AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

A Study of the Impact of the Pandemic on the Increase in Cyber Crimes against Youngsters and the Need for Stricter Legal Enforcement

N. Renuka,
Research Scholar,
University of Technology, Jaipur
Dr. Balasaheb Garje,
Supervisor,
University of Technology, Jaipur

Abstract

The corona virus pandemic had a profoundly negative impact on how people learn, interact, communicate, and run businesses. Online entertainment use increased as a result of people working and socializing from a distance, which provided cybercriminals with a fertile ground to exploit the platforms and their users. This article will look into the increasing trend of cybercrime committed through virtual entertainment, including explicit types like phishing, pantomime, and deceit. The article will also look at the groups that are typically affected by cybercrimes. In addition to the coronavirus pandemic, there is also a cyber pandemic, which affects how criminals commit crimes, and an infodemic, which has to do with the dissemination of false information. The article examines how the Coronavirus epidemic affected cybercrime and provides the most recent research on the number of cybercrime incidents in Poland and their contributing factors. It determines the factors that contribute to the occurrence of an offense and prevents straightforward identifying hoodlums as the perpetrators. Additionally, it suggests modifications to the law and organizational structure that would lessen the frequency and severity of the simultaneous Coronavirus cyberattacks that are most frequently reported.

Keywords: *Pandemic, Increase, Cyber Crimes, against, Youngsters, Stricter Legal Enforcement*

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

1. Introduction

The coronavirus pandemic is more than just a medical problem; it is also accompanied by other unwelcome idiosyncrasies that affect our health, wellbeing, or way of life. The execution of public errands as well as working and learning strategies have been impacted by measures taken to stop the infection from spreading. The sudden changes and unavoidable use of remote work or learning have increased awareness of cyber security risks. The pandemic has also had an effect on how lawbreakers behave. The shutdown has mostly provided cybercriminals with an opportunity to improve the effectiveness of their attacks in light of social engineering. Rapidly emerging new attack vectors have led to adjustments to recently used scenarios. Lockdown has been used by criminals to target large corporations, private businesses, experts in the application of policies, clinics, or individuals. They are motivated by a variety of sources and have clear goals. Both cyber-related and cyber-subordinate crime have increased in number due to lockdown. In addition, criminals who previously committed crimes outside of cyberspace have changed their methods of operation due to restrictions on communication or development and started working the internet as a result of their losses.

The analysis of the Coronavirus pandemic's impact on the criminal scene keeps in mind the elements of changes for situations involving assaults on clients who use the internet, elements that make it easier for criminals to commit crimes, and elements that make it difficult to identify the attackers and deal with them.

Basic infrastructure, like medical care administrations, has also been targeted by cyberattacks. This alert looked at problems like phishing, malware, and stage-divided communications. However, a more thorough analysis of the numerous attacks associated with the epidemic is presumably lacking both here and in the studies. The current state of the craft is very fragmented, with attacks from governments, the media, security associations, and episode groups all being acknowledged. Given the strong environment, it is therefore very essential for associations to nurture appropriate assurance and reaction estimates.

ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

Using a smart timeline of attacks related to the Coronavirus pandemic, we hope to advance research in this work. This schedule and the subsequent analysis can help with understanding those assaults and how they are made, making it easier to plan to resist them if they are ever encountered again. Our timetable directs major cyberattacks against the infection's global spread as well as additional actions, like when lockdowns were implemented. The schedule reveals an illustration of cyber-assaults and missions, which typically occur after events like statements of strategy. This enables us to track how quickly cyberattacks and crimes appeared in comparison to when the majority of local pandemic cases were reported, or, for sure, assuming that attacks coincided with any of these events. We evaluate the extent of the assaults revealed, what they have meant for the labor force, and how the labor force might still be in risk as a supplement to these studies. In many ways, this schedule analysis also frames an important aspect of our work, including the sequential sequencing of assaults and the depiction of missions using a recognized assault scientific categorization. This provides a foundation that is consistent with flow writing and establishes a base that future examinations can definitely build upon.

2. Literature Review

➢ Social media usage and Cybercrime

The broad word "cybercrime" refers to criminal activity that makes use of personal computers or computer networks. These attacks are planned and have major repercussions for the general population because it is assumed that they could pose a risk to public safety, cause mental health issues, and possibly even further financial disruption. Cybercrime is currently becoming a challenging subject. In their report, the NW3C discussed six different types of crimes committed through online entertainment, including phishing and social engineering, infection, wholesale fraud, and cyber-following.

Cybercrime and online extortion have risen throughout the Coronavirus episode, and rates of cybercrime peaked with the months with the toughest lockdown measures. Because of the negative effects mentioned by health professionals, concerns were raised concerning the usage of web-based entertainment as the amount of time spent using it increased. According to a few health reports, over use of online entertainment has led to psychological problems, data overload, and

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

web-based entertainment fatigue. According to the cyber security company Bromium, massive global cybercriminal networks were created as a result of online entertainment platforms that were primarily used to keep in touch with loved ones. Facebook, WhatsApp, and Instagram became places where anyone may unquestionably receive information about someone's location and personal life because people were regularly sharing about day-to-day activities on social media. Additionally, as Coronavirus spread, it became clear that the increasing use of web-based entertainment was causing an enormous influx of cybercrime incidents worldwide. Additionally, there was a striking increase in incidents involving the use of fraudulent spaces, websites, and spam communications. All throughout the world, children, government officials, and medical professionals were targeted by cybercriminals.

- **Cybercrimes against Children during Covid-19**

Children's cybercrimes increased significantly as a result of the advanced change in education that helped children access cyberspace legitimately. Even though children were benefiting greatly from online education, they were frequently defenseless against the risks the internet and online entertainment platforms posed. Kids who used the internet for fun during the pandemic were more vulnerable to becoming victims of cybercrime. The situation was horrifying, especially in India, where the Public Wrongdoing Record Department reported a 400% increase in cybercrime evidence against children in 2020, and almost 90% of these offenses involved the dissemination of materials that showed children acting in physically explicit ways. This is taking place since India has the largest population of young people in the world. Similarly, most kids at the time were turning to online games and virtual entertainment platforms to escape the stresses of daily life and social isolation without realizing that these platforms are defenseless against online predators and that bad actors can undoubtedly exploit them there with false promises of community and security. According to a Seat Exploration Center survey, high school students communicate a wide range of information through online entertainment.

- **Reasons behind Spiking Cybercrime**

ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

Government boycotts and people staying at home led to an increase in Web usage, which in turn led to an increase in cybercrimes. According to the UNODC, the requirement to work from home significantly raised the risk of becoming a victim of cybercrime. According to a report in the Hours of India (an English newspaper), clients' lack of practiced cyber cleanliness was the source of 80% of cybercrime scams. According to another survey, making poor decisions often leads people to fall for a hoax. In other studies, the rise in cybercrime during a pandemic is partially attributed to wrongdoers' fatigue from spending more time relaxing at home. The perception that cybercrime is normally safe is another fundamental component. Additionally, the globalization of innovation and rapid data breakthroughs have contributed to an increase in crime.

3. Most Frequent Attacks Amid Covid-19

It is possible to investigate the variation of assault circumstances because of the coronavirus pandemic, especially those that are geared toward adapting and taking into account societal design. Examining news articles on internet security and data frameworks in Poland and globally reveals several instances of malware being appropriated and fully taken PC tricks. When defensive and cleanliness measures were scarce in the early stages of the pandemic, there were many con artists whose victims damaged their property because they were offered protective measures (such as veils), sterile items, drugs, and meds, fake kits for the crown home testing, and even Coronavirus immunizations, at online sales or phony websites. Paid orders were infrequently fulfilled, or customers might receive things that were subpar, phony, or both. Public and international legal actions are being taken against these thugs. With the supply and demand for sterilized commodities and defensive measures changing in the months that followed, the number of fake sales or online stores really remained consistently high. Many have been compelled to arrange products online due to technological constraints and restrictions on the number of people who can be in a store at once. The number of fake online stores that sell mostly technology, kid's toys, and designer clothing is constantly increasing. Another example of a common form of misrepresentation is dishonest pledge drives for the health sector, including financial support for clinics and medical staff, the construction of temporary clinics, the purchase of ventilators or protective equipment, as well as support for patients and their families. Similar legal authority will apply to attacks referred

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

to as "Nigerian tricks" and "Business Email Split the Difference" (BEC), the circumstances of which have also been modified to account for the current pandemic condition.

An in-depth analysis of examples of prohibited conduct reveals that different units in charge of the procedures use different justifications for initiating them in similar situations, which could result in slightly distorted measurements. The vast majority of inquiries into the subject of cybercrime deal with acts covered by Section XXXIII of the Clean Crook Code (CC) articles, such as violations of data security (Articles 267 CC - 269 b CC) and Article 287 1 CC, which is a wrongdoing against property and includes PC extortion. It should be clear from the graphic below (table 1) that it is not important how many procedures are initiated under Articles 267 CC to 269 b CC. In 2020, 8018 procedures were initiated for demonstrations under Article 267 1 CC, including the suspected PC hacking. The number of procedures started should have increased by 106% north of 2016. Regarding starting processes under Article 287 12 CC, there has been an even larger increase in the number of operations, by 173%.

Simultaneously, in 2020, there were 24455 procedures initiated under Article 286 1-3 CC, including those involving fakes identified in police data sets as online cheaters, an increase of 9% from 2019 and 30% from 2016. In 2020, there were 83 822 procedures total under Article 286 1-3 CC, and cheaters who were "online fakes" according to police data sets accounted for 42% of those operations. Thus, Article 286 CC processes were initiated for the majority of the demonstrations that could be considered cybercrimes.

Table 1: Cybercrime in Poland including the legal basis for initiating proceedings

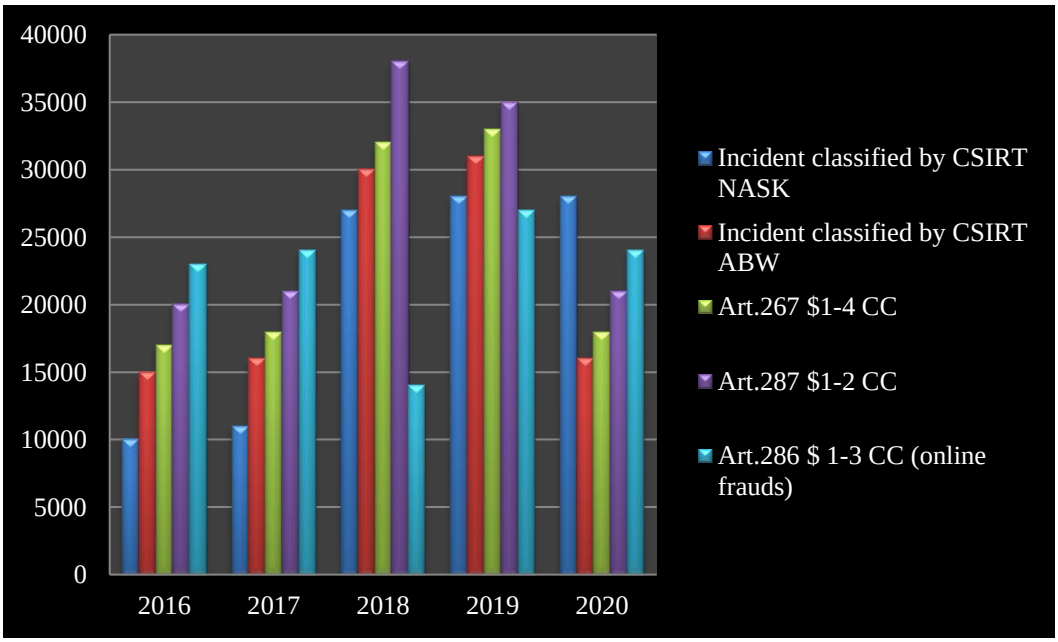
The Legal Basis for Initiating Proceedings	2016	2017	2018	2019	2020
Art.267 $1-4 CC	4302	4328	3567	6827	8018
Art.268 $1-3 CC	324	280	237	273	236
Art.268a $1-2 CC	388	353	471	575	675
Art.269 $1-2 CC	12	14	8	18	8
Art.269a CC	33	38	42	46	22
Art.269b $ 1 CC	25	27	28	44	38

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

Art.286 $1-3 CC (online frauds)	36385	38252	20346	23516	24455
Art.287 $1-2 CC	5202	5445	6303	20682	22328

Investigating the data from the determined infractions class reveals only tangentially different properties. The observed trends in the number of cases filed under Articles 267 CC, 287 CC, and 286 CC (together referred to as online) show a steady increase in the number of cybercrimes. In addition, no significant increase in cybercrime was observed in 2020 while the Coronavirus epidemic was ongoing.

A quantitative analysis of the steps taken in cybercrime situations can be compared to data on the number of episodes requested by CSIRT/CERT groups. In Poland, security incidents are reported to three separate organizations: CSIRT NASK (for the sensitive area and part of the public area), CSIRT GOV (for the public area as a whole), and CSIRT MON (for the military area, where information on incidents is not publicly available). As seen in Fig. 1, there are increasingly more instances and cybercrimes being reported.



AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

Figure 1: Cybercrime and incidents that CSIRT NASK and CSIRT GOV have categorized in Poland

4. Cyber-Bullying

Digital harassment can have a range of negative effects on the victim, from mild to severe. The extreme variety might put the victim under so much pressure and unease that they may commit suicide. Schools, universities, and other organizations are successfully directing studios and online projects to promote mindfulness towards digital abuse and harassment. Such efforts are admirable and ought to continue.

In May 2020, the Bois Storage case made headlines because a student who claimed she was physically upset by her colleague through virtual amusement. The discussion has also been linked to the passing of a seventeen-year-old in Master gram. This has sparked several arguments about the motivations for such incidents and the most effective ways to combat them. A few medical professionals have said that digital torturing is the result of a lack of sex education, which regrettably is still perceived as a no in India. Unquestionably, the continued lack of sex education is the best explanation for such incidents, and teens undoubtedly need sex education. However, another important factor is that young children are also exposed to unfiltered information that is inappropriate for them.

Since their classes and a variety of other activities are held online, the young age has easy access to cell phones and other sorts of technology due to the lockout. In the past, parents had the opportunity to most likely stop their children from using this technology. In this aspect, the epidemic and subsequent lockdowns have rendered guardians' duties considerably more difficult, if not impossible. Therefore, our children presently have easy access to all types of unfiltered content and frequently create communication channels with people that offer all kind of off-base effects. For instance, youngsters commonly interact with mysterious online users who could lead them astray or undermine them to obtain sensitive information about their family or motivate them to engage in criminal activity.

5. Conclusion

ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

One of the most unusual kinds of crime is cybercrime. Cybercriminals are incredibly skilled and flexible. They quickly alter their tactics, the tools they employ, and the social engineering techniques connected to their assaults to achieve their goals. Online entertainment has developed into a powerful platform for intercultural communication, the exchange of ideas and information, the expression of opinions, and entertainment; the number of users will continue to grow. Overall, the internet-based market is being impacted by cybercrimes committed through online entertainment. Less people are using these platforms because they are undermining faith in online shopping malls. People who have been affected feel powerless and unsatisfied because legislatures and law enforcement are also struggling to keep up with the constantly evolving threat landscape. Organizations, governments, and individuals must make every effort to protect themselves against these wrongdoings. This includes utilizing areas of strength, exercising caution when disclosing personal information, and staying up to date on the most recent security initiatives.

References

1. *Almadhoor, L. (2021). Social media and cybercrimes. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2972-2981.*
2. *Beech, M. (2020). COVID-19 Pushes Up Internet Use 70% and Streaming More Than 12%, First Figures Reveal.*
3. *Dalpini, N. (2021). Cybercrime Protection in E-Commerce during the COVID-19 Pandemic (Doctoral dissertation, Utica College).*
4. *Hagen, L., Neely, S., Scharf, R., & Keller, T. E. (2020). Social media use for crisis and emergency risk communications during the Zika health crisis. Digital Government: Research and Practice, 1(2), 1-21.*
5. *India.com (2020) Your privacy may be at Risk: WhatsApp Group Chat Links Available on Google Search, India.com, 22. 2. 2020, (November 15, 2021).*

ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

6. *Kanekar, A., & Sharma, M. (2020, September). COVID-19 and mental well-being: guidance on the application of behavioral and positive well-being strategies. In Healthcare (Vol. 8, No. 3, p. 336). Multidisciplinary Digital Publishing Institute*
7. *Kumar, A. (2020) Coronavirus pandemic: Cyber criminals and scammers prey on Covid 19 fears to scam people, India Today, 22. 4. 2020.*
8. *Lallie, H. S., Shepherd, L.A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., &Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.*
9. *Mkhize, S., & Gopal, N. (2021). Cyberbullying perpetration: Children and youth at risk of victimization during Covid-19 lockdown. International Journal of Criminology and Sociology, 10, 525-537.*
10. *Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International journal of information management, 55, 102171.*
11. *Riek, M., Bohme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. IEEE Transactions on Dependable and Secure Computing, 13(2), 261- 273.*
12. *Sharma, S. & Sharma, K. V. (2020) Cyber Crime analysis on Social Media. BSSS Journal of Computer: ISSN (Print)-0975-7228, E-ISSN - 2582-4880, Vol. XI, Issue-I.*
13. *Tejaswi, M. (2020) Organised crime using COVID-19 for launching phishing attacks: KPMG, The Hindu, 14. 4. 2020.*
14. *Van Der Velden, M., & El Emam, K. (2013). "Not all my friends need to know": a qualitative study of teenage patients, privacy, and social media. Journal of the American Medical Informatics Association, 20(1), 16-24.*
15. *Warnick. A. (2021). Public health vulnerable to cyberattacks during COVID-19 outbreak: US alert issued.*

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by mean if any person having copyright issue or patent or anything other wise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments/updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher)

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN: 2320-3714
Volume 3 Issue 3
September 2022
Impact Factor: 11.7
Subject Law

that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification / Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission /Copyright / Patent/Submission for any higher degree or Job/ Primary Data/ Secondary Data Issues, I will be solely/entirely responsible for any legal issues. I informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Address Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed I website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me

N. Renuka
Dr. Balasaheb Garje

*****