Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 6, July 2021: 6038- 6045

Research Article

Cyber Crimes in the Age of Covid 19

Imtizajul Hussain Shah [a*], Dr Tejasvi Bhatia [b]

[a,b] Forensic Science Department, Lovely Professional University, India

Abstract

The paper discusses the topic of rising cybercrime in the age of COVID-19. Various dimensions related to cybercrime such as rise in internet usage for remote activities, victimization and the aftermath of such crimes upon individuals and large corporations as well as the cyber security measures that lead to the identification of the contributing factors behind the rising rate of cybercrime. Qualitative research methodology has been adopted in this regard for the comprehensive analysis of secondary resources. Few secondary thematic analyses are provided here in this study to discuss and analyze the ratio of cybercrimes perfectly during COVID-19 pandemic situation. Few recommendations have been made regarding further investment in the cybercrime department and awareness raising programs for the prevention of cybercrime.

Keywords: Cyber security, cyber crimes, qualitative research study, COVID-19 pandemic

1. Introduction

Rise in technology usage in contemporary times has provided the population with various advantages in terms of remote operations. However, it has also given rise to criminal activities that have been rising especially during the time of COVID-19 pandemic. These crimes can be classified into five major categories, all leading to unethical usage of personal data and information of unsuspecting internet users.

The activities of cybercrime, though not limited to, can be categorized as ***identity theft, phishing scams, cyber stalking, invasion of privacy, online harassment*** and so on. As per the words of Cheng, Chan & Chau (2020), selection of victims in cybercrimes depends upon an individual's frequency of IT usage. Moreover, the victimization leaves certain psychological aftermath that leads to distaste and distrust in further internet usage. According to an INTERPOL assessment, it has been identified that the rate of cybercrimes during COVID-19 has shifted from targeting the general population to targeting major businesses, government organizations and large-scale corporations (Interpol.int, 2020).

The report on cybercrime has also mentioned that the rate of cybercrime threats in Europe has been 42%, in the USA 12% and in Mena only 10% (Interpol.int, 2020). Thus, the frequency in internet usage has been directly linked with cybercrime threats during COVID-19 which the paper seeks to evaluate and identify the factors behind the rise in cybercrime during COVID-19. The problem statement the paper seeks to address is the impact of COVID-19 in the rise of internet usage and the enhancement of scope for cyber criminals to commit crimes within the cyberspace in various manners that leads to the disruption of individual or organizational activities.

Figure 1: INTERPOL Global Survey on Cybercrime

(Source: Interpol.int, 2020)

The aim of this paper is to identify the critical factors influencing the rise of cybercrime during COVID-19 pandemic. The objectives of this paper can be identified as follows:

- To identify the critical factors contributing to the rise in cybercrime in the age of COVID-19
- To evaluate the conditions of victimization and its aftermath regarding both individuals and various organizations.
- To identify the cyber security measures and their effectiveness in the prevention of cybercrime

The research questions are as follows:

- What are the critical contributing factors to the rise of cybercrime in the age of COVID-19?
- What are the conditions of victimization regarding both individuals and organizations?
- What are the cyber security measures that are in practice and their effectiveness in prevention of cybercrime?

The study seeks to evaluate the critical contributing factors of increasing cybercrime rates in the age of COVID-19. It will also seek to evaluate the effectiveness of current cyber security measures undertaken by both individuals and the government in order to identify any underlying gaps in measures that may be improved in the future. Moreover, by identifying the contributing factors behind the rise in cybercrime, the paper will be able to contribute towards the study of criminology and required reformations in the justice system regarding cybercrime prevention. This will also help the general population as well as the organizationsthat face cybercrime threats to understand the implications of cybercrime and proper measures to be taken for enhancing cyber security.

2. Literature review

Cybercrime in contemporary age

Cybercrime in the contemporary age has been growing significantly faster due to the rise in IT usage for important remote activities that requires saving various sensitive information on the internet. According to Okpe& Taya (2018), the age of globalization requires fast development in IT which has become a critical part of the modern day activities without which various activities can be hindered. Additionally, the lack of proper information about safe internet usage in the developing countries has given rise to the trends of cybercrime.

In contemporary age, the rise in financial activities through IT has given rise to cybercrime phenomena globally. As per the opinions of Ngo & Jaishankar (2017), cybercrime bears dire impact upon various software companies and an estimated cost of $110 billion annually can be attributed to the damages of cybercrime. Therefore, the rise in cybercrime in the contemporary age has been significant that requires proper prevention.

Rise of cyber usage in COVID-19

Rise in cybercrime during COVID-19 has increased significantly due to increased opportunities in various cyber spaces. The activities in cybercrime such as malicious domain, scam, phishing, fake news and on has been experienced in various ranges for different countries. Since the outbreak of COVID-19, an INTERPOL private pater has detected approximately 907,000 fake messages related to the pandemic (Interpol.int, 2020). Moreover,

the phishing or scam trends during the pandemic include financial support initiatives, health emails, tracking app for COVID-19, charity requests related to COVID-19 and so on (Interpol.int, 2020).

The report procured by INTERPOL also identifies the trends in cyber security according to various regions. In Africa, the enforcement of work from home has led to vulnerable conditions and increase in phishing, charity scams and sextortion (Interpol.int, 2020). Various companies in America have faced teleworking cybercriminals that target the employees remotely in order to commit acts of data theft that has affected the large corporations (Interpol.int, 2020).

In Asian and pacific regions, the cybercrime rates have increased in terms of fake medical supplies sales and misuse of teleconference tools for security hampers (Interpol.int, 2020). In Europe, increase in malicious domains related to the spreading of fake news has been significant (Interpol.int, 2020). Thus, during the COVID-19 pandemic, the rise in such criminal activities for both individuals and large corporations has been significant and various countries across the globe have expressed increased concern regarding cyber threats.

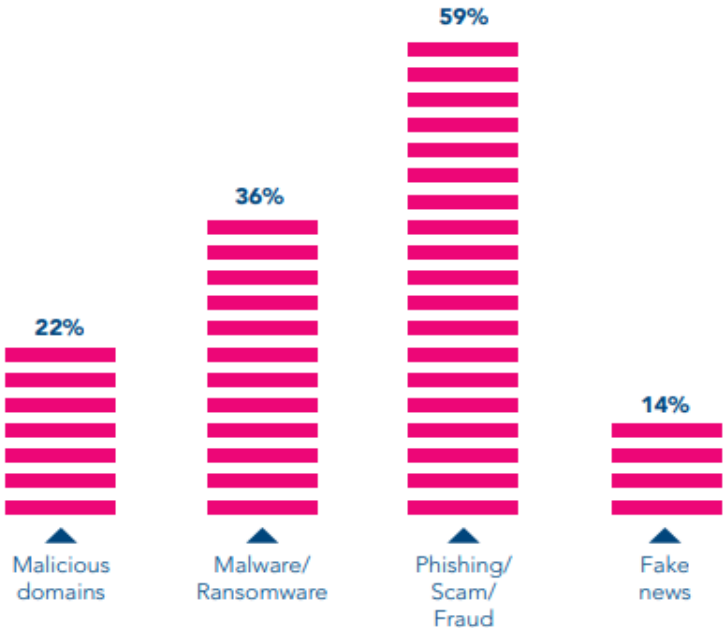

Figure 2: Key COVID-19 inflicted cyber threat distribution

(Source: Interpol.int, 2020)

Cyber security measures

The prevention of crime is dependent upon cyber security measures and the contribution of the justice system of a country to prevent these crimes. The laws and regulations in the USA regarding cyber security are various that are categories according to their functionality and area of crime. According to Kosseff (2017), these laws and regulations include Consumer ***Privacy Protection Act 2017, Health Insurance Profitability and Accountability Act 1996, Gramm-Leach-Bliley Act 1999, Homeland Security Act 2002, Federal Information Security Management Act 2002, Cyber security Information Sharing Act, Cyber security Enhancement Act 2014*** and so on. Individual measures include rising of awareness and providing information about potential cybercrimes in practice. Moreover, the population, which includes the employees of corporations, participated in the organization of training and awareness programs.

Victimization and aftermath of cybercrime

Cybercrime which specifically includes identity theft, sensitive information theft and misuse leads to the victimization of people who are mostly unaware of these acts. As per the words of Kaakinen et al. (2018), cybercrime victims are psychologically affected and suffer from trust-issues that impact their interpersonal relationships. In many cases, financial theft by scamming impacts the lifestyle of the victims.

The rate of online interaction is often surveyed by criminals in order to identify potential victims. As per the opinion of Hamerton (2020), the causes of victimization may also include personal hatred and mentality of revenge due to bullying, violence and so on that may lead to victims to attempt suicide in extreme cases of cyber bullying and cyber stalking. The large corporations that are often targeted sufferers from loss of sensitive data,

financial scam and soon that impacts the operations significantly. Thus, the process of victimization and its aftermath affects the lives of the victims that may even lead to dire consequences for the victims.

Cultural Transmission Theory in criminology

The rise in cybercrime can be understood from the perspective of Cultural ***Transmission Theory in criminology*** that denotes the development of criminal activities in accordance with the changes in cultural perspective through generations. As per the words of Sergi (2018), the cultural transmission of a specific criminal culture leads to behavioral changes among the youth, making them more inclined to commit acts of crime. The rising trend in both internet usages can be attributed to the changes in cultural perspectives. Leading to the rise of crimes related to cyber space in the contemporary age. Additionally, the limitations in identifying the criminals due to the vastness of virtual cyberspace, cybercriminal mentality is provided the scope to develop from youth.

Literature gap

The existing literature found on this topic provides a vast scope of understanding, however, the lack of existing literature on the topic of criminalistics behavior development and the lack in the publication of criminal statuses by the official authorities creates a literature gap.

3. Methodology

The adoption of a proper research methodology is essential for the achievement of findings that are valid, reliable, authentic and relevant. For this particular paper will follow a qualitative research methodology for conducting a thematic analysis on the topic. According to Schoonenboom& Johnson (2017), the research design of a paper highlights the systematic framework that contributes to the achievement of unbiased research answers. Thus the paper will adopt an explanatory research design in order to identify the factors behind the phenomenon regarding criminal activities. It would assume a deductive approach in order to analyses the gathered data based on which the research questions can be answered.

The research paper will also adopt the philosophy of positivism in order to assume an n objective point of view in the analysis of different variables related to the subject. It would also help in the achievement of truth through the analysis of the gathered information. As per the words of Basias&Pollalis(2018), the application of qualitative research methodology in the analysis of information gathered from secondary resources leads to comprehensive evaluation. The instruments of the research will be published books, peer-reviewed articles and published journals and official reports on cybercrime and laws and regulations of cyber security.

The data collection method will be systematic and gathered from reliable online databases such as Google Scholar and Proquest. Official reports on cybercrime and cyber security will be gathered from official websites of the justice department. The inclusion-exclusion method for the sampling and selection process of the resources will include publication year between 2017-2021, published in English language, accessible and available in full-text pdf version and gathered from authentic and reliable sources. Through the adoption of these research methods, approaches and designs, the findings will be accurate and reliable that can be used in future for further analysis (Williams, Chaturvedi& Chakravarthy, 2020). It will also follow the codes of ethical considerations through proper citation and referencing authentic works used in the course of research.

4. Analysis and Discussion

Secondary thematic analysis

Theme 1: The transformation of cybercrime in contemporary age

In this modern era, online accessing activities are rising day by day and it causes cyber threats. As people nowadays provide their maximum personal information in social networking sites and become targets of cybercrime. As opined by Lallie et al. (2021), in recent decades there has been an expanded rate of victimizations of cyber-criminals. 737 incidents related malware, 9007,000 spam messages, and 48,000 malicious URLs found in the pandemic situation (Jürgen Stock, 2020). The impact of cyber-attack can have wide ranging inferences including theft of intellectual property, financial losses, and loss of customer trust and confidence. Estimation of cybercrime the overall monitor impact becomes billions of dollars in a year. In this contemporary world the effect of cybercrime harms society a lot both offline and online. Due to the passing days the ratio of cybercrimes is increasing in a wide range. The frauds based on internet stock have earned millions of amounts per year. As due to this COVID-19 pandemic situation the economic condition is not stable for the majority so maximum fraud chooses this way to earn money for their survival (Puaschunder, 2020). The criminals are taking advantage of that information that people provide in the social networking sites. Getting the

personal information the criminals are able to access and hack their accounts and transfer the money to their account. The cybercrime highlights and perspective the range of cyber-attacks consummated globally especially in this pandemic situation.

Theme 2: Technological usage that supports in growth of cybercrime during COVID-19

In the pandemic condition of COVID-19 and due to the urge of lockdown, many people are forced to stay home by losing their jobs. During staying home they are engaging to access the internet more than before and the number of cybercrimes has become increasing in a huge range (Turner, Turner& Shen, 2020). As the majority of the percentage of the population are engaged with online networking sites and spend more time online it provides opportunities for cyber frauds to take advantage and make more money. Accompanied with developing technologies, hacking personal accounts has become the easiest way for the cyber criminals for increasing their bank balance without doing anything. In the words of Ioane, Knibbs& Tudor (2021), across the world there are an increasing number of cybercrimes in a wide range especially during COVID-19 pandemic situation. As nowadays due to the effect of COVID-19 banks are operating with few limited origins and people are instructed to use phone banking and internet banking so cyber criminals are making phishing calls (Brem, Viardot&Nylund, 2021). In this unstable social and economic situation cyber criminals are developing their knowledge by using advanced technologies to make people fool. Especially it is riskier for the aged people who have a very little knowledge about the technologies and online criminals (Singh*et al.* 2021). They become easily manipulated by cyber frauds phishing calls and share their personal details and the criminals easily hack their accounts.

Theme 3: The dramatically changing cyber security system during COVID-19

Across the world the COVID-19 pandemic situation has brought several challenges for every business. It causes massive shutdowns in maximum offices and other facilities that affect cyber security also. As opposed by Okereafor&Adelaiye (2020), due to working while staying home it makes difficulties for the employees under the cyber security provider system. They are not able to control all the facts properly as they are not accessing their professional system due to staying home. As the whole working process has shifted into online, the risk of cyber-attacks has increased a lot. Especially during COVID-19 pandemic situation cyber security has become the most important need than ever before. As per the view of Singh Lallie et al. (2020), accessing online sites are offered new opportunities for the cyber criminals or hackers to commit crimes. As the employees are not able to be as active as they should in that case day by day the numbers are enlarging very fast. Increasing numbers of cybercrimes should change their strategy and tactics to prevent these offends. Though in this current situation risk management and security leaders are focusing on deploying advanced technologies and solutions to prevent the numbers of cybercrimes (Alsawalqa, 2021). This can be able to lead the process smoothly and perfectly and consequently it can reduce the numbers.

Discussions

During the pandemic situation the case of cybercrimes has been enlarging continuously. Since due to lockdown, the people are forced to do all official work as well as unofficial work from their personal desktops, laptops or mobiles. Getting this opportunity the hackers are directly attacking the system and creating several fake websites to pin down the users. As stated by Menon et al. (2020), the cyber criminals are taking the help of various mediums to trap the user. The number of phishing calls are increasing where cyber frauds make calls to users and ask them for providing sensitive information such as credit or debit number, account number etc. The majority of aged people are getting targeted as they have lack of proper knowledge about these (Nurhayati*et al.* 2021). Another issue that can be found included cybercrimes is fake rumors that are spreading worldwide within misleading information.

Nearly 30 percent of cases related to spread misinformation have increased in this pandemic situation that responded to the global cyber offense survey (Jürgen Stock, 2020). On social media there can be found moreover 200 cases on a daily basis related to victimization in cyber offense. Day by day the number is enhancing and the users are getting trapped by the hackers. As observed by Banerjee & Rao (2020), fast and advanced technology is responsible for this issue along with cyber security is also responsible for it. If the cyber police can take strict action against this factor, the number of cybercrimes can be reduced. Otherwise in this COVID-19 pandemic situation more people will be trapped in these types of cybercrimes and get cheated.

5. Conclusion and Recommendation

Conclusion

The factors behind contributing to rising rates of cybercrime in the age of COVID-19 can be attributed to the rise of internet usage in various domains by individuals and corporations. Moreover, it can be concluded that the

lack of proper security measures has led to the rise in cybercrime rates. The inaccessibility of various cyber spaces such as deep web and dark web by the police hinders the process of criminal identification as well. Thus, these factors lead to the victimization of the general population as well as organizations resulting in long-lasting damages.

Linking with objectives

The objectives of the paper, as stated beforehand, can be fulfilled by the discussion conducted based upon a comprehensive analysis of the current status of cybercrime in the age of COVID-19. Since the pandemic has led to increasing usage of the internet for remote activities, the criminals have found better scope for committing crimes, especially related to scamming, phishing and sensitive and personal data theft.

Recommendations

It can be recommended that, for the prevention of cybercrime, the government should invest more in their cybercrime division as well as impart knowledge regarding cyber security and its requirements through various s\awareness raising programs. Large-scale corporations are recommended to conduct training programs regarding the code of conduct in dealing with cybercrime for the employees and managers.

Future scope

There is a vast scope for future research on the topic that will be beneficial for academic writers as well as organizational leaders and the overall police department dealing with cybercrime. Further research can be consulted on the topic of criminal behavior and the factors contributing towards such behavior regarding cybercrime.

Limitations of the research

The limitations of this research is the inability to identify the factors contributing towards criminal behavior regarding cybercrime and the lack of information on the impact of cultural, political and economic factors leading to the rise of cybercrime.

References

[1] Alsawalqa, R. O. (2021). Cyberbullying, social stigma, and self-esteem: the impact of COVID-19 on students from East and Southeast Asia at the University of Jordan. Heliyon, 7(4), e06711. https://www.sciencedirect.com/science/article/pii/S2405844021008148

[2] Banerjee, D., &Rao, T. S. (2020). Sexuality, sexual well being, and intimacy during COVID-19 pandemic: An advocacy perspective. Indian Journal of Psychiatry, 62(4), 418.https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7597708/

[3] Basias, N., &Pollalis, Y. (2018). Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. Review of Integrative Business and Economics Research, 7, 91-105. https://sibresearch.org/uploads/3/4/0/9/34097180/riber_7-s1_sp_h17-083_91-105.pdf

[4] Brem, A., Viardot, E., &Nylund, P. A. (2021). Implications of the coronavirus (COVID-19) outbreak for innovation: Which technologies will improve our lives?. Technological forecasting and social change, 163, 120451. https://www.ncbi.nlm.nih.gov/pmc/articles/pmc7648540/

[5] Cheng, C., Chan, L., &Chau, C. L. (2020).Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, 108, 106311.https://doi.org/10.1016/j.chb.2020.106311

[6] Hamerton, C. (2020). White-collar cybercrime: evaluating the redefinition of a criminological artifact. Journal of Law and Criminal Justice, 8(2), 67-79. https://doi.org/10.15640/jlcj.v8n2a5

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

[8] Ioane, J., Knibbs, C., & Tudor, K. (2021). The challenge of security and accessibility: Critical perspectives on the rapid move to online therapies in the age of COVID-19. Psychotherapy and Politics International, 19(1), e1581.https://onlinelibrary.wiley.com/doi/abs/10.1002/ppi.1581

[9] Jürgen Stock, 2020. INTERPOL Secretary General. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[10] Kaakinen, M., Keipi, T., Räsänen, P., &Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. Cyberpsychology, Behavior, and Social Networking, 21(2), 129-137. https://doi.org/10.1089/cyber.2016.0728

[11] Kosseff, J. (2017). Defining cybersecurity law. Iowa L. Rev., 103, 985. https://ilr.law.uiowa.edu/assets/Uploads/ILR-103-3-Kosseff.pdf

[12] 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.https://www.sciencedirect.com/science/article/pii/S0167404821000729

[13] Menon, V., Pattnaik, J. I., Bascarane, S., &Padhy, S. K. (2020).Role of media in preventing gender-based violence and crimes during the COVID-19 pandemic. Asian journal of psychiatry, 54, 102449.https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7556255/

[14] Ngo, F., &Jaishankar, K. (2017).Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. International Journal of Cyber Criminology, 11(1).2-9. https;//doi.org/10.5281/zenodo.495762

[15] Nurhayati, S., Musa, S., Boriboon, G., Nuraeni, R., & Putri, S. (2021). Community Learning Center Efforts to Improve Information Literacy in the Community for Cyber Crime Prevention during a Pandemic. Journal of Nonformal Education, 7(1). https://journal.unnes.ac.id/nju/index.php/jne/article/viewFile/26883/11400

[16] Okereafor, K., &Adelaiye, O. (2020). Randomized cyber attack simulation model: A cybersecurity mitigation proposal for post COVID-19 digital era. Int. J. Recent Eng. Res. Develop., 5(7), 61-72. https://www.researchgate.net/profile/Kenneth_Okereafor/publication/343318105_Randomized_Cyber_Attack_Simulation_Model_A_Cybersecurity_Mitigation_Proposal_for_Post_COVID-19_Digital_Era/links/5f22ca1a92851cd302c8a4b5/Randomized-Cyber-Attack-Simulation-Model-A-Cybersecurity-Mitigation-Proposal-for-Post-COVID-19-Digital-Era.pdf

[17] Okpe, V. V., &Taya, S. L. (2018). Political Perspective: Evaluating the Causes of Cybercrime in Nigeria. Asian Journal of Multidisciplinary Studies, 6, 12.https://core.ac.uk/download/pdf/229670437.pdf

[18] Puaschunder, J. M. (2020). The Future of the City after COVID-19: Digitionalization, Preventism and Environmentalism. Preventism and Environmentalism (September 27, 2020). http://society.education/wp-content/uploads/2020/12/ConScienS-Proceedings.pdf#page=130

[19] Schoonenboom, J., & Johnson, R. B. (2017).How to construct a mixed methods research design. KZfSSKölnerZeitschriftfürSoziologie und Sozialpsychologie, 69(2), 107-131.https://doi.org/10.1007/s11577-017-0454-1

[20] Sergi, A. (2018). Widening the antimafia net: Child protection and the socio-cultural transmission of mafia behaviours in Calabria. Youth justice, 18(2), 149-168.https://doi.org/10.1177%2F1473225418791420

[21] Singh Lallie, H., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., &Bellekens, X. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. arXiv e-prints, arXiv-2006. https://ui.adsabs.harvard.edu/abs/2020arXiv200611929S/abstract

[22] Singh, N., Teotia, Y., Singh, T., & Bhardwaj, P. (2021). COVID-19 Pandemic: A Sentiment and Emotional Analysis of Modified Cancellation Policy of Airbnb. In Proceedings of 3rd International Conference on Computing Informatics and Networks (Vol. 167, p. 633). Nature Publishing Group. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7972301/

[23] Turner, C., Turner, C. B., & Shen, Y. (2020). Cybersecurity Concerns & Teleworking in the COVID-19 Era: A Socio-Cybersecurity Analysis of Organizational Behavior. Journal of Advanced Research in Social Sciences, 3(2), 22-30. https://dpublication.com/journal/JARSS/article/download/502/333

[24] Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. Journal of Medical Internet Research, 22(9), e23692. https://www.jmir.org/2020/9/e23692