Page 4987 - 4996 **DOI:** *https://doij.org/10.10000/IJLMH.111018*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Infodemic: How Cybercrimes skyrocketed during Covid-19

MANSI GUPTA[1] AND VAISHALI GAURHA[2]

ABSTRACT

The article titled "Infodemic: How Cybercrimes skyrocketed during Covid-19" derives our focus on how the enhanced dependence of people over the past year because of the prevailing situation of the Sars Covid-19 has led us to another pandemic. Every field, be it education, corporate sector, health-line services, groceries, trading etc. became virtual. As our focus has been shifted to the health crisis, cybercriminals have got an opportunity to attack networks, businesses and global organizations.

As a result of individuals spending more time online and the situation of chaos, fear and anxiety, cybercriminals tend to take advantage and attack their targets globally. Taking advantage of this situation, many criminals have resorted to spreading misinformation, false propagandas and distrust in governments. We have seen many false theories and conspiracy theories throughout the pandemic be it associated with curing the virus from drinking sanitizers, the myths about Hydrochloroxyquine or ultra-violet rays and not to forget various political propagandas. This is the reason it has been named "infodemic" by WHO director because this is the pandemic of misinformation too. Misinformation and disinformation concerning the virus still unfold primarily through social media and encrypted electronic messaging services. The article will ponder upon how the big social media giants are prepared to deal this situation.

Cyber safety is not an issue that is restricted to a particular nation rather it is a concern of international level. Cybercrimes just like the corona virus have a very high rate of transmission and are not restricted by national boundaries. Therefore, all the countries must fight against it at the international level and must assent to the programmes and conventions passed by the inter-governmental bodies.

As technology is an inevitable part of our lives these days, we must also take all the precautions and protective measure necessary to protect ourselves from the wrongdoers. Whether technology becomes a bane or a boon for us is in our hands and with due diligence and precautions it can act as the greatest tool for economic growth and development.

The aim of the current article is to recognize the relationship between the novel corona

[1] Author is a student at University of Petroleum and Energy Studies, India.
[2] Author is a student at University of Petroleum and Energy Studies, India.

 [ISSN 2581-5369]

virus and increase in the cybercrime activities, what has the role of international bodies been significant in combating the cybercrimes and how pandemic has contributed to it and how it has been used to create false agendas, misinformation and distrust in the governments across the world and what could the necessary precautions for it.

Keywords- *Cybercrimes, Infodemic, Covid-19, misinformation, international co-operation etc.*

I. INTRODUCTION

We might not have realised but the years 2020-21, have not only proven to be a threat to our mortal life but also to our cyber life. As the pandemic tightened its grip around the globe, the dependency on digital life also increased in an exponential manner. Every field, be it education, corporate sector, health-line services, groceries, trading etc. became virtual. According to Japan Times, about 59% of the global population has switched to online-based activities such as online meetings, schools, and even online concerts, which they otherwise would have done offline.[3]

Before going any further we must understand the meaning of cybercrimes. Cybercrime is the use of electronic devices such as computers and internet as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography, stealing identities, data trading or violating privacy. As it involves the internet, therefore, cybercrime represents an extension of existing criminal behaviour alongside some novel illegal activities.[4] An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. That is why it is a matter of international law as no particular jurisdiction can limit the global existence of Internet.

As per INTERPOL[5], cybercriminals all across the world are attacking the computer networks and systems of individuals, businesses as well as global organizations at a time when cyber defences might be lowered due to the shift of focus to health crisis. It is a well-known fact that cyber-attacks have been on the internet for decades, but with fear and anxiety about the pandemic combined with the compulsion of being locked down for months has given a huge chance to cybercriminals to take advantage of this situation, either it is to make money or just

[3]Jake Adelstein, *Criminals are taking advantage of fear over COVID-19*. THE JAPAN TIMES (March 2020), https://www.japantimes.co.jp/news/2020/03/02/national/media-national/criminals-taking-advantage-fear-covid-19/#.Xwm4DSgzbb1.

[4]Michael Aaron Dennis, *Cybercrime*s, BRITANNICA (September 19, 2019),https://www.britannica.com/topic/cybercrime.

[5]*Covid-19 Cyber threats*, INTERPOL (June 4, 2020),https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

 [ISSN 2581-5369]

play around by spreading rumours.

The aim of this paper is to recognize the relationship between the novel corona virus and increase in the cybercrime activities, how pandemic has contributed to it and how it has been used to create false agendas, misinformation and distrust in the governments across the world and what could the necessary precautions for it.

II. HOW COVID-19 LED TO THE RISE OF INFODEMIC

The pandemic of COVID – 19 and the consequent imposition of lockdown led to a phenomenal and unprecedented growth in the usage of the internet. Where most may say that usage of the internet has been a silver lining in these though times but the exceeding growth in cybercrime is something that cannot be overlooked. Digital information channel, social media, emails, streaming, cloud service, voice conferencing and video calls are now being used more than ever. [6]In mid-March DE-CIX, a Frankfurt based internet exchange reported peak data traffic of 9.1 Terabit per second.[7] This is the highest ever recorded data usage in the history of cyber networking. A never seen before rise in the usage of internet also indicates an increase in the number of inexperienced and naive users, who are vulnerable to cyber criminals.

The World Health Organization on 23rd of April 2020 reported a dramatic increase in the number of cyber-attack cases directed at its staff and emails affecting the public at large. The scammers impersonated the WHO officials in their emails and channelled donations to a fictitious fund and not to the authentic COVID-19 Solidarity Response Fund. The number of cyber-attacks is five times the number directed by the organization last year. [8]

Which is now termed as "cyber pandemic", has many aspects to it, from ransom ware to data breaches and from election security to unemployment fraud, COVID 19 has in many ways unleashed new challenges and has accelerated the existing ones.[9] An INTERPOL assessment on the impact of COVID-19 on cybercrimes has shown a significant shift from individuals and small businesses to big corporations, government and critical infrastructure. [10]

---

[6]Johannes Wiggen, *The impact of COVID-19 on cybercrime and state-sponsored cyber activities*, JSTOR,(20 June 2020)https://www.jstor.org/stable/resrep25300?seq=2#metadata_info_tab_contents

[7]Id. at 5

[8]*WHO reports fivefold increase in cyber attacks*, urges vigilance, WORLD HEALTH ORGANIZATION, (23 April, 2020), https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[9]Dan Lohrmann, *2020: The year the covid-19 crisis brought a Cyber Pandemic*, GOVERNMENT TECHNOLOGY,(December 12, 2020)https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html

[10]INTERPOL report shows alarming rate of cyber attacks during COVID-19, (4 August 2020) https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

 [ISSN 2581-5369]

INTERPOL suggests that the following are the widespread landscapes of cybercrime in relation to COVID-19:

1. **Online scams and Phishing** - Phishing is the fraudulent practice of including individuals to reveal personal information such as passwords, credit card numbers and OTP numbers through fake websites or emails.
2. **Disruptive Ransom ware** – INTERPOL's Cybercrime Threat Response Team has also warned of cybercriminals using ransom ware to hold hospitals and medical services digitally hostage, preventing them from accessing vital files unless a ransom is paid.[11]
3. **Malware-** Cybercriminals are taking advantage of the widespread global communications on the corona virus to mask their activities. Malware, Trojans and spywares have been found embedded in various interactive COVID-19 maps and websites. Spam emails are also cajoling users into clicking on links which automatically download malware to their personal computers or mobile phones.
4. **Misinformation** – Social media platforms are well known for the spread of misinformation and denial of scientific literature. Fake news may range from the causes of spread of virus, its carriers, prevention, home remedies and the symptoms. More often than not, this information has proven to be false and fictitious. The WHO and various other health organizations have time and again urged users to not fall for the blandishments of false medications and information that spreads like wildfire on social media platforms. [12]

Therefore, it can be construed that although cybercrime has been pre-existent and is not something which was only developed in the due course of the pandemic but the rise in cybercrime cannot be ignored. As the statistics mentioned above depict that misinformation, fraud, scams and phishing have exponentially increased which can be solved by stringent and swift laws by the international and national bodies.

III. DESTITUTION IN PEOPLE- A BREEDING GROUND FOR CYBERCRIMES

As a result of individuals spending more time online and the situation of chaos, fear and anxiety, cybercriminals tend to take advantage and attack their targets globally. The subjects to their attack could be anyone be it individuals, businesses, government agencies, and even hospitals.

[11] *Id* at 10
[12] Fabio Tagliabue, *The Pandemic of Disinformation in COVID 19,*(August 1 2020)https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7395797/

 [ISSN 2581-5369]

Taking advantage of this situation, many criminals have resorted to spreading misinformation, false propagandas and distrust in governments. An INTERPOL assessment of the impact of Covid-19 on cybercrimes showed that there has been 14% surge in fake news. Unverified information, inadequately understood threats and conspiracy theories have contributed to anxiety in communities and in some cases it has expedited the commitment of cyberattacks. Nearly thirty per cent of nations that seasoned the global cybercrime survey confirmed the circulation of false information associated with COVID-19.[13]There are also reports of misinformation being linked to the illegal trade of fraudulent medical commodities. The situation is so worse that UN has termed it as 'infodemic' of misinformation.

"We're not just fighting an epidemic; we're fighting an infodemic," said Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO) at a gathering of foreign policy and security experts in Munich, Germany, referring to fake news that "spreads faster and more easily than this virus."[14]

This is not just the case of healthcare misinformation; similar kinds of conspiracy theories are operating for governmental and political issues as well. In an article of Harvard Kennedy School, the researchers in a national survey of U.S. adults fielded June 4–17, 2020, found that conspiracy theories, particularly those promoted by visible partisan figures, exhibited higher levels of support than medical misinformation concerning the treatment and transmissibility of COVID-19. This means that capable dangerous health misinformation is harder to believe than abstract ideas concerning the villainous intentions of governmental and political actors.[15]

We have all seen that how this has been used to blame China as a villain, waging bio hazardous war against the world or scapegoat throughout 2020 by prominent leaders and governments all over the world. Similarly, there has been plenty of URLs available telling the medicinal properties of disinfectants, the myths about *hydroxychloroquine* and ultraviolet rays.

The beliefs in conspiracy theories and misinformation are differentially associated depending upon the political ideology and trust or distrust in experts—these orientations colour one's interactions with new information and fill in the (perceived) motivations of scientists,

[13]Faradias Izza Azzahra, *The Raise of Cyber-Crime Due to COVID-19 Pandemic,* UNIVERSITAS HASANUDDIN MODEL UNITED NATIONS, https://unhasmun.wordpress.com/2020/12/08/the-raise-of-cyber-crime-due-to-covid-19-pandemic/.

[14]*UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis,* UNITED NATIONS OFFICE ON DRUGS AND CRIME, (March 31, 2020),https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19.

[15]Adam M. Enders & Ors. *The different forms of COVID-19 misinformation and their consequences,* MISINFORMATION REVIEW, (November 16, 2020), https://misinforeview.hks.harvard.edu/article/the-different-forms-of-covid-19-misinformation-and-their-consequences/.

politicians, and other elites in their public communications about the pandemic.

Business Email Compromise[16] (phishing-compromised email accounts which pretend to be a senior official in the target organization) continues to use social-engineering, enhanced by the added urgency of the pandemic, to encourage the movement of funds to a criminal bank, foreign exchange or crypto currency account, or is used to obtain sensitive data for malicious use including espionage.

Also, the attention of various counter cybercrime specialists has been shifted to supporting government measures, such as quarantine enforcement against the COVID-19 outbreak. And many of them are themselves battling with the virus so this has reduced the capability of States to counter new and increasing cybercrime threats.

Misinformation and disinformation concerning the virus still unfold primarily through social media and encrypted electronic messaging services. Social media companies, conjointly challenged by remote operating, struggle to address the amount of misinformation content, how to systematically and consistently apply internal policies and the impact of local legislation. [17]Such misinformation and disinformation and attacks on Critical National Infrastructure undermine public trust and weaken the effectiveness of public safety measures.

IV. THE ROLE OF INTERNATIONAL BODIES IN COMBATING CYBER CRIME

Under this topic we shall discuss the role of international bodies and the approach adopted by them to curb cybercrimes. Various international bodies had long before realised the importance of cyber security and the need to take meticulous and combined steps to eradicate cybercrimes. Unlike other crimes, cybercrime is not confined to a particular state, it spreads across like ripples and therefore boundaries for it are obliterated. There have been various conventions and programmes at the international level to effectively protect users and simultaneously eradicate cybercrimes. Some of them are as follows-

United Nations - the Global Program on Cybercrimes is mandated to assist member states in their struggle against cyber-related crimes through capacity building and technical assistance.[18]The Global Programme is designed to respond flexibly to identify needs in

[16]Anonymous, *Business Economic Compromise (BEC),* TRENDMICRO https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

[17]*CYBERCRIME AND COVID19: Risks and Responses*, UNITED NATIONS OFFICE ON DRUGS AND CRIME (April 14, 2020), https://www.unodc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf.

[18]*Global Programme on Cybercrime*, UNITED NATIONS OFFICE ON DRUGS AND CRIME,https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

developing countries by supporting Member States to prevent and combat cybercrime in a holistic manner.

The objective of the programme is as follows-

- Increased efficiency in the investigation, prosecution and adjudication of cybercrimes.
- Strengthening national and international communication between countries, law enforcement authorities and private sector along with increased knowledge of cyber risks.
- To ensure the elimination of safe havens for cybercriminals
- To exchange information for fighting cybercrime
- To train and equip law-enforcement personnel to address cybercrime
- To protect the computer systems and data from cybercrime

1. **Budapest Convention-** The convention on cybercrime or the Budapest Convention on Cyber Crimes was the first ever international treaty seeking to address computer crimes by enhancing national laws and improving investigation techniques. It had 65 signatories.
2. **INTERPOL-** INTERPOL was created in 1923 that facilitates international police co-operation via its global police system. In November 2020, the INTERPOL instituted two schemes for the prevention of cybercrimes. . One of them is the Cybercrime Knowledge Exchange workspace that is associated with general, non-police information and is available to all users. The second one is the Cybercrime Collaborative Platform-Operation, which assists the law enforcement authorities, with access restricted only to the operational authorities.[19]

V. DEALING WITH PANDEMIC AND INFODEMIC GO HAND IN HAND

With the surge in cybercrimes, the question of keeping our cyber hands sanitised becomes more evident and crucial. It becomes important for us to know how we can self-isolate our data. Like the pandemic, the strata that is more prone to fall a victim of cybercrime is elderly people (as technology is new to them) and young children (who are spending more time online because of virtual classrooms, social media and they often don't distinguish between real and virtual

[19] Devesh K Pandey, Interpol creates cybercrime-related communication services, THE HINDU (Novermber 4, 2020) https://www.thehindu.com/news/national/interpol-creates-cybercrime-related-communication-services/article33023647.ece

 [ISSN 2581-5369]

words).

To fight them and be vigilant about them, we must know the kinds of cyber-attack happening and how it affects us. Once again, just like the SARS COVID virus, they can be everywhere in the form of apps, malicious mails, URLs, domains etc. So, we have to exercise caution while touching anything and everything online. And once the malware has attacked one of the systems, there is a potential risk of the security of the systems of the members of an organization being compromised. This can affect the whole grid of systems by which the organization is staying connected and there can be a huge loss of confidential data.[20]

In order to control this spurt of cyber-attacks, INTERPOL has suggested some preventive measures[21]-

1. **Keep your information safe-** This includes backing up all the important files and storing them independently in the system (maybe on cloud or external device). Also, the verification of the company's legitimate website before logging in is very crucial.
2. **Check your software and systems-** This includes-
    - Having the latest anti-virus software installed on your pc and mobile devices.
    - Strengthen your home network.
    - Disable third-party or outdated elements that might be used as entry points.
    - Download mobile applications or any other software from trusted platforms solely.
    - Perform regular health scans on your computers or mobile devices.
3. Be alert.

- Have conversation with your family −including kids − about how to stay safe online.
- Regularly check and update the privacy settings on your social media accounts.
- Update your passwords and make sure that they are robust.
- Do not click on links or open attachments in emails that you weren't expecting to receive or come from an unknown sender.

Also, to tackle various myths and false information being forwarded, the team of WHO "Myth Busters" are working with search and media companies like Facebook, Google, Pinterest, Tencent, Twitter, TikTok, YouTube and others to counter the spread of rumours, which include

[20]Priya Adlakha and Kiratraj Sadana, *India: Cyber Crime During Coronavirus Pandemic*, MONDAQ (April 22, 2020) https://www.mondaq.com/india/operational-impacts-and-strategy/921026/cyber-crime-during-coronavirus-pandemic.
[21]Supra at 4

 [ISSN 2581-5369]

misinformation like the virus cannot survive in hot weather, taking a high dose of *chloroquine* medication can protect you, and that consuming large quantities of ginger and garlic can prevent the virus.[22]

These corporations, consistent with the news reports, are squaring measures that sharply filter out the unfounded medical advice, hoaxes and different false data that they assert might risk public health. In a rare move, Facebook and Twitter have taken down a post from a head of State that falsely stated that a drug was working everywhere against the corona virus.

Delhi Police also issued guidelines amid rising fraud cases in relation to WHO advisories. They insisted on checking the authenticity of the website and pay attention to the type of personal information one has been asked to share. In no circumstances, there would be a need of passwords. Also, there are no lotteries, prizes, grants or certificates offered by WHO through emails and if you are asked to open any such attachment then it's better to do it by official page of the same.

The vaccination drives are in progress in various countries so there is vast number of chances that people are asked for all kinds of information in order to become the beneficiaries of the vaccination drive. Covid-19 related scams and developments resulting from them will continue as long as virus dominates the headlines. But this should not mean that we put our guards down as there is a vaccine to the virus but not to offenders. So, these preventive steps should be followed at all the times and not just during the pandemic. This threat can be reduced to an acceptable level only by the joint efforts of the population, businesses, organisations and governments.

The endeavours should be made to reach out to the people and make them digitally sound. There should be large scale campaigning and awareness programs that highlight the dangers posed by phishing mails. There should be an increase in the digital literacy programmes in schools, universities and in adult education also. Small and Medium sized industries usually don't have sufficient funds to have a proper IT cell and train their staff regarding cybercrimes. They should be financially supported, and a proper criteria and strategy should be provided.

As far as law enforcement agencies are concerned, their capacities and expertise for preventing and investigating cybercrime should be expanded.[23]The vacant IT security jobs should be filled, and the training programs should be conducted to so that the staff is adequately trained.

[22]Supra at 11

[23]Wiggen, Johannes, *The Impact of COVID-19 on Cyber Crime and State-Sponsored Cyber Activities*,JSTOR, (June 2020),https://www.jstor.org/stable/resrep25300?seq=2#metadata_info_tab_contents.

 [ISSN 2581-5369]

VI. CONCLUSION

In the last couple of months our dependency on the internet and online means of communication has increased manifolds. The only thing that has kept us together, united and in continuity is the internet. We cannot disregard the amount of relief that people have had in these tough times to be able to work from home, shop online, order food online, sell items and be connected to one's loved ones, all this possible only because of cyber technology. But like any other advancement in the world, this also has its own cons. Cyber criminals have detected the dependency of a large number of people on the internet and saw this is as an opportunity to use it to commit crimes.

As was rightly said by Max Baucus, "*We would not sit ideally when an offence is committed in the real world, so why should we sit ideally when an offence is committed in the cyber space*?" This phrase fits well in the conundrum that we are in today. The numbers of cybercrimes that we are facing today are unprecedented and are still increasing in an alarming rate, it is about time that we pull up our socks and take the most diligent and swift steps to protect ourselves. It becomes even more important to keep a check on cybercrimes at this time because any false or misleading claim made by the lobbyists might lead to fatal results. All these things lead to baseless rumours that spread like wild fire and have a tendency to affect the health and even the economy in the long run.

As technology is an inevitable part of our lives these days, we must also take all the precautions and protective measure necessary to protect ourselves from the wrongdoers. Whether technology becomes a bane or a boon for us is in our hands and with due diligence and precautions it can act as the greatest tool for economic growth and development. Therefore, the enforcement authorities as well as the citizens must be on their toes to keep themselves safe.

Cyber safety is not an issue that is restricted to a particular nation rather it is a concern of international level. Cybercrimes just like the corona virus have a very high rate of transmission and are not restricted by national boundaries. Therefore, all the countries must fight against it at the international level and must assent to the programmes and conventions passed by the inter-governmental bodies.

*****

 [ISSN 2581-5369]