websites. In a group conference call, don't share screens or provide screenshots that include sensitive data. Set up secure remote access to the organization's files, provide enough protection, and ask personnel not to use personal computers while working. Finally, send employees to cyber-security training sessions to improve their skills. Now is the time to develop a strong global system to combat cybercrime. Protecting India's vital information infrastructure and its citizens from the perils of digitalization requires improved regulation and enforcement. A new National Cyber Security Strategy (NCSS) for 2021 may assist the government better reconcile outdated cybercrime policies to rapid technological change. The NCSS 2021 must take a proactive rather than reactive strategy to mitigate cybercrime risks and impact. The most critical step is to ensure victims may

easily obtain information. To improve India's cybercrime complaint-to-FIR conversion ratio, authorities must be held more accountable. The legal framework's weakness in delegitimizing such conduct contributes to the massive surge in cybercrime. Cybercrime has evolved considerably in recent years. Recalibrate the Information Technology Act so that it can accept more cutting-edge technology like quantum computing and artificial intelligence. It's also hard to ignore the business sector's role in preventing and managing cybercrime. Enterprises must prioritise data and intellectual property security. Reengineering security procedures and increasing budgets for anti-fraud technology expenditures are urgently required. Companies must do frequent risk assessments and present staff with current security information. Due to India's rapid expansion in the cyber security field, partnerships with Indian start-ups are important. The pandemic has changed many things. Immediate action is required to address the underlying concerns. In the last year, cybercrime has increased, revealing the flaws in our digital infrastructure and the policing system in place.

Keywords: cybercrimes; covid -19. Information Technology Act, NCSS 2021, phishing, cybersecurity, PM Care fund, FIR, Intellectual Property.

INTRODUCTION

One of the most pressing issues of our time is how to keep our personal information safe and secure in this age of globalisation. As a landside revolution takes place, cybercrime continues to rise at an alarming rate. Do we have a solution to these cybercrimes despite the efforts of so many governments and organisations? This is one of the world's most pressing issues, but no long-term solution has yet been found. IT Act defines "a criminal act done with the use of computers as a tool or for targeting it" as cybercrime. It is assuming the place of unlawful access to a computer system without the true owner's knowledge or consent. Phishing, spoofing, DoS (Denial of Service) attacks, credit card fraud, online transaction fraud, cyber defamation, and child pornography are among the most prevalent and trending cybercrimes. COVID 19, a highly contagious and lethal virus, governments around the world were forced to implement lockdowns and social seclusion measures. As a result, many people were compelled to work from home, fostering a work-from-home culture reliant on online shopping, banking, and other electronic services. At first, COVID 19 was a curse for humanity, but it soon became a gift for those who wanted to take advantage of Information Technology in the form of cybercrime attacks such as social engineering. There are no geographical boundaries to cybercrime, so it can be committed from anywhere in the world. It is imperative that countries, including India, remain prepared with proper legislative measures in order to resist the threat. Long arm statutes like the Information Technology Act, 2000 (hence referred to as IT Act, 2000) have jurisdiction over violators in other jurisdictions, and those who aid or attempt cybercrimes governed by IT Act, 2000 face penalty. The IT Act of 2000 does not preclude the use of other legal mechanisms to seek redress, and those mechanisms themselves may be invoked as part of a legislative response. Nearly a year after the epidemic began, there were 377.5 million brute-force attacks in February 2021, a significant increase from the 93.1 million

recorded at the start of 2020. Cyber fraudsters have been busy exploiting vulnerabilities in the wake of the epidemic and the rise of remote working. A record number of data breaches occurred in 2020, and the trend appears to be continuing. From 93.1 million RDP brute force attacks worldwide in February 2020 to 277.4 million in March 2020, according to Kaspersky's telemetry, the number of RDP brute force attacks increased by 197%. In February 2020, there were 1.3 million people in India, while in March 2020, there were 3.3 million people. Monthly attacks never dropped below 300 million from April 2020 onward, and in November 2020 they hit a new peak of 409 million worldwide. The number of attacks in India will reach 4.5 million in July 2020, the greatest amount ever recorded. There were 377.5 million brute-force attacks in February 2021, about a year after the start of the pandemic, compared to just 93.1 million at the beginning of 2020. In February 2021, there were 9.04 million attacks in India alone. During the months of January and February of 2021, India recorded over 1[illegible] million attacks. In light of the COVID 19 epidemic, it is vital for legislative adjustments to take into account select but widespread cybercrimes. Employees must take great care of the company's data and keep it out of the hands of family members and friends in order to prevent the misuse of data or the leak of secret information. A growing number of Cyber Attacks puts at danger not just corporate data but also the private and sensitive information of individuals, including their financial information. In the wake of the epidemic, cybercriminals are increasingly turning to data as a weapon against national security, necessitating the passage of data protection legislation. The Personal Data Protection Bill, which was introduced in Parliament two years ago, has yet to be passed. There are no provisions in the Information Technology Act, 2000, which dealt with cybersecurity and cybercrime, to take into account the most recent developments in business practises and the methods by which crimes in cyberspace are perpetrated. In the wake of the epidemic, cybercriminals are increasingly turning to data as a weapon against national security, necessitating the passage of data protection legislation. The Personal Data Protection Bill, which was introduced in Parliament two years ago, has yet to be passed. There are no provisions in the Information Technology Act, 2000, which dealt with cybersecurity and cybercrime, to take into account the most recent developments in business practises and the methods by which crimes in cyberspace are perpetrated.[1]

1. TYPES OF CYBER CRIMES IN COVID-19

1.1.*Infections by spyware, malware, ransomware, and COVID 19*: During the lockdown, internet games like Candy Crush, FarmVille, and Pokemon Go have become increasingly popular. The internet makes this all possible. It is common for users to contribute personal information stored on their phones, laptops, or social media accounts to applications for their services to function. Users frequently need financial

[1] Alawadhi, S.S. & N. (2021). India becomes favourite destination for cyber criminals amid Covid-19. Business Standard India. [online] 5 Apr. Available at: https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html.

information to download apps or use online services. Affirming the government's'stay home, stay safe' campaign, more and more people are using payment gateways to pay their utility bills and insurance premiums online. These actions have increased the frequency of ransomware and malware. A user's login credentials and other personal information are stolen by ransomware via malware. These attacks may cause huge losses and several organisations advise countermeasures and good habits to prevent such attacks. Operating systems and secure programmes provide regular updates to users to correct security holes and add extra protection. Globally, cyber thieves are targeting major hospitals and medical institutions to obtain data on COVID 19, according to a new investigation by the International Criminal Police. India now has over 22 malware kinds. Theft or hacking of sensitive data is prevented by using antivirus software and other security measures on mobile devices, PCs, and apps.[2]

1.2.***Phishing Attacks: EMI moratorium Frauds, Banking Frauds*:** People are recommended to use Internet banking or phone banking to access financial services currently because banks have limited resources. Bank customers are being targeted by cyber criminals who pose as bank officials and ask for personal information such as their account number, credit or debit card number, CVV, OTP, etc. via phishing calls or emails. EMI/Term Loan Installments and Interest/Interest on Working Capital payments would be postponed for three months beginning on March 1, 2020 under the Reserve Bank of India's COVID 19 regulatory package. On the premise that they are discussing the postponement of their EMI payments, cyber attackers are now approaching loan holders and asking them to give an OTP, CVV, password or PIN associated to their accounts in order to take advantage of the moratorium provision. In order to protect yourself, don't click on links or open attachments from untrusted sources, or share personal data with anyone.

1.3.***Rumors or Falsehoods*:** Fake news and rumours have also developed as a major problem in the United States. Rumors and their consequences are examined in the following sections. During the lockdown, there were also rumours that the administration planned to decrease pensions by 30%. Many rumours about the COVID19 virus turned out to be unfounded and were spread solely for the purpose of frightening people. A hoax article claiming to list a cure for COVID 19 was widely disseminated. It's not just unethical, but it might also have serious ramifications for those who hear it. Maharashtra and Karnataka Cyber Police have decided to take harsh action against anyone seen spreading false and unverified material about COVID-19 on social media in light of the growing quantity of fake news. Misinformation that is shared on Whatsapp groups will be held accountable by the 'Group Administrator' and penalised by law if it is proved to have been shared in his/her group. There are efforts being taken by the Indian government, social media, and the police to

[2] Indo-Asian News Service. (2019). *Hackers attack Indian healthcare website, steal 68 lakh records*, *India Today*. Available at: https://www.indiatoday.in/crime/story/hackers-attack-indian-healthcare-website-steal-68-lakh-records-1590345-2019-08-22 (Accessed: February 26, 2022).

stop the spread of rumours. The Indian government has set up a WhatsApp chatbot to answer questions from citizens and dispel rumours about the coronavirus outbreak. It's not the first time Facebook has attempted to combat the spread of rumours by creating a chatbot for India. India's Cyber Crimes are regulated by the Information Technology Act, 2000 (as modified). The e-governance department of India's Ministry of Communication and Technology is also promoting new COVID19-controlling apps. As a result, it is important to exercise caution and responsibility when distributing or distributing company data, as well as before posting any message on social networking sites. India does not have sole provision on criminalising fake news, thus certain other laws may be relied upon. There needs to be stricter reporting requirements for intermediates like Google, Facebook and Twitter because so much information is exchanged through them. The Intermediary Regulations 2011 should be updated to require more thorough due diligence from intermediaries. Technical support and all facilities to agencies (Central government or its authorised officer) are also required under section 69B (2) by these intermediaries to enable, provide, and aid online access the computer resource involved in distributing bogus COVID 19 news. Besides the IT Act of 2000, news about misleading warnings that cause panic should attract the Disaster Management Act of 2005. As a precaution, several law enforcement agencies issued a special order reminding people to observe the curfews imposed by them during the COVID 19 shutdown and to avoid causing confusion in the minds of people regarding the order's execution and therefore causing disobedience of the order disseminated. An offence under section 188 of the IPC 1860 was punishable by law. Misleading video clips were another danger posed by the spread of fake news on social media, which incited community violence and hatred. The government has the legal authority to restrict public access to such materials. In addition, the **Epidemic Diseases Act of 1897,** gives the authority to adopt regulations and orders, including those that control and prevent the dissemination of false information. Punishment is meted out for those who break the rules. Global research by Reuters Institute found the following COVID-19-related subjects as the most common in the rise of fake news and misinformation: public official's action; community has grown; Medical and scientific news; High-profile actors Explanations for Transmission of the Virus; Preparation of the public and Development of vaccines.[3]

1.4.*Online Impersonation* : Pandemic paralysed much of the world's economies, but those organisations that provided important services or could run their operations via the internet were able to carry on as usual. Virtual offices began to take shape as a result of video sharing platforms, social media, and other online tools. Impersonation of systems such as Zoom, Cisco, and others was part of this. In the same way, domain names imitating the World Health Organization and other health organisations grew rapidly. These were typical phishing cases, punishable by Section 66-D of the IT Act, 2000, which punishes for cheating by personation through computer resources, and

[3] Cybercrime & digital threats. (2020). *Trendmicro.* Available at: https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/ (Accessed: February 26, 2022).

Section 415 of the IPC 1860, which punishes for cheating. Data privacy is being violated by this type of impersonation, which aims to obtain personal information from the victims. Currently, the Indian Penal Code, 1860, and the Information Technology Act, 2000, both permit charges to be filed at the same time. Cyber squatting and typo squatting were the result of large domain name registrations. The lack of an explicit provision for punishing cyber squatting does not mean that the same should not be protected. Laws governing 'passing off' can, of course, help to keep them safe. Scams like this are on the rise because domain name registrants aren't doing enough background checks before allowing registration. Requests for registration of domain names that appear to be similar to established and legitimate domain names, such as during a pandemic, should be taken with significant caution. Targeted by cyber criminals are Zoom Domains. Slightly more evidence or proof than is customary should be collected when requests are this dubious. This will allow registration to proceed more smoothly. So, whether the request comes from a corporation or a Limited Liability Partnership, the registered deed of incorporation is required; if it comes from a private individual or a company, the Memorandum of Association is necessary; and so on. Bogus emails from the World Health Organization, for example, were also seen in addition to the fake domain names. In order to spy on and gather information from the victim, the attacker planted key loggers (a sort of computer contaminant) in these emails. An online payment gateway login ID and password can be used to steal money from a victim's bank account. Fraudulent or dishonest use of a user ID and/or password is punishable under Section 66C of the IT Act, 2000, and the attacker is also guilty of a felony under Section 43(c) of the IT Act, giving the victim the right to sue and seek restitution. Using email breach tactics, fraudsters have recently been using them to buy gift cards, avoid tax refunds, and other financial transactions. Despite the fact that impersonation is a key weapon in carrying out such attacks, the most important trap for victims has been fake business grants and loans in the wake of COVID 19 or a warning that an individual has come into contact with a COVID positive patient or a fake email asking for a transfer of money to be made in a different account due to an audit of coronavirus.[4]

1.5. ***Internet chaos and terror are fueled by Covid 19 frauds***: Section 420 of the Indian Penal Code (IPC) deals with fraud, and a contract entered into as a result of deception is voidable under the law. The corona virus prompted people to search for ways to safeguard themselves. To exploit this, fraudsters sold what they claimed was anti-virus software to protect victims' devices from the corona virus, but it was actually malware designed to infect the device. Section 43(c), 66 of the IT Act, 2000 can be used to deal with this. Counterfeit medicines/drugs and medical equipment were also sold online at inflated prices. Complaints may be filed in order to prevent an immediate threat. Scams claiming to raise money for health institutions were used to con individuals out of their money by claiming that the funds will be used for that purpose. There is no formal set of legislation

[4] *Growth in Cyber-Crimes in the COVID-19 times and Fragile Cyber Laws in India*. (2021). Latest Laws. Retrieved February 26, 2022, from https://www.latestlaws.com/articles/growth-in-cyber-crimes-in-the-covid-19-times-and-fragile-cyber-laws-in-india.

for crowd fundraising in India, hence crowd funding falls under the purview of SEBI's consultation paper on the subject. As a result, legislation governing crowd fundraising is required.[5]

1.6.***Privacy Violations in Health Apps:*** Because of the high contagiousness of the coronavirus, it was necessary to quarantine any locations where COVID 19 positive patients might be found. Counting the number of affected people in the area helped determine the severity of the threat, which allowed officials to restrict outdoor activities. Apps that provide location-specific data for COVID 19 positive patients have been flooding in. Many of these programmes were used to commit fraud by installing malware and trojans designed to steal sensitive data, damage computers, or divert funds to a different bank account than the one intended. Aarogya Setu, a government-backed COVID 19-related app, was helpful for cyber criminals since it allowed them to create identical and fraudulently similar apps in order to deceive their victims. Phishing, spreading computer contamination, criminal trespass, stealing, etc. are all examples of these crimes. In spite of their effectiveness, penal codes are rarely used to penalise crimes of computer tampering, despite the fact that they are quite effective. The problem of privacy with the State-sponsored COVID 19 software is just another cause for concern. It is possible to gather a huge amount of personal information with GPS and the app. [6]

1.7.***COVID 19 spamming:*** E-commerce and online delivery of products have led to a spike in spam email inviting recipients to pick up their orders at an address specified in the attachment. These spam messages install a remcos backdoor or spyware (a contaminant) and connect the PC to a botnet. Under the IT Act, 2000, India does not have a distinct legislative provision. As a result of **Shreya Singhal Case(2015),** there is uncertainty as to how much or how little of the provision was thrown down; In the absence of guidance, law enforcement agencies are stymied in their efforts to combat the threat. However, the Law of Torts acknowledges the torts of nuisance and trespass if an individual has to seek redress in these situations. Spam mails infringe on computer systems, resulting in irritation and inconvenience. There are two ways to get compensation: through the established legal process or by suing for compensation in court. In order to properly apply Tort law, mailboxes and cyberspace must be considered property as well. As with spamming, the section 268 of the Indian Penal Code 1860 can be used when a large number of people are subjected to it. Section 268 of the IPC 1860, which governs the extent and breadth of annoyance to the public, should be extended to spam mails. A separate provision or piece of legislation to combat spam, on the other hand, remains essential.[7]

[5] Dewan, D. M. (2020, April 25). *COVID 19 Lockdown: Increasing Cyber Crimes in India*. Lexology; RK Dewan & Co. https://www.lexology.com/library/detail.aspx?g=f33f6b37-6b62-425a-852b-0be29cbe46a7.

[6] A&A. (2021, December 15). *Data Protection and Privacy – Cyber Security Laws in India*. Ahlawat & Associates. https://www.ahlawatassociates.com/blog/data-protection-and-privacy-cyber-security-laws-in-india/.

[7] *Developing story: COVID-19 used in malicious campaigns*. (2020). Trendmicro.Com. Retrieved February 26, 2022, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

1.8. Online Pornography: Online pornographic content consumption has risen unexpectedly, particularly during the government-imposed lockdown period caused by COVID 19. Private online shows with sexually explicit content were made public because of social distancing rules. A specific legislation in India punishes online pornography and obscenity as well as the breach of women's physical privacy, despite the fact that viewing porn is not illegal. Furthermore, Section 2000 of the IT Act similarly prohibits and serves the same objective. In India, online viewing of child sex abuse material has risen nearly twice as fast as the number of people accessing it. Laws against child pornography and the prosecution of child pornography are specifically addressed in the statutes. The law controlling child pornography is substantially tougher than that which governs online pornography in general. It is not a criminal to see porn, but some specific behaviours have been declared unlawful by law. It is also possible to rely on POCSO legislation requirements in this way. As per the new guidelines, intermediaries must use caution when dealing with obscene, pornographic, or paedophilic content.[8]

1.9. In the wake of the corona epidemic, the number of cyber-attacks on businesses has multiplied many times over, according to a new Pricewaterhouse Coopers analysis. As a result of the recent hacking spree, many companies have implemented a virtual private network (VPN). The software of the companies is being hacked by hackers in order to acquire access to all of the company's valuable information and data. For phishing attacks on businesses, the usage of pre-made malware called 'AZORult' has increased. Unwanted software has attempted to enter corporate systems in the hopes of stealing or delivering malicious payloads. PAN Cards, GST numbers, phone numbers, and email addresses have all been targeted by hackers in an attempt to get access to the Indian State Tax Department's servers. The hackers have made a number of attempts to reach the brokerage through banks and stock markets. Hackers have also targeted the PM's COVID fund.

1.10. In addition to assaults on local hospitals and testing centres in the United States, the World Health Organization (WHO) has also been the target of cyber-attacks in an attempt to acquire the credentials of WHO employees. An increasing number of hospitals and other testing facilities have been hit by ransomware attacks, when patients' essential files are seized and not returned until the ransom is paid. To keep tabs on the corona patients, hospitals have been warned of ransomware websites posing as government-advised watchdogs.[9]

[8] The Economist. (2020, May 10). Pornography is booming during the covid-19 lockdowns. *Economist (London, England: 1843)*. https://www.economist.com/international/2020/05/10/pornography-is-booming-during-the-covid-19-lockdowns.

[9] *Who.int*. (2020). Available at: https://www.who.int/docs/default source/coronaviruse/situation-reports/20200211-sitrep-22-ncov.pdf?sfvrsn=fb6d49b1_22020 (Accessed: February 26, 2022).

2. OTHER INSTANCES OF CYBER CRIMES INDIA AND IN WORLD[10]

1. Mobikwik's latest data breach is an example of this. 3.5 million people were said to have been affected by the data breach, which exposed personal information like as addresses, phone numbers, Aadhaar cards, and PAN cards. This data leak has been denied by the corporation thus far. Following an order from Reserve Bank of India (RBI) to perform a forensic audit and submit a report, Mobikwik has been working with appropriate authorities ever since. There can be no guarantee that your information will not be accessed by anybody other than those who have a need to know about it, according to the company's privacy policy. As soon as we learn that your information has been released in a way that is inconsistent with this Privacy Policy, we will notify you as soon as we are able and permitted by law of the type and extent of the disclosure. There was no notification given to any of the people whose data ended up on the dark web. Data breaches disclosed by security firms or cybersecurity researchers are included in the box titled "Recent data breaches in India." The information was not made public by any of the companies, and neither were their consumers or the media.

2. Customers are being contacted by scammers pretending to be Airtel personnel, he added this could be due to an incomplete Know Your Customer (KYC) form. In order to avoid being defrauded, customers may be asked to download and install the "Airtel Quick Support" app from Google Play. The fraudster can remotely control a victim's device and the accounts linked to it using the TeamViewer Quick Support programme. As a result, if the consumer decides to install the device, the fraudster will be able to access all of the accounts linked to it. Additionally, the scammers make phone calls to the victim, professing to be interested in purchasing a pre-owned item from the website, and then ask for the victim's UPI information so that they can send money to their own account. SMS link is given to the customer's phone to authorise the transaction, which debits the money from the account rather than crediting it.[11]

3. There are serious ramifications to a ransomware attack on the Colonial Pipeline, such ransomware attack on Colonial Pipeline, operator of the largest petroleum pipeline in the U.S., in May 2021 was one of the most significant cyber attacks in recent years, even if it had no effect on UK petrol outlets. In fact, it may have finally sparked a concentrated effort against ransomware criminals. According to our initial coverage of what happened immediately following the terrorist attack, a federal emergency was declared, and in order to improve flexibility in the supply chain for fuel, the Department of Transportation temporarily relaxed regulations governing how long truckers could be behind the wheel.

[10] Scroxton, A. (2021) *Top 10 cyber crime stories of 2021*, *ComputerWeekly.com*. Available at: https://www.computerweekly.com/news/252510733/Top-10-cyber-crime-stories-of-2021 (Accessed: February 26, 2022).

[11] PTI. (2021, May 20). Rise in cyber fraud amid pandemic; working relentlessly on user safety: Airtel CEO. *Deccan Herald*. https://www.deccanherald.com/business/rise-in-cyber-fraud-amid-pandemic-working-relentlessly-on-user-safety-airtel-ceo-987973.html.

4. The Kaseya ransomware robbery by the REvil team is demanding $70 million in ransom. As part of a traditional supply chain hack, the REvil ransomware gang demanded a total of $70 million in ransom from over 1,000 firms after locking their IT systems after the group breached services provider Kaseya. Because of the severity of the attack on the REvil network, the organisation was forced to go into hiding until it was discovered by law authorities that their network had been hacked. Several gang members are either in custody or on the run. One faces extradition to the United States.

5. BlackMatter gang attacks many victims with greater intensity. Ransomware gangs come and go for a variety of reasons, but one thing is for sure: There will always be someone else eager to take their place. In September, we reported on a wave of attacks against various targets by the emerging 2021 ransomware group known as BlackMatter, prompting concerns from the security industry.

6. A huge ransomware attack has devastated the Irish healthcare system. Contri ransomware gained headlines on May 14 when it infected the networks of the Irish Health Service Executive in a heinous and inhuman cyber attack. Many patients were unable to receive treatment because of the incident, and the army was called in to help. Fortunately, no one was killed as a direct result of the incident, but the service hasn't entirely recovered during the past six months.

7. The stolen Covid-19 vaccination data from Pfizer/BioNTech was leaked. When information about the Pfizer/BioNTech Covid-19 vaccine was published online in January 2021 as a result of a cyber attack on the European Medicines Agency in December 2020, cyber thieves did their hardest to sabotage the rollout in Europe. Documents including PDFs and PowerPoint presentations were included in the data dump in addition to screen pictures taken from emails.

8. After the Anom cryptophone software was cracked by investigators in a massive hacking operation, police raids took place around the world. Sixteen countries' police forces conducted raids after intercepting the communications of organised criminal groups in June. Gangs were unaware that the FBI was running an encrypted communications network via which they had been exchanging messages with each other. However, this raid was just one of a number in 2021 that have sparked serious worries about police enforcement's ability to conduct surveillance, as well as their ability to use the evidence they gathered to convict criminals.

9. Conti cyber thieves demand a $2 million ransom from FatFace, a retailer. Following a successful cyber attack on FatFace's servers in January, Computer Weekly reported that the fashion business had paid a $2 million ransom to the Conti ransomware group. After a lengthy negotiation, the ransomware operators agreed to lower their initial demand to $8 million, or around 213 bitcoin at the current exchange rate.

10. Inadvertently exposing false Amazon review data. Seeing in May that cyber crooks and fraudsters are also terrible at operational security was encouraging for Computer Weekly, which has repeatedly highlighted data loss instances at organisations that failed to secure their databases adequately. More than 13 million entries in an open ElasticSearch database were accidently

revealed by this unhappy fraudster and in doing so uncovered an extensive and widespread phoney review scam that involved hundreds of third-party Amazon sellers.

11. Acer's $50 million ransomware demand is the highest ever, according to Acer's CEO. Perhaps members of the REvil ransomware group were inspired by Roy Castle and Cheryl Baker, who taught a generation of British kids that records are meant to be broken. Regardless, the $50 million ransom demand made against Acer, a PC manufacturer, was the biggest ever made for a period of time. Computer Weekly's sister publications LeMagIT and SearchSecurity were important in finding and reporting the ransomware demand in the record-breaking double-extortion attack that revealed in March.

12. Ransomware gangs are looking for persons with interpersonal abilities in order to negotiate a payment plan. Finally, in July 2021, we reported on how ransomware operations were putting together their operations, seeking out specific manpower and skillsets, as a result of the increased sophistication of the cyber criminal underground. Some gangs are becoming more and more like corporations, with several responsibilities and even outsourced victim bargaining. With the aim of sweet-talking their victims into paying, gangs have a clear need for persons with strong interpersonal skills.

4. OTHER COUNTRIES CYBER LAWS[12]

India's cyber regulations are far less developed than those in the United States and Europe. A variety of laws are in place in the US to deal with this issue, including the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, and Cyber Intelligence Sharing and Protection Act. In addition, all states in the United States have the authority to create additional laws and regulations as necessary. Canada, like the United States, has very severe regulations in place to combat cybercrime. Online crimes against hospitals, testing facilities, laboratories, and clinics are the subject of separate health sector privacy rules. To combat phishing and hacking, the Personal Information Protection Act and the Electric Documents Act were passed. Anti-fraud centre in Canada is formed to combat marketing frauds. Several European countries have ratified the Budapest Convention on Cyber Crime, which is a major step toward strengthening cyber-laws against online fraud. Privacy and confidentiality breaches, as well as hacking into computer systems and stealing personal information are all criminalised by the treaty. England, Russia, and Brazil, for example, have effective laws and mechanisms in place to combat cybercrime. While not a member of the Budapest Convention, India has not established any processes for tracking down and apprehending cyber offenders. While the 2013 National Cyber Security Policy planned to create a workforce of 500 thousand competent experts, this goal has yet to be met. The number of ethical hackers in India is

[12] Is COVID-19 changing the cybercrime landscape?. *Chatham House – International Affairs Think Tank.* Retrieved February 27, 2022, from https://www.chathamhouse.org/2021/02/covid-19-pandemic-and-trends-technology/03-covid-19-changing-cybercrime-landscape.

significantly greater than the number of experienced IT professionals who work for the cyber police.

5. EXISTING INDIAN CYBER LAWS LACUNA[13]

The lack of a defined definition of cybercrime in any act or law in India is the root of the problem. In spite of the IT Act of 2000's provisions for legislation and remedies, many questions remain. Copyright, trademark infringement, and other forms of intellectual property ownership are all included in this category. Hacking and internet fraud are the only areas that cover the scams against large corporations, and hence they must be classified as such. There are no specific policies in place to deal with cybercrime targeting the healthcare industry. Another key issue that is not particularly addressed by any cyber legislation is that of territorial jurisdiction. Because cyber crimes are committed on computers and the internet, the hacker may be located in a different state, making it difficult to determine jurisdiction. Another issue is the preservation of evidence. The deletion of evidence is made simple by the fact that the vast majority of data and proofs are stored online and in systems. In addition, existing rules are confined to theoretical sanctions because it is difficult to pursue the guilty because of anonymity. There are no specific methods to take action against these internet criminals and no strategy to discover these crooks sitting far away in comfort far from the actual place. Everything about ransomware attacks has changed in recent years to become an exercise in "naming and shaming." For a long time before Covid, hackers would encrypt firm data and demand a ransom in exchange for releasing the decryption key. By extracting data first, they can then use that information to blackmail and coerce the firm into paying up or risk having their customer data sold on the dark web if it does not do so. Secure and very impossible to track, Bitcoin appears to be the new preferred payment method. The general state of cyber hygiene is harmed by the absence of well-defined regulatory frameworks and policies for their implementation. Policy improvements are needed for cybersecurity researchers who uncover breaches, as many suffer legal consequences without legislative protection. In order to establish a more robust digital economy, it is necessary to implement cybersecurity legislative laws that serve as guidelines for all parties involved. Mandatory reporting of incidents is also a good idea.

6. FOREIGN POLICY AND INTERNATIONAL LAW: COVID-19[14]

6.1. There are both states and non-state entities taking advantage of the COVID-19 pandemic in cyberspace. There are a number of international law principles that they break, including those requiring them to respect other countries' sovereignty, bans on interference and the use of force, and international human rights law requirements and prohibitions. Both state and non-state actors have been involved in destructive

[13] A&A. (2021, December 15). Data Protection and Privacy – Cyber Security Laws in India. Ahlawat & Associates. https://www.ahlawatassociates.com/blog/data-protection-and-privacy-cyber-security-laws-in-india/.

[14] COVID-19 and international cyber law .(2020). *directions blog*. Available at: https://directionsblog.eu/covid-19-and-international-cyber-law/ (Accessed: February 26, 2022).

cyber operations targeting medical facilities and public health capabilities during the COVID-19 pandemic. Espionage is involved in some operations, such as the claim that China has been actively attacking U.S. research on coronavirus vaccines. Others are criminal in character, such as the ransomware attack on Hammersmith Medicines Research, which had been designated as a UK location for vaccine testing. Many of them cause havoc. A phishing attempt was launched against European supercomputers working on COVID-19 research, while the World Health Organization was the target of another. In addition, there's a lot of misinformation out there. Hundreds of Iranians perished as a result of bogus social media claims that drinking high-proof whiskey would protect them from the illness. One of the most heinous crimes perpetrated by cyberattacks has been their direct impact on public health. For example, Brno University Hospital had to shut down its IT network after being attacked, resulting in the postponement of surgeries and the cancellation of the COVID-19 testing that was part of the Czech government's pandemic response.

6.2. States and international organisations have responded in a variety of ways. Anti-phishing and virus distribution operations, scanning activities, and DDoS attacks have all been urged to stop by the EU's High Representative. The Council of the European Union also extended its cyber sanctions regime until May 2021 as a result of these operations, some of which harmed essential infrastructure needed to handle the pandemic. A hazardous amount of misinformation has been spread by national leaders in countries like the United States and Brazil via social media.

6.3. ***"Prohibitions under International Law"*** : States are governed by international law in the majority of cases. If the cyber operation in question is related to COVID-19 and is characterised as infringing international law, it must be proven that a state agency, such as an intelligence agency, or a non-state actor, such as an activist group, was involved in the operation. For political naming and shaming or for judicial adjudication, a certain level of certainty is required in order to assign an operation to the state. A generally acknowledged rule states that an operation should only be attributed to the source when a reasonable state under the same circumstances would do so.

6.4. Respect for other states' sovereignty is the rule that is most likely to be broken by a COVID-19-related cyber activity. There are two ways this rule can be broken. This law is violated in two ways: first, since it causes harm or damage on another state's territory when an attack on medical and public health infrastructure results in infection, worsens disease, or ruins the targeted infrastructure (including loss of functionality necessitating repair). Intentional disinformation that causes people to avoid treatment or dangerously self-medicate is a violation of the rule when such outcomes are foreseen. Non-injurious or non-damaging consequences have not been established in law as to whether they infringe the sovereignty of the state into which cyber operations are conducted. Second, interference with a state's "**inherently governmental responsibilities**" constitutes a violation of sovereignty. One of these functions is crisis management, which includes the formulation and implementation of pandemic response plans. The government designated Brno University Hospital as a COVID-19 testing facility, while

Hammersmith Medicines Research was in charge of vaccination testing in the United Kingdom. On this basis, any interference with these functions constitutes a violation of sovereignty. As an example, interfering with the nation's public health response by a COVID-19-related cyber operation can put citizens at risk of illness or death and thus breach sovereignty on both counts. To be fair, the UK has publicly rejected the idea that there is such a thing as international law's rule of sovereignty. Several European countries, including the Netherlands, France, Austria, and the Czech Republic, have rejected this viewpoint as unjustified in law. Neither the United States nor any other country has given it their full support.

6.5. ***COVID-19-related cyber operations may also violate a second international law prohibition:*** interfering with another country's internal affairs. The International Court of Justice has remarked that two conditions must be met before intervention can occur: Domain réservé is an area of activity that international law allows to the states to govern, and 2) the conduct is coercive in that it forces a state to act against its will, in the sense of forcing it to take action or refrain from taking action. There is some misunderstanding as to how the rule should be applied in the medical field. This cyber operation's goal must be to deny control over health crises in a state's domain réservé, even though this is a legitimate concern for a government entity. There was no desire to modify UK policy or its implementation in the WannaCry ransomware attack that crippled the British NHS; rather, the goal was to force payment of ransoms.

6.6. As a result, many COVID-19-related cyber actions would be classified as state-sponsored. For example, an aspect of the Czech government's pandemic reaction strategy was frustrated by the surgery that stripped Brno University Hospital of its testing capability. Furthermore, even a quick DoS attack on a public health ministry's social media messaging constitutes involvement because it prevents the state from addressing the situation in the manner it deems appropriate. It would not be an intervention if a misinformation campaign ran alongside the state's social media activities because the state would still be able to implement its public health agenda. A violation of sovereignty might still be proven if the misinformation put people's health or life at risk. **Article 2(4) of the United Nations Charter** and customary international law may apply to some COVID-19-related cyber actions. Cyber operations that do not result in major casualties or physical damage do not appear to violate the prohibition on the use of force, although it is unclear whether and when they do so. When it comes to any COVID-19-related cyber activity that has the potential to injure or kill a considerable number of people, the state is clearly responsible. In the same way, a cyber-attack that results in serious disease or death could be said to be a cyber-attack. Prime Minister Theresa May has previously stated that the Russian poisoning of Sergei and Yuliana Skripal in 2018 was an illegal use of force.

6.7. Customary international law and numerous treaty provisions, such as Article 6 of the International Covenant on Civil & Political Rights (ICCPR), Article 12(1) of the International Covenant on Economic & Social and Cultural Rights (ICESCR), Article 2 of the European Convention on Human Rights directly implicate COVID-19-related

cyber operations. States are required by international human rights law (IHRL) to respect and safeguard these rights. It is more likely that a distant cyber-attack on another state's medical or public health infrastructure will violate this restriction. Human rights duties may become extraterritorial if these operations can be linked to a specific country, in which case persons in other countries who are harmed may have their human rights violated by the country that is carrying them out. Unfortunately, the issue is still unresolved in law, although the tendency is certainly toward extraterritorial application.

6.8. Obligations Under International Law (ILOs): To prevent substantial harm to the rights of other countries, nations have a duty under international law to ensure that no cyber operations originate from or pass through their territory. According to some states, this "due diligence" responsibility has been established as an international law principle, while others have only gone so far as to describe it as an optional and non-binding obligation. There's no greater justification than that it's a legal requirement, as it is in the non-cyber setting. International human rights law also imposes a positive obligation on states to safeguard the lives and health of those who reside inside their borders. Both customary law and treaties like ICCPR's Article 2(1) make this requirement clear. As a result, states have a legal obligation to take all reasonable steps to stop harmful cyber operations, regardless of who is behind them, that put the health of citizens on their soil at risk. States are also required to take reasonable steps to ensure that COVID-19 information is correct.

6.9. International law infractions have long been overdue when it comes to harmful cyber operations that target medical capabilities or public health activities or endanger individual health. Only the Netherlands and Australia are prominent outliers; others include the backers of a proposal before the UN's Open-ended Working Group, which is now under consideration. Those around them must take responsibility and follow suit as soon as they are given the green light. To name and shame states that break international law will certainly not be an effective solution, but it is undeniably effective at deterring others from doing the same. Cyber attacks that breach international law open the door to reactions that were previously unavailable, including countermeasures (responses that would be unlawful but for the fact that they are designed to compel an attacker to end its own unlawful cyber operations). Article 51 of the United Nations Charter allows a victim state to use force in self-defense if necessary. A growing number of states are unable to simply denounce hostile cyber activities without calling them out for what they are—blatant violations of international law.

7. EFFORTS BY THE GOVERNMENT TO REDUCE THE NUMBER OF CYBER ATTACKS[15]

1. An NCIIPC (National Critical Information Infrastructure Protection Center) will be established to safeguard the nation's critical information infrastructure.

[15] Nextias.Com. Retrieved February 26, 2022, from https://www.nextias.com/current-affairs/13-11-2021/cybercrime-went-up-by-500-during-pandemic.

2. Digital service providers are required by law to immediately notify CERT-In of any issues related to cyber security.
3. Malicious software detection and removal tools have been provided by the Cyber Swachhta Kendra.
4. Guidance for Chief Information Security Officers (CISOs) on their primary duties and responsibilities in securing applications and infrastructure and complying with regulatory requirements.
5. Prior to the hosting of government websites and applications, and at regular times thereafter, there should be an audit provision.
6. Countering cyber assaults and cyber-terrorism requires the development of a Crisis Management Plan.
7. To assess the cyber security posture and preparedness of government and critical sector organisations by conducting cyber security simulated drills and exercises.

8. SUGGESTIONS FOR THE FUTURE[16]

1. Increase the effectiveness of law enforcement agencies by following the rules set forth by traditional law enforcement and information technology security organisations (ISOs).
2. In order to create new skills and opportunities, these industries should collaborate. People should always use a strong combination of passwords for every other account and ensure that their social media accounts have security settings in place to protect their personal information and images.
3. Ensure the security of your data i.e. the most sensitive files, such as financial records and tax returns, should be encrypted to keep them safe.
4. Online identity protection to be overly careful than underly cautious when it comes to online identity protection. Personal IDs such your name, address, phone number, and/or financial information should be kept private on the Internet.
5. In addition, INTERPOL is actively participating in the multilateral strategic debates organised by the World Economic Forum in order to develop alliances and partnerships against cybercrime. It is also a member of the World Economic Forum's Center for Cybersecurity Advisory Board. As part of our efforts to keep law enforcement aware of new and high-risk cyberthreats, we publish INTERPOL Purple Notices. X is among the warnings sent out via the INTERPOL network. Compromise and execution of ransomware against important organisations and infrastructures necessary to aid in the reaction of COVID-19, the use and spread of a banking Trojan, have been identified by the CFC of INTERPOL.
6. Users, ISPs, CERTs, and Cyber Cells should all work together to put legislation into action. It is necessary for online adjudicating authorities, such as adjudicating officers and the Telecom Dispute Settlement Authority Tribunal, to rule on matters. There are a number of legislative measures that must be implemented as soon as possible, including a policy or provision on cyber espionage, the designation of the health care sector as a "critical infrastructure" to ensure that it receives the highest level of cyber security, and the creation of penalties for cybersquatting in the Technology or Patent Law. Legislative actions such as the ones outlined above should be implemented as soon as possible.

[16] Ahmad, Tabrez. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN Electronic Journal. 10.2139/ssrn.3568830.*

9. CONCLUSION

In order to combat cybercrime, it is critical that the public and private sectors work together, but this has proven difficult in the past due to issues of distrust and miscommunication. Because of COVID-19 cybercrime, new processes and networks have been set up to meet the issues that have always existed when it comes to improved cooperation. COVID-19's cybercrime danger is not a one-time phenomena. Since the pandemic's onset, there has been a substantial increase in the number of cases. Although cybercrime and the enforcement gap were already at unacceptable levels before the epidemic, they have continued to rise throughout the crisis as well. Malicious cyber actors have generally remained the same, but their methods have evolved to take advantage of the pandemic environment and exploit a pool of prospective victims that has grown tremendously. They have. It is now more critical than ever for some industries to protect themselves from cybercrime in order to prevent the virus from spreading and to mitigate its devastating economic impact. Cybercrime culprits of all kinds will necessitate extensive cooperation across borders and sectors in order to impose appropriate penalties. Not all of the consequences of the COVID-19 conflict will be positive for this cooperation. As a result of the recent rises in cybercrime, politicians are paying more attention to the extent of the threat, which may and should be harnessed to bring forward legislative changes that encourage greater cross-border cooperation. If the momentum created by COVID-19 for international cooperation to combat cybercrime is not sustained, it will be a squandered opportunity.

References

Journals and Articles

A&A. (2021, December 15). *Data Protection and Privacy – Cyber Security Laws in India*. Ahlawat & Associates. https://www.ahlawatassociates.com/blog/data-protection-and-privacy-cyber-security-laws-in-india/.

COVID-19 and international cyber law. (2020, June 30). Directions Blog. https://directionsblog.eu/covid-19-and-international-cyber-law/.

Cybercrime & digital threats. (n.d.). Trendmicro.Com. Retrieved February 26, 2022, from https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/.

Developing story: COVID-19 used in malicious campaigns. (n.d.). Trendmicro.Com. Retrieved February 26, 2022, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

Dewan, D. M. (2020, April 25). *COVID 19 Lockdown: Increasing Cyber Crimes in India*. Lexology; RK Dewan & Co. https://www.lexology.com/library/detail.aspx?g=f33f6b37-6b62-425a-852b-0be29cbe46a7.

Growth in Cyber-Crimes in the COVID-19 times and Fragile Cyber Laws in India. (n.d.). Latest Laws. Retrieved February 26, 2022, from https://www.latestlaws.com/articles/growth-

in-cyber-crimes-in-the-covid-19-times-and-fragile-cyber-laws-in-india.

Indo-Asian News Service. (2019, August 22). *Hackers attack Indian healthcare website, steal 68 lakh records*. India Today. https://www.indiatoday.in/crime/story/hackers-attack-indian-healthcare-website-steal-68-lakh-records-1590345-2019-08-22.

PTI. (2021, May 20). Rise in cyber fraud amid pandemic; working relentlessly on user safety: Airtel CEO. *Deccan Herald*. https://www.deccanherald.com/business/rise-in-cyber-fraud-amid-pandemic-working-relentlessly-on-user-safety-airtel-ceo-987973.html.

Saini, A. P. (n.d.). Cyber Crime during COVID-19. *International Journal of Science and Research (Raipur, India)*. https://doi.org/10.21275/SR20530132248.

Scroxton, A. (2021, December 22). *Top 10 cyber crime stories of 2021*. ComputerWeekly.Com. https://www.computerweekly.com/news/252510733/Top-10-cyber-crime-stories-of-2021.

The Economist. (2020, May 10). Pornography is booming during the covid-19 lockdowns. *Economist (London, England: 1843)*. https://www.economist.com/international/2020/05/10/pornography-is-booming-during-the-covid-19-lockdowns.

(N.d.). Nextias.Com. Retrieved February 26, 2022, from https://www.nextias.com/current-affairs/13-11-2021/cybercrime-went-up-by-500-during-pandemic.

(2020). Who.Int. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200211-sitrep-22-ncov.pdf?sfvrsn=fb6d49b1_22020.

Ahmad, Tabrez. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. SSRN Electronic Journal. 10.2139/ssrn.3568830.

Acts

Ss. 67, 67-A and 66-E of IT Act, 2000.

Ss. 292, 293 of IPC 1860 broadly covers and punishes the foresaid acts involving selling, letting for hire, and publicly exhibiting obscene content. Indecent Representation of Women (Prohibition) Act, 1986 and Young Persons (Harmful Publications) Act, 1956.

Section 67-B of IT Act, 2000 punishes publishing or transmitting of material depicting children in Sexually explicit act.

S. 67-B Information Technology Act, 2020.

S. 14 Protection of Children from Sexual Offences Act, 2012.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rr. 3 and 4.

Section 69-A of IT Act, 2000 and Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

Epidemic Diseases Act, 1897, S. 3.

S. 441 of IPC 1860 punishes for entering into or upon property in possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property.

*****