Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Unveiling the Shadows: Exploring Cyber Criminology and the Plight of Cyber victimization in Bangladesh

Md. Nazmul Hasan[a]

[a]Bangladesh University of Professionals, Dhaka, Bangladesh

Received 24 June 2023; *Accepted* 22 July 2023; *Published* 26 July 2023

Globally cybercrime is increasing rapidly & Bangladesh is no exception. Due to digitization, People in Bangladesh depend on the Internet for their daily work. The main reason behind cyber victimization is that many people are not aware of the pattern of cybercrime. Sometimes people cannot identify how they become victims of cybercrime. Because of that, this article tries to identify the pattern of cybercrime from the perspective of routine activity theory & space transition theory. According to routine activity theory, a crime occurs when there is a motivated offender, a suitable victim & absence of a capable guardian. An offender becomes motivated to commit an offense when there is a lack of capable guardians protecting the victim. This article applies this theory to understand the pattern of cybercrime in Bangladesh. This article also applies space transition theory to identify the reasons behind cybercrime. The main proposition of space transition theory is that individuals act differently when moving from physical space to cyberspace. This article discusses the individual's online lifestyle and connects the pattern of cyber victimization with the online lifestyle. This article also checks the applicability of cyber laws in Bangladesh from the perspective of cybercrime patterns. Furthermore, this article recommends some preventive & punitive measures to minimize cyber victimization.

Keywords: *cybercrime, cyber victimization, victimology, routine activity theory, space transition theory.*

INTRODUCTION

Cybercrime is a major concern in this digital era. There was a time when crimes were limited to the physical world. Nevertheless, in this modern time, crime is not limited to only physical space, it also spreads through cyberspace. It is challenging to control cybercrime because cyberspace is such a vast area. In physical space, all countries maintain boundaries and jurisdictions for peaceful living. There are many regulations to control people in real space. However, in cyberspace, there are no boundaries or jurisdictions. People can do whatever they want in cyberspace because, most of the time, they know that no one can catch them because cyberspace ensures anonymity. Because of these issues, cyber victimization is also increasing in huge numbers each year. As per the Forbes report, 95% of cyber security breaches happen because of human error.[1] It is difficult for law enforcement agencies to capture cybercriminals because they are more innovative and have outstanding knowledge of technology. In Bangladesh, the rate of cyber victimization is enormous, and thousands of reported crimes are listed at the concerned police stations every month.[2] It is necessary to identify the pattern of cybercrime to minimize cyber victimization. Understanding the crime pattern will make it easier to regulate cyberspace, which will help minimize cyber victimization. Most of the time, people cannot identify how they became a victim of cybercrime. Due to digitalization, people need to share their information in different online mediums. The chance of victimization is increasing because everyone is dependent on the Internet at some point. Cybercriminals use this as an advantage for them. They set various traps for people online. Since the formation of the cybercrime tribunal, more than 4500 cybercrime cases have been filed.[3] According to the Cybercrime Awareness Foundation report, all types of cybercrime have increased in Bangladesh by a large number. They surveyed 199 people of different ages, gender, and profession, and they

---

[1] 'Cybercrime: Rising Concern to Cyber World' (*Threat Cop*, January 2022) <https://threatcop.com/blog/cybercrime/> accessed 27 May 2023

[2] '55% cybercrime victims failed by police: Survey' *The Business Standard* (Bangladesh, 13 August 2022) <https://www.tbsnews.net/bangladesh/55-cybercrime-victims-failed-police-survey-476406> accessed 27 May 2023

[3] 'Bangladesh sees rise in cybercrime cases, but suspects are mostly acquitted' *The Financial Express* (06 September 2021) <https://thefinancialexpress.com.bd/home/bangladesh-sees-rise-in-cybercrime-cases-but-suspects-are-mostly-acquitted-1630908341> accessed 27 May 2023

found that among them, 23.79% are victimized by hacking & data theft. They also found that 15.06% are victimized while buying something from Facebook pages & websites.

Furthermore, 9.34% are the victims of pornography, and 50.27% are the victim of cyberbullying. They also found that 80.90% of victims in Bangladesh are between 18-30 years of age. Among the online victims, 56.78% are men & 43.22% are women in Bangladesh.[4]

METHODOLOGY

This research is qualitative & quantitative oriented. This study uses the Routine Activity theory & Space Transition theory to explain the pattern of cybercrime in Bangladesh and check Bangladesh's approach to internet regulation. The data from the survey, statutes, books, and case laws are the primary resources for this study. Additionally, the research utilized magazines, newspapers, online journals, and blogs as secondary sources of information.

For this study, the total sample size is 156 for the survey. The participants are from various backgrounds, such as Law students or Legal Practitioners, Doctors or Medical Practitioners, Engineers, Teachers, Government or Civil Service & Banking services. The majority of the participants are students & young professionals. The survey was conducted online through Google Forms. The participants were asked 27 questions related to their internet use. Most of the questions are related to their online lifestyle & their ways of using the internet. The participant wants to keep their personal information private, like name & email address, because some sensitive questions exist in the survey related to their internet lifestyle. This study ensures that this research will only use the data they provided, and their identity will not be disclosed anywhere.

The main reason behind choosing these participants is that many technical terms are used in the survey question. A minimum level of education is required to understand the question; that is why most of the participants in this survey are students & young professionals. However, this

[4] '50.27% are victims of cyber bullying: CCA Foundation Study' *DGI Bangla* (Bangladesh, 13 August 2022) <https://digibanglatech.news/english/81939/> accessed 27 May 2023

research also surveys people not included in the category of students or young professionals, such as homemakers, Labour, Poet & Unemployed people. This study assists them in understanding the survey question.

The data from the survey is analyzed in the Google Sheet. This study breaks down the data from the perspective of their online lifestyle & understanding of the cyber threat. Column chart, line chart, pie chart & area chart is used in this research to analyze the survey data. This research divides the data into several categories and then inserts them manually in the Google sheet. After that, this study uses the built-in data analysis process in Google Sheets to determine the final version of the survey result. In Google Sheets, this study breaks down the data into several parts. This survey tries to find people's internet behavior & establishes an explanation regarding the pattern of cybercrime in Bangladesh from the perspective of victimology.

LITERATURE REVIEW

Many academics are attempting to understand the pattern of cybercrime from a new angle. Scholars believe understanding cybercrime patterns will make it easier to reduce cyber victimization. Cybercrime differs from traditional crime in many ways. Because cyberspace is vast, it can be challenging to pinpoint the exact location of the cybercriminal.

Mahesh Bhalla in his paper 'Theorizing Cybercrime: Applying Routine Activities Theory' attempted to identify the pattern of cybercrime by applying one of the victimology theories, routine activity theory.[5] The author successfully explained some cybercrime patterns but did not apply this theory to any specific region; rather, the author generalized cybercrime and attempted to explain the patterns from the perspective of routine activity theory.

Behzat Yucedal tried to explain the crime pattern of cyberspace from the perspective of routine activity theory and lifestyle exposure theory in his book 'Victimization in Cyberspace: an

[5] Micah-Sage Bolden and Mahesgh Bhalla, 'Theorizing Cybercrime: Applying Routine Activities Theory' (2014) CJ 801

application of routine activity and lifestyle exposure theories'.[6] In his book, Behzat Yucedal explained guardianship of the digital space which is a significant analysis in this field of study.

Brigadier General Md. Khurshid Alam, in his paper, 'Cybercrime in Bangladesh: implications and response strategy' discussed the cybercrime pattern and cybercrime victimization from the perspective of Bangladesh.[7]

In his paper, he discussed different types of cybercrime and recommended some preventive measures from the perspective of Bangladesh. In 'Cybercrime in Vietnam: an analysis based on routine activity theory'[8] Trong Van Nguyen discussed the pattern of cybercrime in Vietnam from the perspective of routine activity theory. Trong Van Nguyen checks the applicability of routine activity theory on the cybercrimes of Vietnam by analyzing various data.

Md. Kamruzzaman, Md. Ashraful Islam, Md. Shahidul Islam, Md. Shakhawat Hossain and Md. Abdul Hakim in their paper 'Plight of Youth Perception on Cyber Crime in South Asia' conducted a descriptive cross-sectional study at Tangail and Dhaka north city corporation areas in Bangladesh.[9] This study shows exciting findings and data regarding Bangladesh's nature and cybercrime victimization.

In his book 'Code and Other Laws of Cyberspace' Lawrence Lessig tried to analyze the code of cyberspace laws from four different perspectives. Those codes are the architecture, market, law, and norm codes.[10]

---

[6] Behzat Yucedal, 'Victimization in cyberspace: an application of routine activity and lifestyle exposure theories' (DPhil Theses, Kent State University 2010)

[7] Brigadier General Md. Khurshid Alam, 'Cybercrime in Bangladesh: implications and response strategy' (2011) 10(2) NDC E-Journal <https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/view/82> accessed 27 May 2023

[8] Trong Van Nguyen, 'Cybercrime in Vietnam: an analysis based on routine activity theory' (2020) 14(1) International Journal of Cyber Criminology <https://doi.org/10.5281/zenodo.3747516> accessed 27 May 2023

[9] Md. Kamruzzaman et al., 'Plight of Youth Perception on Cyber Crime in South Asia' (2016) 2(4) American Journal of Information Science and Computer Engineering <https://www.semanticscholar.org/paper/Plight-of-Youth-Perception-on-Cyber-Crime-in-South-Kamruzzaman-Islam/5e13a21ade35026922f3623546949456a65f9d3e> accessed 27 May 2023

[10] Lawrence Lessig, *Code: And other laws of cyberspace* (2nd edn, 2009)

Hee Jhee Jiow, in his paper 'Cyber Crime in Singapore: An Analysis of Regulation Based on Lessig's Four Modalities of Constraint' adopted four of Lessig's codes for analyzing Singapore's approaches to internet regulation. The author concentrated solely on regulation and did not attempt to connect pattern and regulation.[11]

Mohammad Mamunur Rashid & Sharmin Akter, in their paper 'Combating Cybercrime in Bangladesh: National and International Legal Framework' discussed that cooperation among the countries is required to prevent cybercrime. Universally common laws & Cooperative laws are essential for the prevention of cybercrime & minimization of cyber victimization.[12]

Md. Raziur Rahman in his paper 'Prevention of Cybercrimes in Bangladesh' also suggested a proper legal framework for regulating cyberspace & for the prevention of cybercrime.[13]

Badshah Mia in his article 'Cybercrime & Its Impacts in Bangladesh: A Quest for necessary legislation' discussed the impacts of cybercrime in Bangladesh and analyzed it from the perspective of personal life and the workplace. He also provided guidelines for policymakers regarding the prevention of cybercrime.[14]

Md. Abu Bakar Siddik & Saida Talukder Rahi, in their paper 'Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context' discussed cybercrime in social media and the existing laws related to cybercrime in Bangladesh.[15]

---

[11] Hee Jhee Jiow, 'Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint' (2013) 7(1) International Journal of Cyber Criminology <https://www.cybercrimejournal.com/pdf/Jiow2013janijcc.pdf> accessed 27 May 2023

[12] Mohammad Mamunur Rashid and Sharmin Akter, 'Combating Cybercrime in Bangladesh: National and International Legal Framework' (2014) 8(1) Society & Change <https://societyandchange.com/uploads/1509597597.pdf> accessed 27 May 2023

[13] Md Raziur Rahman, 'Prevention of Cyber Crimes in Bangladesh' (2017) 11(4) Society & Change <https://societyandchange.com/uploads/1537010147.pdf> accessed 27 May 2023

[14] Badsha Mia, 'Cybercrime & Its impact in Bangladesh: A quest for necessary legislation' (2014) 2(4) International Journal of Law and Legal Jurisprudence Studies <http://ijlljs.in/wp-content/uploads/2015/06/Cyber-Crime_Article_IJLLJS1.pdf> accessed 27 May 2023

[15] Md Abu Bakar Siddik and Saida Talukder Rahi, 'Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context' (2019) 5(1) BiLD Law Journal <https://bildbd.com/index.php/blj/article/view/34/32> accessed 27 May 2023

K Jaishankar in his paper 'Establishing a Theory of Cyber Crimes' introduced a new theory to explain the pattern of cybercrime. The theory's name is the space transition theory. The author stated that according to space transition theory, individuals feel comfortable committing an offence in cyberspace because of the anonymous nature of cyberspace.[16]

Ajibade. A. Abayomi in his paper titled 'Applying Space Transition Theory to Cyber Crime: A Theoretical Analysis of Revenge Pornography in the 21st Century' applied space transition theory to cybercrime to analyze revenge pornography. The author discussed seven propositions in his paper to check the applicability of space transition theory.[17]

In his book 'Cybercrime & Internet' David Wall discussed the connection between criminology & cybercrime. Wall organized his book into three sections. In the first section, the author discussed cybercrime & Internet. In the second part, the author tried to connect cybercrime with criminology, and in the final section, the author discussed cybercrime & criminal justice system.[18]

Moreover, in the book 'Cybercrime & Society' Majid Yar offers a concise, methodical, and insightful introduction to the ongoing discussions about cybercrime. It is the first book to examine the full spectrum of cybercrime-related issues by combining criminology, sociology, law, politics, and cultural studies perspectives.[19]

K Jaishaknar in his book 'Cyber Criminology: Exploring Internet Crimes and Criminal Behavior' explains the pattern of internet crime & criminal behaviour in cyberspace from the perspective of cyber-criminology. The author discussed that victimization in cyberspace is increasing

[16] Karuppannan Jaishankar, 'Establishing a theory of Cyber Crimes' (2007) 1(2) International Journal of Cyber Criminology <https://doi.org/10.5281/zenodo.18792> accessed 29 May 2023
[17] Ajibade. A. Abayomi, 'Applying Space Transition Theory to Cyber Crime: A Theoretical Analysis of Revenge Pornography in the 21st Century' (2020) 5(11) International Journal of Innovative Science and Research Technology <https://ijisrt.com/applying-space-transition-theory-to-cyber-crime-a-theoretical-analysis-of-revenge-pornography-in-the-21st-century> accessed 29 May 2023
[18] David Wall, *Cybercrime & Internet* (1st edn, Routledge 2001)
[19] Majid Yar and Kevin F. Steinmetz, Cybercrime & Society (3rd edn, SAGE Publications Ltd 2019)

because cyber criminals developed various ways to remain anonymous. The nature of cyberspace generally provides the offender with these advantages.[20]

Hamid Jahankhani in his book 'Cyber Criminology (Advanced Sciences and Technologies for Security Applications)' provided a thorough overview of the ongoing and new problems associated with cyber criminology & victimization. It is a compilation of the collaboration between academics and professionals in cybercrime, IT law, and security.[21]

Elza Syarief in her paper 'Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia' discussed the security issues of electronic land registration. In this paper, the author discusses the significance of electronic land registration and analyzes the legal policies against hacking & online fraud in digital land registration systems.[22]

In the paper 'Routine Activity Theory and the Determinants of High Cybercrime Countries' Alex Kigerl discussed routine activity theory & cybercrime. This study found that the cybercrime rate is higher in those nations with more internet users. The author conducts the study on high cybercrime countries only, not individuals.[23]

Bradford W. Reyns in his paper 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses' tries to expand the scope of routine activity theory in cyberspace where offender & victim never come into physical contact. According to his paper, the individual who uses the Internet for banking,

---

[20] K. Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (1st edn, CRC Press 2011)
[21] Hamid Jahankhani, Cyber Criminology (Advanced Sciences and Technologies for Security Applications) (1st edn, Springer 2018)
[22] Elza Syarief, 'Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia' (2022) 16(2) International Journal of Cyber Criminology <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/88> accessed 29 May 2023
[23] Alex Kigerl, 'Routine activity theory and the determinants of high cybercrime countries' (2012) 30(4) Social Science Computer Review <https://doi.org/10.1177/0894439311422689> accessed 29 May 2023

email/messages become victimized by identity theft most of the time. He added that online shopping & downloading behaviour is also one of the reasons behind online victimization.[24]

Eric Rutger Leukfeldt & Majid Yar in their paper 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis' analyzed different sorts of cybercrime from the perspective of routine activity theory. They used routine activity theory as an analytical framework to study cybercrime.[25]

Sarah Gordon & Richard Ford in their paper 'On the definition and classification of cybercrime' defined cybercrime and analyze cybercrime from two different categories. As per their study, there are two types of cybercrime. These are cybercrimes that are technological in nature & cybercrime which contain human elements.[26]

Nataliya B. Sukhai in her paper 'Hacking & Cybercrime' discussed hacking & applicable laws & regulations for hacking in the U.S.[27]

Furthermore, Jia-Rong Sun, Mao-Lin Shih and Min-Shiang Hwang in their paper 'A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure' discusses the cybercrime investigation procedure & they also make a comparative analysis between the cybercrime investigation and traditional method of investigation.[28]

---

[24] Bradford W. Reyns, 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses' (2013) 50(2) Journal of Research in Crime and Delinquency <https://doi.org/10.1177/0022427811425539> accessed 29 May 2023

[25] Eric Rutger Leukfeldt and Majid Yar, 'Applying routine activity theory to cybercrime: A theoretical and empirical
Analysis' (2016) 37(3) Deviant Behavior <https://doi.org/10.1080/01639625.2015.1012409> accessed 29 May 2023

[26] Sarah Gordon and Richard Ford, 'On the definition and classification of cybercrime' (2006) 2 Journal in Computer virology <https://link.springer.com/article/10.1007/s11416-006-0015-z> accessed 29 May 2023

[27] Nataliya B. Sukhai, 'Hacking and Cybercrime' (1st Annual Conference on Information Security Curriculum Development, October 2004) <https://dl.acm.org/doi/abs/10.1145/1059524.1059553> accessed 29 May 2023

[28] Jia-Rong Sun et al., 'A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure' (2015) 17(5) International Journal of Network Security <http://ijns.jalaxy.com.tw/contents/ijns-v17-n5/ijns-2015-v17-n5-p497-509.pdf> accessed 29 May 2023

Wingyan Chung, Hsinchun Chen, Weiping Chang & Shihchieh Chou in their paper 'Fighting Cybercrime: a review and the Taiwan Experience' defines different types of cybercrime and make a comparative study on laws & regulations related to cybercrime in different countries. Furthermore, they also discuss the nature of cybercrime in Taiwan & their existing laws & rules to regulate cybercrime.[29]

CA Virendra K. Pamecha in his book 'The Cyber Crimes & The Cyber Law: Be Aware and Beware of'elaborately discussed the major cybercrime from an Indian perspective. The author also analyzes the existing Indian laws & case laws related to cybercrime. Furthermore, the author also discusses preventive measures against cybercrime.[30]

Travis C. Pratt, Kristy Holtfreter & Michael D. Reisig in their paper 'Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory' analyzed routine activity & consumer behaviour and tries to establish how consumer behaviour online exposes them to the motivated offender. This paper explains the online fraud pattern from the routine activity theory perspective.[31]

Alice Hutchings & Hennessey Hayes in their paper 'Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?' surveyed 104 people & finds that among them, 50 participants received phishing emails from cyber offenders. The study discusses the victimization pattern of phishing from the perspective of three elements of routine activity theory.[32]

Furthermore, Meghan E. Hollis, Marcus Felson & Brandon C. Welsh in their paper 'The capable guardian in routine activities theory: A theoretical and conceptual reappraisal' analyzed the

---

[29] Wingyan Chung et al., 'Fighting cybercrime: a review and the Taiwan experience' (2006) 41(3) Decision Support Systems <https://doi.org/10.1016/j.dss.2004.06.006> accessed 29 May 2023

[30] Virendra K. Pamecha, *The Cyber Crimes & The Cyber Law: Be Aware and Beware of!* (Xcess Informatics & Services 2018)

[31] Travis C. Pratt et al., 'Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory' (2010) 47(3) Journal of research in crime and delinquency <https://doi.org/10.1177/0022427810365903> accessed 29 May 2023

[32] Alice Hutchings & Hennessey Hayes, 'Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?' (2009) 20(3) Current Issues in Criminal Justice <https://doi.org/10.1080/10345329.2009.12035821> accessed 29 May 2023

concept of a capable guardian, which is one of the important elements of routine activity theory. Their paper shows the evolution of the concept of a guardian in routine activity theory.[33]

Nevertheless, E. Rutger Leukfeldt in his paper 'Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization' discussed the nature of phishing victimization in the Netherlands from the perspective of routine activity theory. The author also discusses a few factors, such as visibility, value & accessibility, to explain the pattern of online victimization by phishing.[34]

Md. Abu Hanif in his paper 'Cybercrime and Cyber Law: Growth of The State Concerns and Initiatives in Bangladesh' analysis the existing laws & regulations of Bangladesh regarding cybercrime. The author also discusses the regional approach & international approach to regulating cybercrime. Moreover, the author also suggests some preventive measures to minimize cyber victimization.[35]

The existing literature analyzes cybercrime from various perspectives. Some scholars focused on the legal & policy related to cybercrime & others focused on the analytical study of cybercrime. In Bangladesh, not enough paper focuses on the cyber victimization pattern. Apart from this, study related to cyber victimization in Bangladesh from the perspective of routine activities & space transition theory is very rare. There need to be more studies that discuss the cybercrime pattern in Bangladesh. Some literature deals with the pattern of cyberspace crime in foreign countries, but studies from Bangladesh's perspective are very few. The existing literature on cybercrime in Bangladesh mainly discusses cybercrime rates and legal frameworks. Very few studies apply theories of victimology to understand cybercrime. This study applies victimology theories to understand the pattern of cyberspace crime in Bangladesh.

---

[33] Meghan E. Hollis et al., 'The capable guardian in routine activities theory: A theoretical and conceptual reappraisal' (2013) 15 Crime Prevention and Community Safety <https://link.springer.com/article/10.1057/cpcs.2012.14> accessed 29 May 2023

[34] E. Rutger Leukfeldt, 'Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization' (2014) 17(8) Cyberpsychology, Behavior, and Social Networking <https://doi.org/10.1089/cyber.2014.0008> accessed 29 May 2023

[35] Md. Abu Hanif, 'Cybercrime and Cyber Law: Growth of The State Concerns and Initiatives in Bangladesh' (2018) 5(2) Journal of Logistics, Informatics and Service Sciences <http://www.aasmr.org/liss/Vol.5/Vol.5_No.2_2.pdf> accessed 29 May 2023

In Addition, this study also discusses the existing legal framework in Bangladesh. The architecture of cybercrime is not fixed, and the nature of cybercrime is changing continuously, that's why more studies in this field are required to understand cyberspace better. If the legislator wants to enact a proper law regarding cybercrime, they first need to understand the architecture of cyberspace. This study tries to fulfill the gap by studying online victimization in Bangladesh from the perspective of victimology.

CONCEPTUAL FRAMEWORK

There was a time when cybercrime was known as computer time[36] because to conduct a crime in cyberspace, two things were essential. Those are a computer and a stable internet connection. Sometimes, an internet connection is optional for committing a cyberspace crime as it is known, data theft or the illegal transfer of data from one computer to another is also known as cybercrime or Digital Crime. That's why this type of crime was once known as computer crime.

Nevertheless, recently, under the new perspective of cybercrime, it is not only limited to the only computer. Now, the offenders use their cell-phone and electronic gadgets to commit cybercrime. Devices connected through the internet are now a potential tool for cyberspace crime; also, people with stable internet connections are potential victims of cyberspace crimes.

It is the uniqueness of cyberspace crime. In cyberspace, some common crimes are as follows:

Hacking: Hacking means unauthorized access to a computer or network system.[37] The cyber offenders involved in Hacking are highly skillful & well-trained. It takes sufficient knowledge and expertise to breach a computer system. Hacking is well-known and considered the most severe offence in cyberspace.

Phishing: Phishing is quite similar to Hacking. However, there is a slight difference between Hacking and Phishing. In Phishing, the victim also participates. The offenders send phishing links to the potential victim, and when the potential victim clicks the link by mistake, all his

[36] Behzat Yucedal (n 6)
[37] Lawrence Williams, 'What is Hacking? Types of Hackers (Introduction to Cyber Crime)' (*GURU99*, 30 June 2023) <https://www.guru99.com/what-is-hacking-an-introduction.html> accessed 29 May 2023

login credentials transfer to the offender's device[38] and then, the offenders take control of the victim's online accounts.

Ransomware Attack: Ransomware is a kind of Malware. Internet Users sometimes download software or games from pirated sites because pirated sites get these for free. The cyber offenders use this as a trap, attaching malicious codes with the cracked software.[39] When the users install pirated software on their computers, the offenders control the victim's computer entirely by utilizing malicious codes. The offender encrypted all the data on the victim's computer and demanded money for the files. It is the concept of a ransomware attack.

Identity Theft: Identity theft is one of the most common cybercrimes in Bangladesh. Cyber-offenders sometimes pretend to be a close relative of the potential victim and sometimes pretend to be a well-known person and ask for money.[40] Sometimes offenders use fake identities to steal data from the computer system.

Internet Fraud: Cyber-offenders use the logo of a well-known brand and create fake social media accounts & websites by using those brand logos. They create a fake marketing campaign with unbelievable discounts & offers. These campaigns misguide online users and become victimized by Online Fraud.

Cyberbullying: Cyberbullying is also the most common cyberspace crime. Teenagers & Females are the primary victims of cyberbullying. Cyberbullying consists of sending, uploading, or spreading harmful, inaccurate, or offensive information about another person. It may involve

[38] Danny Palmer, 'What is phishing? Everything you need to know to protect yourself from scammer' (*ZDNET*, 08 April 2023) <https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more/> accessed 29 May 2023

[39] 'What Is Ransomware?' (*ProofPoint*) <https://www.proofpoint.com/us/threat-reference/ransomware#:~:text=Ransomware%20scans%20a%20local%20device,could%20halt%20services%20and%20productivity> accessed 29 May 2023

[40] Ben Luthi, 'What Is Identity Theft and How Do I Make Sure It Doesn't Happen to Me?' (*Experian*, 19 September 2023) <https://www.experian.com/blogs/ask-experian/what-is-identity-theft/> accessed 29 May 2023

disclosing private or confidential information about another individual that causes embarrassment or humiliation.[41]

Malware: The concept of Malware is similar to phishing & ransomware attacks. Cyber Criminals sometimes send phishing emails with attachments. That attachment contains malicious codes; whenever the victim ìdownload those attachments, the offender can access the victim's computer.[42] In a Malware attack, the cyber offender can steal the victim's passwords and other important documents from the victim's computer.[43]

ROUTINE ACTIVITY THEORY & CYBERCRIME

According to routine activity theory, three elements are vital when a crime occurs. Those three elements are potential victim, absence of capable guardian & motivated offender. However, victimization under routine activity theory can be discussed under the four major concepts. Those are as follows:

Proximity: Generally, when a crime occurs in the physical world, it is evident that the victim & the offender met with each during the incident. In another way, it can be said that the offender needs to know the victim's location and check the accessibility before committing a crime.[44] If the potential victim is not accessible or lives in a highly secured zone, it is difficult for the offender to commit the crime. So, accessibility is one of the main factors behind crime. Interestingly in cyberspace, everyone lives under the same roof. Here the word 'roof' is used as a metaphor. Because in cyberspace, there is no boundary, and any motivated offender can attack a potential victim from anywhere in the world without any physical contact. That is why the rate of victimization is higher in cyberspace because if an internet user somehow makes a tiny mistake while browsing then there is a high chance that the user will become the victim of

---

[41] Ashley Abramson, 'Cyberbullying: What is it and how can you stop it?' (*American Psychological Association*, 07 September 2022) <https://www.apa.org/topics/bullying/cyberbullying-online-social-media> accessed 29 May 2023

[42] Ivan Belcic, 'What Is Malware and How to Protect Against Malware Attacks?' (*Avast*, 20 January 2023) <https://www.avast.com/c-malware> accessed 17.04.2023

[43] Ben Lutkevich, 'Malware' (*Tech Target*, June 2022) <https://www.techtarget.com/searchsecurity/definition/malware> accessed 30 May 2023

[44] *Ibid*

cybercrime. For example: If someone clicks any unknown links or attachments then there is a chance of cyber victimization. Cyberspace is like a high crime rate area where the motivated offender always seeks a suitable target. The architecture of cyberspace is unique in that it sometimes feels like living with the offender in the same neighbourhood.

Exposure: In the physical world, if a person walks alone in a high crime rate area, then theoretically, he is exposed to crime, and the offender will take the chance to attack him because the target is visible.[45] The visibility of the suitable target is basically known as exposure to crime Exposure to crime or the target's visibility in cyberspace does not work like in the physical world because each & every piece of information an internet user shares are reserved on a different server. Sometimes people share their personal information on many popular websites, thinking that it will remain safe. Everything is visible in cyberspace. An offender just needs to break the privacy to get access to the data. Cyberspace is a high crime rate area, and anyone can be a suitable target because of the visibility of the information.

Target Attractiveness: In the physical world, the offender's main targets are jewellery, money, and other valuable objects. These things always attract the offender because of their value. However, in cyberspace, digitally stored data, photographs, and documents are the main target for the offender.[46] Sometimes the offender demands money from the victim in exchange for data, or sometimes, they sell the data on the dark web to the highest bidder. The offender chooses the potential target from their lifestyle in cyberspace. They generally stalk random persons and select a suitable target whose activities in cyberspace indicate that they may contain confidential data or that personal data might have a huge monetary value. Celebrities are the primary victim when the offender only targets an individual's confidential information. However, sometimes cybercriminals take control of the victim's personal computer and demand money in exchange for the existing files & documents. If the victim is unwilling to pay the ransom, the offender destroys the documents & files from that personal computer.

[45] Eric Rutger Leukfeldt and Majid Yar (n 25)
[46] Behzat Yucedal (n 6)

Guardianship: According to routine activity theory guardian means any person or object which demotivates the offender from committing a crime. For example: Friends, Parents, a Door lock, a CC camera and Police Van.[47] The presence of these elements demotivates a potential offender from committing a crime. When someone hears about a guardian, they may think it means parents, close friends, or relatives. However, in routine activity theory, guardianship is slightly different. If someone keeps a bicycle in an insecure place, the bicycle will become a potential target for the motivated offender. Nevertheless, if a CC camera covers the area, the offender will restrain himself from committing the crime. Here, the CC camera plays the role of guardian. A police van in a high crime rate area plays the role of guardian. Parents, friends, and an unknown crowd sometimes play the role of a guardian under this theory because these elements demotivate an offender from committing a crime. To analyze the crime pattern in cyberspace, scholars started to divide the concept of guardianship into two parts. Those are physical guardians & digital guardians.[48] The concept of digital refers to the software & security measures mainly used for online security and privacy, such as Antivirus software, Password Managers, Virtual Private Networks (VPNs), Encryption Software, Two-Factor Authentication, Firewalls, Ad Blockers, and Anonymous Web Browsers.

SPACE TRANSITION THEORY & CYBERCRIME

Space transition theory was proposed by K. Jaishankar in 2008.[49] **The proposition of this theory is as follows:**

According to this theory, due to their status & position in the physical world, sometimes people restrain themselves from committing crimes in the physical world. However, in cyberspace, people can easily hide their status & position, and they feel comfortable committing an offence in cyberspace. Individuals care about their social status and position. That is why they usually avoid any types of occurrence which may harm their reputation in the physical space. In a society, people are also bound by laws & social norms, which also play a vital role in

[47] Micah-Sage Bolden and Mahesgh Bhalla (n 5)
[48] *Ibid*
[49] K. Jaishankar (n 20)

demotivating a potential offender to engage in any offence in physical space. K. Jaishankar used the term 'Repressed behaviour' to explain this type of behaviour of the offender. Repressed behaviour does not mean criminal behaviour that is repressed from childhood, instead, it means characteristics of an individual who does not fully express him in the physical world because of dignity & social status.

Another proposition of this is that cyberspace ensures anonymity & identity flexibility.[50] The flexibility of identity encourages a potential offender to commit a cyber offence. Furthermore, criminal behaviour in cyberspace is sometimes imported into physical space, and criminal behaviour in physical space is sometimes exported to cyberspace. People often unite in cyberspace to commit an offence in physical space. In the same way, sometimes, people unite in physical space to commit an offence in cyberspace. Another serious concern about cyberspace is that one can never know with whom one interacts. People can always assume false identities and continue to chat with you for days or months before you finally discover that the person you are communicating with is not who he claims to be. In other words, one cannot accurately determine the identity and the information given by the person in cyberspace.

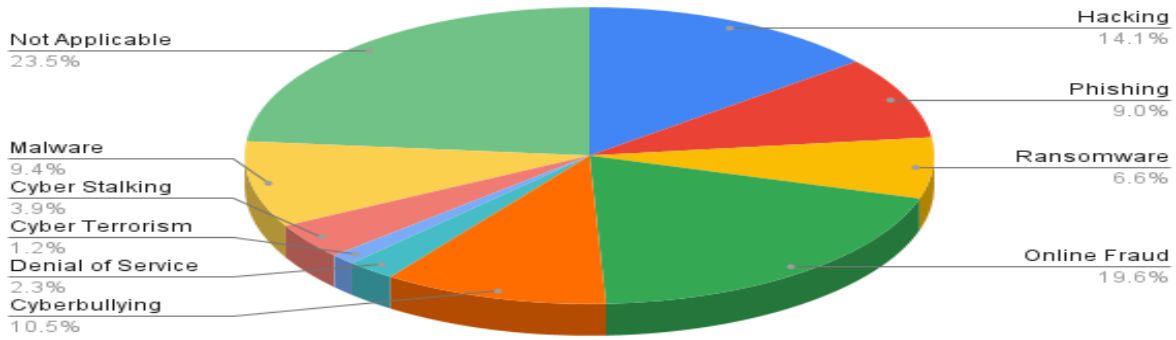
Prior to the year 2000, cybercriminals were acting alone.[51] They committed the majority of computer-related crimes in an individual capacity. The primary motivation that drove them into so solo offending was anonymity in cyberspace. However, in the last few years, cybercriminals have become more professional than their previous profile. They involve in hacking and other computer-related crimes either as a pastime or sometimes even to earn extra money. Furthermore, in cyberspace, people download & share pirated music, movies, tv-series & video games from different websites. Piracy is considered a major crime. However, in cyberspace, people do not care about laws or ethics. They continuously browse pirated sites knowing that these sites are illegal. The main reason behind this is that cyberspace ensures anonymity, and people believe that their illegal activities will remain identified. Law-abiding citizens of physical space are also involved in these types of online activity.

[50] *Ibid*
[51] *Ibid*

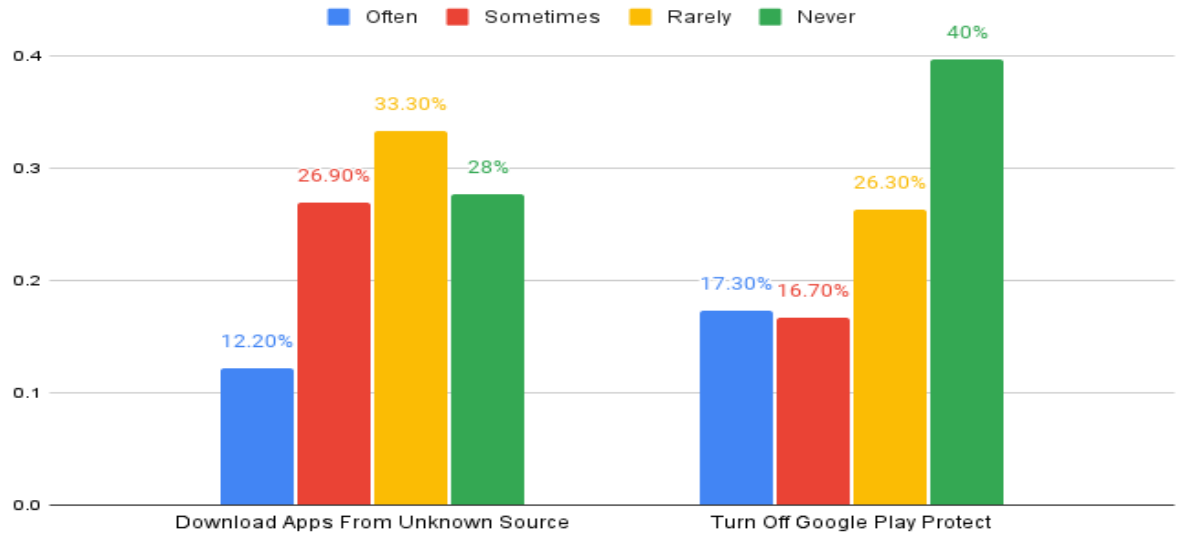
PATTERN OF CYBERCRIME IN BANGLADESH

This study asks the participants various questions related to the online lifestyle. A total of twenty-seven questions were asked to the participants in four categories. In the first category, the study asks them about their experience with online Victimization. The second category question is about their online lifestyle, the third category is about their online security measures and the fourth is about knowledge and opinion regarding existing cyber laws in Bangladesh.

Most of the participants faced multiple cybercrimes as per the survey. As per the data provided by the participants, 19.6% of people were victimized by online fraud. The rate of Victimization by Hacking is 14.1%, Victimization by cyberbullying is 10.5%, Victimization by Malware Is 9.4%, Victimization by phishing is 9.0% & ransomware attacks victimized 6.6%. The participants were also victimized by cyber offences such as Cyber Stalking, Cyber Terrorism & Denial of Service Attacks.



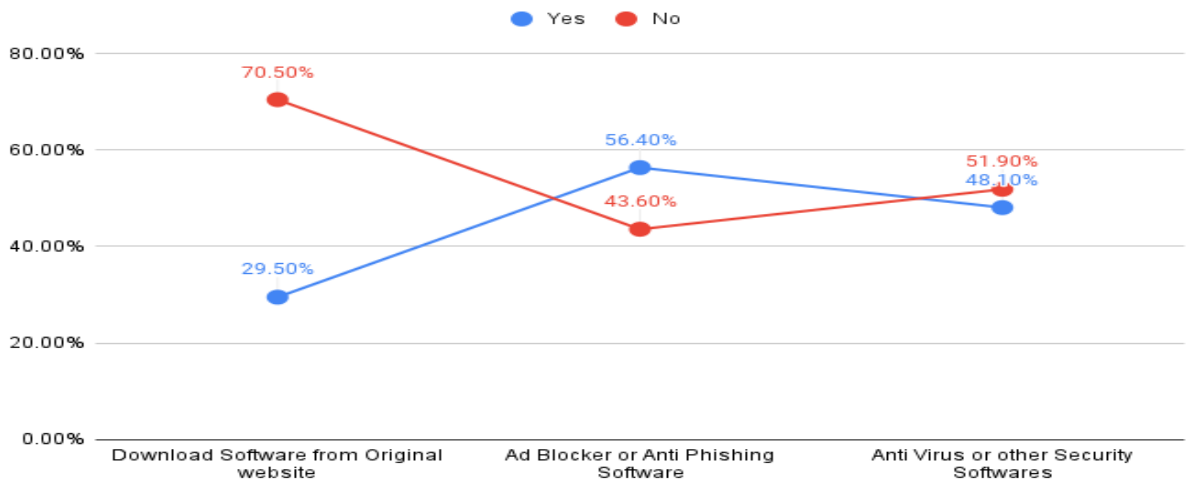
One of the main reasons behind this is that most participants do not use proper security measures in cyberspace. They download apps from unknown sources & to install these apps they sometimes turn off their google play protect. Google Play protect use to protect the device from harmful apps.



From the data, this study finds that 72% of participants downloaded apps from unknown sources at some point. Furthermore, 60% of participants turn off google play protect to install those apps on their devices. This types of activity of the users create the risk of victimization. When the user downloads apps of unknown developers, there is a chance that those apps may contain malicious codes. That is why when they try to install these apps, google play protect does not recognize the codes or the developer. 'Google play protect usually restricts app that contains malicious codes from installing on the device.[52] To forcefully install the app on the device, the users turn off their google play protection. The user download apps from unknown sources because they get cracked app from that source. If they legally download it from the google play store, they sometimes have to pay money to use some unique app features. To get that unique feature for free, the user mainly downloads cracked apps from illegal sources. From the perspective of routine activity theory, security options such as google play protect play the role of digital guardian. The offender knows that people will search for the free version of the paid app online. That is why most of the time, they create fake websites and upload fake apps with viruses.

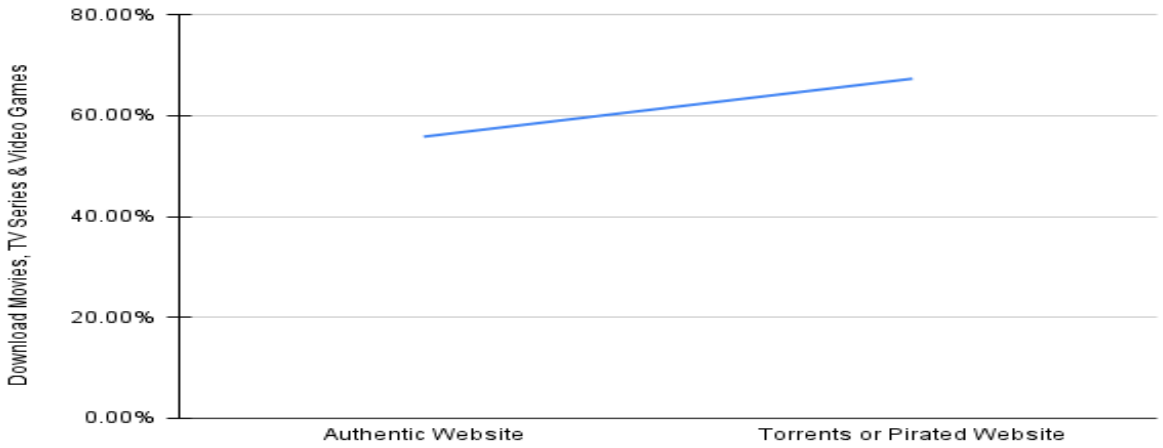
[52] 'Google Play Protect' (*TechTarget*) <https://www.techtarget.com/searchsecurity/definition/Google-Play-Protect> accessed 02 June 2023

According to the routine activity theory, the users who download these apps from unknown sources are potential victims. Furthermore, when they turn off their google play protect to install these cracked apps, this can explain by the absence of capable guardians. In this way, people become victimized in cyberspace. Though people know downloading apps from the pirated site is illegal, they are still doing it. Moreover, in the survey, most participants represent the educated class in Bangladesh. So, from the perspective of space transition theory, law-abiding & educated citizens in physical space are completely doing different acts in cyberspace. Furthermore, this survey finds that many participants do not buy software from original websites. They use pirated or cracked software, one of the main reasons behind victimization through hacking & ransomware attacks. The survey shows that 70.50% of participants do not buy software from the original website. The number is shocking. The high price rate of the original software is the main reason behind this. Typically, cracked software contains malicious codes; when the users install it on their personal computers, the hacker can easily take control of all the files on the victim's computer.[53] When hackers take control of the victim's computer then they demand money in exchange for the control. That is why this crime is also popularly known as a ransomware attack.



[53] Mary McMahon, 'What is Pirated Software?' (*Easy Tech Junkie*, 07 April 2023) <https://www.easytechjunkie.com/what-is-pirated-software.htm> accessed 02 June 2023

Moreover, most participants do not use Anti-Virus or other security software on their devices which is also a reason behind cyber victimization. This survey shows that only 56.40% of participants use Ad-Blocker or Anti-Phishing software, and 48.10% use Anti-Virus or other security software to protect their devices. Furthermore, the participants also download movies, video games & TV series from pirated websites. The attachments or files in the pirated website are full of viruses and when the user clicks or downloads these files, they become victimized by the malware attack.[54]



As per the survey, 67.30% of participants download movies, tv series & video games from torrents or pirated sites. If people want to watch movies & tv series on an authentic website, they need to pay subscription fees yearly, half-yearly or monthly. People download original content from pirated sites because sometimes they cannot afford the subscription fee.

This pattern is also similar to the previous crime pattern. When people download software from pirated websites, they need to turn off their Windows security system to install this software.[55] Turning off the windows defender system is considered the absence of a digital guardian. Most of the time, people become victims of ransomware attacks by installing pirated software on their

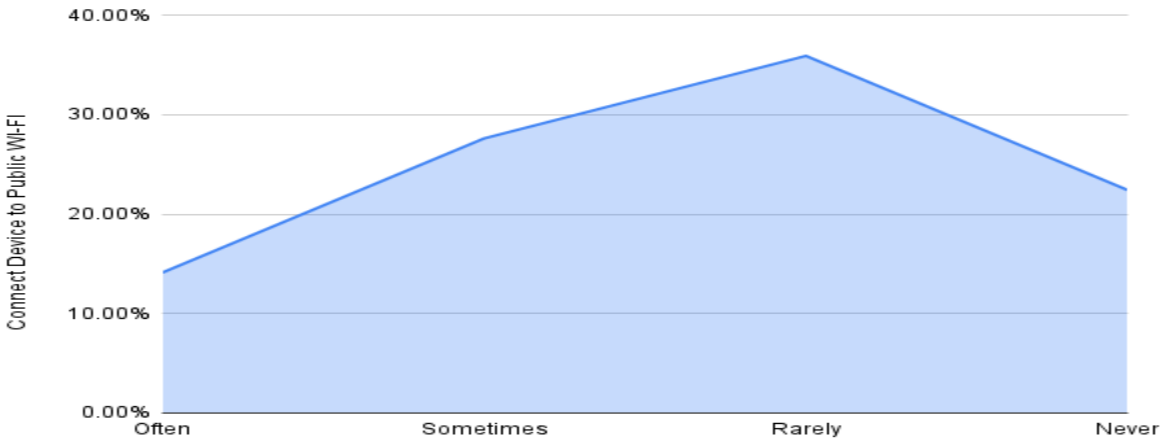
[54] Silviu STAHIE, 'Pirated Movies Are Used to Distribute Malware' (*Bitdefender*, 30 April 2020) <https://www.bitdefender.com/blog/hotforsecurity/pirated-movies-are-used-to-distribute-malware/> accessed 02 June 2023

[55] Mary McMahon (n 53)

computers. The offender knows that people will search for free software, which is why they take this advantage by tricking people into downloading software containing malicious codes.

The same goes for downloading movies, tv-series & video games from unknown sites. Many people become victimized by malware attacks by clicking unknown attachments. Software like Anti-virus & Anti-phishing works as a digital guardian in these cases. Sometimes people click unknown links to download something from illegal sites. The Anti-Virus or Anti-Phishing software can detect these malicious links. The motivated offender uses these tricks to find a potential victim. If the potential victim increases the security system or digital guardian and browses safely, he is less likely to be victimized.

Recently, Cybercriminals have used Public WI-FI as a tool for hacking. Nowadays, people connect their phones to the Public WI-FI network whenever they visit restaurants or shopping malls. Most of the time, criminals use this WI-FI network as a trap. When the potential Victim connects his device to public WI-FI, the offender can access all the files on Victim's phone.[56] The scary thing is that the offender can use the feature of the Victim's device, such as a camera & microphone.



[56] Kathy Haan, 'The Real Risks Of Public Wi-Fi: Key Statistics And Usage Data' (*Forbes*, 9 February 2023) <https://www.forbes.com/advisor/business/public-wifi-risks/> accessed 03 June 2023

As per the survey result, this study finds that 77.60% of people at some point connect their devices to public WI-FI. Only 22.40% of people never connect their devices to public WI-FI. Cybercriminals can utilize public WI-FI and monitor every activity, password, and transaction in the connected devices. From the survey, this study realizes that most participants are unaware of the risk of Public WI-FI. Some think WI-FI in popular restaurants, coffee shops or shopping malls is safe. Nevertheless, it works differently. The criminals use the technique known as MTM (Man in the Middle) to take control of the device connected to public WI-FI. In this technique, the victim will believe that he is connected with the original WI-FI but behind the scene, he is connected with the offender's device.

The security of public WI-FI is vulnerable. The restaurants & shopping malls provide free WI-FI or give easy passwords by considering their customers' benefits. Many devices are connected to public WI-FI, so the offender becomes motivated to target it. The vulnerable security system of public WI-FI can be considered as the absence of capable guardians. Because of the vulnerable security, many people become victimized using free WI-FI networks. People in Bangladesh are now highly dependent on different technology & gadgets. The offender takes this as an advantage for committing cybercrime. According to routine activity theory, visibility and accessibility are essential factors behind cybercrime.[57]

Most of the online users in Bangladesh are young aged people. They depend on the Internet for their daily work, making them visible to the cyber offender. When individuals spend most of their time online, they become accessible too. For example, a person who rarely opens his email has less chance of victimization in case of him. Nevertheless, the person who frequently uses his email for work becomes a suitable target for a motivated offender. That's why young aged people are victimized primarily in Bangladesh because of their online activities.

Recently, the email server of Biman Bangladesh was attacked by some hackers who took control of the server. The hackers demanded 5 million USD from Biman Bangladesh.[58] They claimed

[57] Behzat Yucedal (n 6)
[58] Zyma Islam and Rashidul Hasan, 'Hackers Want $5M for Biman Data' *The Daily Star* (24 March 2023) <https://www.thedailystar.net/news/bangladesh/news/hackers-want-5m-biman-data-3279041> accessed 04 June 2023

they had access to information about the passengers, passports of staff, and essential documents of Biman Bangladesh. The IT specialist discovered that the malware they used to attack the email server of Biman Bangladesh was a 'Zero-Day Attack'. Sometimes the developer is unaware of the flaws or vulnerabilities of a server. The hackers utilize the server's flaws, then attack it and take control. It is the primary idea of the Zero-Day Attack. In Biman Bangladesh, the same incident happened. Biman Bangladesh was unaware of the flaws in their server. That is why they faced this attack. From the theoretical perspective, here, flaws in the server mean the absence of a capable guardian. These flaws in their server motivated the cyber offender to commit the crime. If Biman Bangladesh inspects the vulnerability of its email server on day to day basis, then it might protect itself from the attack.

Most of the hacking in Bangladesh occurred due to the website's vulnerability. The security & privacy of the websites is not well developed most of the time. In Chattrogram, some hackers took control of the birth registration server & issued almost 84 birth certificates unlawfully.[59] In this incident, the password was compromised. There was no two-factor authentication system enabled on their server. Because of that, it becomes easier for the hacker to take control of the account. According to routine activity theory, two-factor authentication works as a digital guardian because it ensures an extra layer of security that helps protect a user's account.

In Madaripur, Police arrested three hackers who hacked almost 2000 Facebook accounts using phishing links.[60] They trick people and manipulate them into clicking the fishing links. When the victims click the links, the account information is transferred to them. They collect personal photographs from the account and demand considerable money in exchange for this. Most of the victims in this incident do not use two-factor authentication or other anti-fishing app or software. By the phishing method, hackers mainly get the password of the account.

[59] '84 birth certificates compromised in registration account hacking' *Daily ProthomAalo* (Chattogram 22 January 2023) <https://en.prothomalo.com/bangladesh/local-news/irmsr23gi9> accessed 04 June 2023

[60] Mohammad Jamil Khan, 'Careful what you click' *The Daily Star* (03 October 2021) <https://www.thedailystar.net/news/bangladesh/crime-justice/news/careful-what-you-click-2189321> accessed 04 June 2023

Nevertheless, if two-factor authentication is enabled in an account, the hackers cannot access the account easily though he knows the password. Apart from this, anti-fishing software blocks the fishing links. So, if they take these security measures, they can protect themselves from this cybercrime. From the perspective of routine activity theory, here lack of security in the account motivates the cyber offender and helps them to choose the potential victim. If the victims utilized features like two-factor authentication & anti-fishing software, then this could work as a digital guardian in cyberspace, which protects the online user from cybercrime.

Interestingly, the hackers in the Madaripur incident led to a very regular life in physical space. The police arrested three hackers: Obaidur Rahman, a seller of women's purses; Sajib Hossain, a tailor & Shamim Sharder, an electrician. In the physical space, their life was ordinary and they were not involved in criminal activities. However, in cyberspace, they were leading a criminal life where they hacked people's accounts and continuously blackmailed the victims by demanding money in exchange for their personal information & photos. According to space transition theory, individuals restrain themselves from committing crimes in the physical world because of social norms & their dignity but cyberspace ensures anonymity. That is why they commit an offence in cyberspace because no one can identify them quickly in cyberspace.

In 2021, Zahid Bin Aziz, a former tech company employee, committed online fraud by creating Facebook Page by pretending to be the chief whip, Noor-E-Alam Chowdhury. He lured his targets by promising them govt. jobs & other benefits. When people see that the Facebook Page has many likes, they easily trust it and become victimized by online fraud. According to routine activity theory, Zahid Bin Aziz is the motivated offender & the people who believe in fake Facebook Pages are the victims. In this case, the concept of guardianship is challenging to explain. Most of the time, victims of online fraud make financial transactions with the offender. Financial institutions and other organizations can act as capable guardians by providing fraud detection & preventive measures such as educating customers about fraud risk, and promptly responding to fraudulent activities.[61]

[61] Nurul Amin, 'Pandemic prompts cyber-crime epidemic' *The Business Standard* (21 February 2022) <https://www.tbsnews.net/bangladesh/crime/pandemic-prompts-cyber-crime-epidemic-205075> accessed 04 June 2023

Furthermore, Zahid Bin Aziz was a former employee in a tech company and was not involved in criminal activities in the physical world. Nevertheless, he started committing online fraud using his technical skills in cyberspace. This study agrees with the point of view of K. Jaishankar that space transition does not mean an individual has a criminal mind from childhood, instead, it provides the idea that an individual's criminal mind becomes expressed when he moves from physical space to cyberspace.[62] In Zahid Bin Aziz's situation, the proposition of space transition theory is applicable. A motivated offender became a dangerous criminal when he shifted to cyberspace, but while he committed the crime in cyberspace, he maintained a good profile in the physical world.[63] In Jheniadah, police arrested two people, including a housewife, for cheating people online. Online fraud is the most popular cybercrime In Bangladesh.[64] Many people are victimized by online fraud because of their lack of knowledge about cyberspace. Cybercriminals in Bangladesh follow the online activities of potential victims and then target the potential victim based on his/her choices and area of interest.

People in Bangladesh use instant messaging apps like IMO, WhatsApp, Viber, Line, and Telegram to communicate with relatives & friends. However, the security system of most instant messaging apps is not well developed. By using some essential hacking tools, hackers can take control of apps that are not well-developed. In many instant messaging apps, there is no option for two-factor authentication, and one can easily send phishing links to others because there is no built-in feature to block phishing links in these apps. For this reason, many people are victimized every day in Bangladesh. This lack of security of these apps can be identified as an absence of capable guardians under routine activity theory.

NATIONAL LEGISLATION OF CYBERCRIME

The laws related to cybercrime in Bangladesh are the Information and Communication Technology Act of 2006, Digital Security Act 2018, Digital Security Rules 2020, The Bangladesh

[62] K. Jaishankar (n 20)
[63] *Ibid*
[64] 'Jhenaidah police nabs 2 on cybercrime charge' *Bangladesh Post* (15 September 2022) <https://bangladeshpost.net/posts/jhenaidah-police-nabs-2-on-cybercrime-charge-94727> accessed 04 June 2023

Telecommunication Act 2001 & The Pornography Control Act 2012. Previously Information and Communication Technology Act 2006 dealt with unauthorized access to the government computer system, hacking & other common cyber offences. But after the enactment of the digital security act. 2018, many provisions related to cybercrime have been repealed. Recently, the Digital Security Act 2018 deals with cybercrime such as illegal access to computers, digital devices & computer systems in Bangladesh.

Digital Security Act 2018 mainly discusses the punishment for most common cyber offences. Nevertheless, as the pattern of cybercrime is changing, now it is required to enact new laws related to the pattern of cybercrime because as per this study, cybercrime victims also participate in a crime. Cyber offenders spread the traps in cyberspace in various forms. When a user browses any illegals, there is a high chance of victimization. In these scenarios, The Digital Security Act 2018 only focuses on the false & threatening information on a website.[65]

Nevertheless, the discussion about fake files on websites is silent. Many websites in Bangladesh contain pirated movies, video games, and software from foreign countries. Most of the time, it is difficult to frame a charge against cybercrime because of the limitations in the existing legislation. Previously, it was challenging to submit & prove digital evidence in Bangladesh because of a lack of provisions. However, because of the recent amendment of the Evidence Act 1872, digital evidence is now admissible in Bangladesh's court.[66]

However, some limitations still exist because it is challenging to gather digital evidence. It is easy to destroy digital evidence. Nazrul Islam, Special Public Prosecutor (PP), said in Prothom Alo that most cybercrime cases are dismissed because the evidence can easily be removable online.[67] However, the digital evidence in social media accounts, Facebook posts, or email accounts is sometimes hard to recover because when the offender deletes the accounts or posts, there is very little chance of recovering those evidence. Nevertheless, evidence that exists in

[65] Digital Security Act 2018
[66] Evidence (Amendment) Act 2022
[67] Asaduzzaman, 'Cybercrime: 97 per cent cases dismissed' *The Daily ProthomAlo* (Dhaka, 22 September 2021) <https://en.prothomalo.com/bangladesh/crime-and-law/cyber-crime-97-per-cent-cases-dismissed> accessed 16 June 2023

computers, mobile phones, digital cameras, hard drives, USB memory sticks, cloud computers, and servers is easier to collect.

The primary laws dealing with cybercrime are Bangladesh Digital Security Act 2018, Information & Communication Technology Act 2006[68] and the Pornography control act 2012[69]. All of these discuss Security. However, Security & privacy are two different things. No law exists in Bangladesh regarding the data privacy of individuals. However, there is a proposed Data Protection Act and the purpose of this act is to protect individual data. Nevertheless, the exciting fact is that this act does not define personal data. Further Clarification is necessary regarding this term.

Apart from this, the purposes of the Digital Security Act 2018 & Draft Data Protection Act-2022 are different. The primary purpose of the Draft Data Protection Act 2022 is to preserve the data and ensure the privacy of the data. On the other hand, the primary purpose of the digital security Act is to remove the data that causes a threat to Security. Apart from this, no criteria are mentioned for the technical skills of the investigation officer in this act which is also essential to include. From the discussion of cybercrime patterns, this study finds that many people are victimized by ransomware attacks & Malware. Nevertheless, the existing cyber laws in Bangladesh contain no provisions related to this. The law only focuses on the punishment of some major cybercrimes. Still, the pattern of cybercrime is changing & the user is continuously victimized because of their lack of knowledge. There are no proper guidelines available from the government related to internet behaviour.

REGIONAL APPROACH TO REGULATE CYBERCRIME

The existing cyber laws in India recognize various unique types of cybercrime. Those are Child pornography or sexually abusive material (CSAM), Cyberbullying, Cyberstalking, Cyber

[68] Information & Communication Technology Act 2006
[69] Pornography Control Act 2012

Grooming, Online job fraud, Online sextortion, Phishing, Vishing, Smishing, Credit card fraud or debit card fraud & Impersonation and identity theft.[70]

Cyber Grooming means when a stranger builds a relationship with a teenager to lure him into a sexual act. The rate of internet use among teenagers is increasing daily and because of that, offenders in cyberspace are continuously targeting them. Apart from this, 'Vishing' means tricking a person by voice call. Sometimes offenders call the victim and convince the victim to reveal their information. Smishing is identical to phishing. Nevertheless, the difference in smishing is that the offender sends text messages to the victim and convinces him to download the malware or share his data.

While addressing these unique cybercrimes, India also enacted some rules & regulations to deal with cybercrime. Most cybercriminals use cybercafes or public computer networks to commit cybercrime because their identity will be untraceable. In India, all cyber café must be registered with the appropriate authority, and they must record their user identities & internet uses as per The Information Technology (Guidelines for Cyber Cafe) Rules, 2011. Furthermore, a dedicated cyber help desk in India is available 24/7 to help cyber victims. Additionally, cyber victims can report cybercrime incidents through the helpline within 24 hours as per Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules). This emergency response team will immediately take action against the offender and try to trace the footprint of the offender by using high-tech equipment.

This type of emergency response team is essential because, as everyone knows, electronic evidence is easily destroyable. So, if the concerned authority does not take immediate action, there is very little chance of recovering cybercrime evidence. In Pakistan, the existing laws related to cybercrime are the Electronic Transaction Ordinance, 2002, Payment Systems and Electronic Fund Transfers Act 2007, Prevention of Electronic Crimes Ordinance Pakistan 2007 and 2008 & Prevention of Electronic Crimes Act 2016. The Prevention of electronic crimes act is

[70] Nikunj Arora, 'Cybercrime laws in India' (*iPleaders*, 28 April 2022) <https://blog.ipleaders.in/cyber-crime-laws-in-india/> accessed 07 June 2023

the latest law related to cybercrime in Pakistan. This Act addresses the offences such as unauthorized access & Transmission. This Act also elaborately discusses the investigation process of cybercrime. Investigation under this act involves seizing, saving & retaining information and collecting or recording real-time data by warrant or court orders. However, this act also focuses on the security of online users.[71]

In Srilanka, existing cyber laws are Information & Communication Technology Act, 2003 and Payment & Settlement Act 2005, Electronic Transactions Act 2006, Payment Devices Frauds Act 2006 & Computer Crimes Act 2007. The Computer Crimes Act 2007 addresses hacking-related offences and tries to cover crimes committed using the computer. Interestingly, in 2015 as a South Asian Country, Srilanka first ratified the Budapest Convention.[72]

Furthermore, the Electronic Transaction Act 2006 was enacted by following the standards set by Model Law on Electronic Signatures (2001) & United Nations Commission on International Trade Law Model Law on Electronic Commerce (1996). The primary purpose of this act is to promote national & international electronic commerce by removing legal barriers. This act also tries to encourage people to use reliable electronic commerce. Apart from this, another time-befitting act in Srilanka is the Payment Devices Frauds Act. This Act's primary purpose is to prevent using unauthorized payment devices. This act also has strict regulations regarding counterfeit payment devices.

In the Philippines, The existing legislation regarding cybercrime is the Cybercrime Prevention Act of 2012. Like other cybercrime laws, this act also discusses the crimes against computers and crimes by using computers. This Act was also enacted by following the standards set by European Convention 2001. This act addresses the crimes such as Cybersex, Cyberstalking, Hacking and Child-Pornography. It also covers the regulations related to online business as well. However, the unique feature of this act is to address the term 'Cybersquatting'.

---

[71] 'Pakistan: Repeal amendment to draconian cyber law' *Amnesty International* (28 February 2022) <https://www.amnesty.org/en/latest/news/2022/02/pakistan-repeal-draconian-cyber-crime-law/> accessed 07 June 2023

[72] Ravindu Yasas, 'Laws In Sri Lanka to Prevent Cyber Attacks' (2020) SSRN <http://dx.doi.org/10.2139/ssrn.3690552> accessed 07 June 2023

Cybersquatting means unauthorized domain registration similar to trademarks, service marks, and company names.[73] It is now one of the common problems in Bangladesh too. Many people in bad faith buy the domain name identical to other trademarks. This type of activity creates confusion among the customers & sometimes people use these types of domains to trick people into fraud.

FINDINGS

This research studies the pattern of cybercrime in Bangladesh from the perspective of routine activities & space transition theory. This study uses the data from the field survey & reported incidents to discuss the pattern of cybercrime in Bangladesh. The findings of this study are discussed as follows:

Routine Activity theory tries to explain how a crime occurs. According to the routine activity theory, three elements are required in a crime. Those are a motivated offender, a suitable victim & absence of a capable guardian. Scholars define the guardian into two parts, which are physical guardian & digital guardian. Physical guardian refers to any person or object which demotivates the offender from committing any crime. For example, Parents are physical guardians,and Friends are also considered physical guardians. The concept of guardianship slightly differs from the legal meaning of guardians under this theory. An object can work as a guardian as per this theory. For example, A door lock, CC camera & Police Van. These objects demotivate a person from committing any offence. That is why these are considered guardians.

However, in cyberspace security systems & security software, two-factor authentication & strong passwords are considered digital guardians. This study finds that many people in Bangladesh many people are not aware of two-factor authentication & they use weak passwords, which makes their social media accounts vulnerable. When the offenders target these accounts, they can quickly access them because of the lack of security in the account. The absence of two-factor authentication can be defined as the absence of a capable guardian in

[73] Sanjay Kumar, 'All you need to know about the Cybercrime Prevention Act in the Philippines' (*iPleaders*, 17 October 2021) <https://blog.ipleaders.in/all-you-need-to-know-about-the-cybercrime-prevention-act-in-the-philippines/> accessed 07 June 2023

cyberspace. And the absence of a capable guardian generally motivates an offender to choose a suitable victim.

This study also finds that most of the people in Bangladesh download software from unknown sites. The main reason is that most of the original software price is too high. In a country like Bangladesh, it is challenging to afford original software for most people. That is why people download cracked software. The security system of this cracked software is vulnerable; most of the time, this software contains malicious codes. When someone installs the cracked software on the computer, there is a high chance that all the files will be encrypted. A decryption key is required to access the files, and in exchange for the decryption key, the cyber offenders demand an enormous amount of money. When people install this cracked software, they usually turn off Window's built-in defence system because Windows defence systems do not allow software installation from unknown developers. When people turn off their windows defending system, this can be defined as the absence of a capable guardian per routine activity theory.

One of the significant findings of this study is that cybercrime is unique to conventional crime because in cybercrime, a victim also willingly participates in the crime. For example, cybercriminals do not force anyone to download malicious attachments or cracked software on their device. Instead, most of the time, when an internet user feels the necessity of software or movies or video games, he starts looking for the free or cracked version because of the high price of the original software, movies & video games. So, here the victim is participating in the crime & also becomes victimized by cybercrime. As per this study, cyberspace is a high crime rate area where the potential victim & motivated offender live together.

People know that downloading software from pirated sites is not legal, but still, they do it because they believe no one will be able to track them or know about it. This study survey finds that many educated & law-abiding citizens are involved in this type of activity. As per the space transition theory, individuals act differently when they shift from physical space to cyberspace. Furthermore, this study discusses a few cybercrime incidents in Bangladesh and finds that most cybercriminals live a regular life in the physical world. Most of them have no previous criminal records. This study connects the situation by analyzing it through space transition theory and

finds that because of social status and norms, individuals restrain themselves from committing crimes in the physical world. However, because of the anonymous nature of cyberspace, they become motivated to commit offences in cyberspace.

This study finds that in cybercrime, people cannot identify how they become the victim of cybercrime. Many people are unaware of the dangerous risk of downloading & installing software and video games from unknown websites. People become victimized by browsing unknown & illegal websites. They also do not maintain sufficient security measures in their social media accounts. That's why, it is necessary to educate people about the pattern of cybercrime. If they understand how cybercrime occurs, this process will help minimize cyber victimization.

The existing cyber laws in Bangladesh address the most common types of cybercrime, such as unauthorized access, defamation, data theft & identity theft. The nature of cybercrime is changing, and many more crimes are increasing in Bangladesh, such as Cyber Grooming, Malware Attacks, Denial of Service Attacks and Ransomware Attacks. A proper definition is not available for the term ransomware attack, Denial of Service Attack, Sexting, cyber grooming & Phishing. From the pattern of cybercrime, this study finds that people are not aware of safe browsing of the Internet. The existing laws in Bangladesh only focus on punishments for cybercriminals. However, there is a lack of provisions regulating people's online lifestyle, such as demotivating the user from visiting unknown & pirated sites. Furthermore, this study also finds that people become victimized in cyberspace because they lack knowledge about it. Cybercrime is different from conventional crime. Most of the time, people do not know how they become victimized online. There are no proper guidelines available regarding safe internet browsing. The government takes many initiatives to make people aware of cybercrime. Nevertheless, those also lack clarity regarding the pattern of cybercrime in Bangladesh.

RECOMMENDATIONS

1. It is recommended that people need to be aware of cyberspace security measures. The awareness campaign needs to start at the school level. In the ICT book, the pattern of cybercrime needs to be included.

2. Many people in Bangladesh download software, video games, movies & tv series from pirated websites. The files available on pirated websites contain malicious viruses. People become victimized by malware and ransomware attacks by downloading files from these websites. The government needs to regulate these sites. The government also needs to ban torrents and other pirated websites.

3. People also need to be careful about their online behaviour. They need to be careful before clicking any links online. Sometimes offenders create identical website names to trick people. For example, Azamon.com, apax.com, and rkomoari.com. When people unintentionally browse this website, they make the task easier for the cyber offender. So, victims also unintentionally participate in the crime. Proper awareness of this issue is required. People need to double-check the website name before browsing something.

4. Bangladesh needs to monitor the cyber activities of internet users. To some reasonable extent, cyber-monitoring is required in Bangladesh.

5. The government must collaborate with different NGOs and run more awareness campaigns. The awareness campaign should start by questioning 'How'. If people understand how cybercrime occurs, then they will be able to know which types of online activity they should refrain from doing.

6. The laws in Bangladesh need to clarify some major cybercrime concepts. The existing cyber laws in Bangladesh very broadly explain everything. Nevertheless, each cybercrime has some unique pattern. The laws only focus on punishments for certain cybercrimes, but people do not understand cybercrime properly. Proper clarification is required in different terms of cybercrime for general people & the laws need to be reformed.

4. It is further recommended that Bangladesh can follow India's policies to deal with cybercrimes. Bangladesh must build a quick emergency response team with enough technical skills to deal with cybercrimes. Most of the time, cybercriminals destroy the evidence & footprints before the police start the investigation. In cybercrime, emergency response is essential to recover the evidence. Many people in Bangladesh are also victimized by online fraud. Internet user & online marketplace is increasing in Bangladesh rapidly. Proper regulation of the online marketplace is essential for Bangladesh. Each online business must show its registration number on its Facebook page or website. In this way, people can verify the business page. Furthermore, Proper awareness is essential regarding the pattern of cybercrime to minimize cyber victimization.

CONCLUSION

Cybercrime is different from conventional crime. This study discusses the concepts of routine activities & space transition theory to understand the pattern of cybercrime in Bangladesh. According to the routine activity theory, many people are victimized in cyberspace in Bangladesh for lack of capable digital guardians. Lack of security measures motivated the cyber offender to commit to cyberspace. Individuals become suitable victims because of the lack of digital guardians. It is the typical pattern of cybercrime in Bangladesh according to routine activity theory. However, according to space transition theory, individuals act differently when they move from physical space to cyberspace. This theory explains the pattern of cybercrime from both victim's & offender's perspectives. Internet users download movies, software & video games from pirated sites, indicating the opposite behaviour of physical space.

Apart from that, because of cyberspace's anonymous nature, an offender becomes motivated to commit an offence in cyberspace. Individuals who lead a very regular life in real life utilize the anonymous nature of cyberspace & motivated to commit an offence in cyberspace. The government cannot prevent cybercrime alone because of the unique nature of cybercrime. Cooperation from the general people is required to minimize cyber victimization risk. It is essential to educate people about internet browsing. Because people are not aware of the cybercrime threat appropriately, they visit illegal sites and download apps and software from

unauthorized & pirated sites, which make them a potential victim of cybercrime. An awareness campaign and strict government regulation are necessary to overcome this situation.

Apart from this, Cooperation among the countries is also essential. Cybercriminals can operate crimes from anywhere in the world. If countries do not want to cooperate, it will be challenging to capture a cyber-criminal. So, it is suggested that enough Cooperation, collaboration & awareness can help reduce cyber victimization.