Causes of Cybercrime Victimization: A Systematic Literature Review

Abu Taher Muhammad Abdullah1, Israt Jahan2

1MA Criminology, School of Sociology and Social Policy, University of Nottingham, UK.
2MA Digital Media, School of Computing and Digital Media, London Metropolitan University, UK.

Corresponding Author: Abu Taher Muhammad Abdullah

ABSTRACT

A systematic literature review on causes of cybercrime victimization has been done for this study to explore the severity of cybercrime. While 111 articles from Scopus and ASSIA databases were thematically analyzed to find trajectories of factors of cybercrime. Cyberbullying are prevalent among various forms of cybercrime. It is evident that adolescents are most targeted victims of cybercrime. It observed attitude, low self control, psychopathic behaviors, bystander behavior, social inequality, more use of cell phone and Internet, and school delinquency as the main causes of cyberbullying. Particularly, older member of the society is responsible for online fraud. The causes of online fraud found vulnerability, greed, trust, naiveté, strong emotions, access to internet from home, lack of awareness, and chronic underreporting of cybercrime. In addition, software piracy, online harassment and computer hacking as cyber deviance caused due to availability of personal information in Social Networking Sites (SNS), socioeconomic, psychosocial, and geopolitical aspects, pornography, sexual promiscuity, minor daily stressors, living without parents and less active offline social life. Crypto market is a new form of cybercrime where criminals maintain a website to keep them anonymous for drugs dealing. Breakup of relationship and coercion to woman by male counterparts are the causal factors of cyber stalking and sexting respectively. However, follow up strategy, warning, sanction and educational programs were identified as prevention initiatives. Hence, this study is not beyond the limitation of empirical observations which will be the future research initiative to construct reporting mechanism of cybercrime.

Keywords: Cybercrime, Cyberbullying, victimization, fraud, deviance, online, victims

INTRODUCTION

Nowadays Internet is becoming part and parcel of a modern lifestyle of the people throughout the world. Whereas, online criminality have also been risen with the developments in Internet activities. At present, the risk of cybercrime can visualize in the form of offences analogous to the physical world, such as cyberbullying and online harassment which are termed as cyber-enabled crimes, or through security risks that affect the computer itself, such as malware infections, ransomware infections, and theft and misuse of personal data which is called cyber-dependent crimes. [1] With the development of information technologies and the expansion of the internet cybercrime is becoming an increasingly technologically advanced, aggressive and one of the fastest-growing types of crime. [2] Hence, abuse of computer and Internet put together some people to commit crime and victimize others. [3]

Cyberspace users have excessive confidence to use cyberspace which lead them to be exposed to risks in cyberspace. However, their perception is that the likelihood of their victimization is lower than other potential victims from the traditional crimes in the real world. Moreover, ‘knowledge on crime patterns, their commission and victims’ responses are crucial for developing prevention strategies.
and user awareness-raising programmes’. As ‘formal social cybercrime control is much worse than offline crime control’, which indicated the need for more studies on the causes of cybercrime victimization, to fight growing threats from cyberspace. This research explicitly examines causes of cybercrime victimization through detailed analysis of existing etiological literature with a systematic literature review process to have insights on routine activity theory.

LITERATURE REVIEW
Cybercrime and Cyber-Victimization
Cybercrime is the “destruction, theft, or unauthorized or illegal use, modification or copy of information, programs, services, equipment or communication network”. According to Council of Europe “any criminal offence committed against or with the help of a computer network is identified as cyber crime”. Computer or computation related device is an essential for cyber crime perpetration and victimization. No country is immune as cyber crime is a worldwide problem. ‘Computer crime or cyber crime is a form of crime where the Internet or computers are used as a medium to commit crime’. Specifically, cybercrime is the commission of a crime utilizing of technology, including computers, smartphones, or tablets. To this end, ‘this form of criminality has been extremely costly to the economy, with estimates of $575 billion lost annually worldwide’.

However, cybercrime takes place in a different context than traditional crimes, ‘which may lead to different risk factors for both offending and victimization’. While traditional offending and victimization require physical interaction between victims and offenders, on the other hand, in cybercrime ‘there is no physical convergence in space and time of offenders and victims’. In other word, opportunities for cybercrime and victimization are widespread like Internet in terms of access, time zones and nations, and the integration in daily activities. For instance, people who spend more time online and make more online purchases are more likely to be victimized by internet fraud. Likewise, other kinds of cybercrime victimization such as cyber-stalking, cyber-harassment, hacking, or malware infection, empirical studies have also found online exposure to risks cybercrime victimizations. Conversely, ‘Ngo and Paternoster found no evidence that online exposure had significant effects on cybercrime victimizations’.

‘Online sexuality’ like ‘pornography, sex shops, sex work, sex education, sex contacts, and sexual subcultures’ which engaged large volume of Western people irrespective of age, gender and sex. While Doring argues internet sexuality should not be considered as “virtual pseudo-sexuality” in comparison to “real sex” as 'online dating' services is successful mechanism to meet the sexual partner in the real world. On the other hand, online sexuality has either positive or negative consequences in the individual life who engaged in the online sexuality as 'sexual satisfaction' in some instances, sexually transmitted diseases, sexual disorders and sexual victimization. Hence, it has impacts on sexual attitude and identities. Whereas Cooper et al. argues two motivation works for cybersex—one recreational for sexual felicitation or relax and the other, problematic person to reduce stress, emotional regulation or for fantasies.

Recidivism is directly related with the criminogenic needs of an offender’s life. While low self-control, anti-social personality, anti-social values, criminal peers, substance abuse and dysfunctional family are directly related to crime. The effects of victimization in cyberspace evolved underpinning on the characteristics of victim’s, incident, and post-victimization experience. In absence of knowledge and awareness regarding potential measures against cybercrime, the victims fail to come forward for remedy. It is important to know cyber behavior and victimization to understand the characteristics of victims, crime patterns and crime trends. However, few researches have been
conducted on the etiology of cybercrime which leads the current study to find the various cybercrimes with their causes and remedial measures.

**Theoretical framework**

This study reviewed causes of cybercrime which tends to set Routine Activity Theory (RAT) as a theoretical framework to explore the theoretical implications of this research. While regarding RAT Cohen and Felson\(^{[12]}\) argue 'criminal victimization' occurs when a probable 'offender' and 'suitable target' that is victim convergent in a 'specific material, historical times and spaces' where there is insufficient capable guardian to safe the victim or to retard the offender to commit offence.\(^{[13]}\) However, causes of cybercrime researches are very scarce which justify the present research is to examine causes of cybercrime through the lens of RAT.

**METHODS**

The present review conducted in accordance with 'PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses)' guidelines to ensure quality.\(^{[14]}\) An electronic literature search conducted depending on the Scopus and ASSIA (Applied Social Sciences Index and Abstracts) databases from 2014 to 2018 time scale. Terms in each search added sequentially in time in the following way\(^{[15]}:\)

- (cybercrime) OR (cyber and crime) OR (cyber-crime) AND (causes)
- (cybercrime) OR (cyber and crime) OR (cyber-crime) AND (severity)
- (cybercrime) OR (cyber and crime) OR (cyber-crime) AND (policing)
- (cybercrime) OR (cyber and crime) OR (cyber-crime) AND (criminal justice)

Based on some inclusion criteria were used to retrieved full articles.\(^{[16]}\) While the focus provided on the journals that illustrated causal factors of cybercrime. Then, the priority was given to severity of cybercrime, police responses, and challenges to cybercrime response. Next, criminal justice matters related articles were also documented. On the other hand, considering exclusion criteria, different traits were focused like the publications which were written other than English excluded for syntactical analysis.\(^{[17]}\) Next, other than peer-reviewed articles were excluded. Then, time frame strictly followed which was fixed from 2014 to 2018 for last five (5) years to exclude the articles. Finally, technical matters were repelled during the literature search. Therefore, the articles were analyzed and extracted results.

From 270 articles, 120 and 150 articles were found from Scopus and ASSIA databases respectively. While 14 articles had similarity, where 6 articles were similar amongst Scopus articles, 7 were in ASSIA articles and 1 article was between Scopus and ASSIA articles. In Scopus database, 40 articles and 7 articles were excluded for technical aspect and other reasons respectively. On the other hand, 46 articles were not related with cybercrime, 17 were bullying other than cybercrime, and 8 articles were excluded for ‘other reasons’ in case of ASSIA database. In literature search, other reasons mean the articles belonged on book review, editorial, and other crimes beyond cybercrime which were not relevant with this study. After first screening 137 articles were selected for full reading, and 119 articles were excluded. To this end, 111 articles were fixed for the analysis for this review and 26 articles were excluded.

A systematic literature review method followed for this study.\(^{[18]}\) As systematic literature review is the explicit 'accumulation, transparent analysis and reflective interpretation' of previous research findings and outcomes of 'a specific questions'.\(^{[19]}\) This research conducted based on the four criteria, such as search, appraisal, synthesis and analysis which comprised a mnemonic 'SALSA'.\(^{[20]}\) While 111 articles were searched based on Scopus and ASSIS databases to collect information on 'causes', 'severity', 'policing' and 'criminal justice' related with
cybercrime. After carefully reviewing sources, key analysis has been done through thematic analysis method to assess the causes to minimize the victimization of cybercrime. [21] For analysing articles thematically, six steps were followed like 'familiarising with documents' from the Scopus and ASSIA databases, 'data generating initial codes, searching for themes, reviewing themes, defining and naming themes and producing the report'. [22] Finally, report production has been done after reviewing of themes, defining, naming, and sub-themes creation (24) to initiate the write up of this study. [23] In this review, few findings were produced in tabular and graphs format to show the richness of the findings. Besides, some sorts of findings were discussed elaborately to have an in-depth understanding of the logics on causes of cybercrime.

RESULT

In this article, themes on causes of cybercrime victimization have been discussed to observe strategies of fighting against cybercrime. Adolescents showed pro-cyberbullying attitude which is an important cause of cyberbullying as shown in the Figure 4 below. [24] The reason for this attitude is that they take cyberbullying as a fun. For instance, posting someone a photo or video to another person which is embarrassing seems to sender as "banter" or "fun". [24] Both 'males and females lower self control' influence to participate in cyberbullying online through various means, for example, 'posting hurtful message or pictures to Facebook'. [25] The logic is that lower self-controlled person is impulsive and risky for sending nasty comments without thinking the ultimate result of their act. In addition, both sexes react similarly if they had bullied earlier, [25] which are also signified other findings that cyber-victimization is caused due to other forms of victimization and perpetration of crime. [26] Whether, these findings supported by van Geel et al. [27] as cyberbullying has an association of psychopathic behaviours of youth. Besides, bystander behaviour [26], social inequality [29], age, gender, father's age and family income [30], breakfast skipping [31], cell phone and Internet and school delinquency [34] are others causes of cyberbullying, which are found in the cyber world and indicates the severity of cybercrime. While cyberbullying effect found as affect of post-traumatic stress, paranoia, health and self-esteem, negatively impact on ICT satisfaction and longer recovery from stress, whereas countering mechanism found follow up strategy, sanction and educational programs, as shown in Figure 1.

Table 1 illustrates fraud which is a severe form of cybercrime found in online. Online fraud is particularly done by older member of the population of the society, where men usually lost more money than women due to online fraud. [35] In addition,
any person of age 5 to 75 years, either sex or any ethnic group could be target of online fraud. The cause of this offence identified human nature as ‘vulnerability, greed, trust and naivete’. Furthermore, victim running after smarter person and victim provide information, money and love own-self to online fraudster. [35] Ironically, strong emotions are used for online ‘Romance Scam’ to collect money from their partners by the fraudsters, for instance, scammers of this romance fraud are prevalent in Nigeria and Ghana who used personal love story to draw a relation and ultimate target to take money from their affectionate partners to victimize financially and emotionally. [36]

Other forms of online fraud is online property crime (OPC), which comprises cyber-vandalism that are computer viruses, service denial and other attacks and cyber-theft for profit gain, [37] cyber attack in the financial companies where consumer incur losses like insurance companies [38, 39] and financial cybercrimes targeted to the bank where money transferred by the hackers from the consumers account. [40] and digital piracy. [41] Subsequently, another online fraud is the predatory publishing and consumer fraud. [42] While this type of cybercrime constitute huge loss to the victims like identity theft, stealing personal information, credit card loss and embezzle money from the bank account. In other word, causes are identified as access to internet from home, lack of awareness, chronic underreporting, weak policing and international cooperation, jurisdictional arbitrage, and employee collusion of financial companies and bank to share information with the perpetrators and willingness to pay (WTP) impact digital piracy. [37-38,40-45]

In response to this cybercrime, identification of scam warning to the victims [36] and personnel risk assessment are identified as prevention initiatives. [43]

<table>
<thead>
<tr>
<th>Nature of online fraud</th>
<th>Mechanism</th>
<th>Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Older member of population</td>
<td>Strong emotions</td>
<td>-Identify scam and warning to victims</td>
</tr>
<tr>
<td>Online Romance Scam</td>
<td>-Users access to internet at home</td>
<td></td>
</tr>
<tr>
<td>Online property crime (OPC)</td>
<td>-Lack of awareness</td>
<td></td>
</tr>
<tr>
<td>Predatory publishing and consumer fraud</td>
<td>-Chronic underreporting</td>
<td></td>
</tr>
<tr>
<td>Financial companies</td>
<td>-Weak policing, weak international frameworks and jurisdictional arbitrage</td>
<td></td>
</tr>
<tr>
<td>Financial cybercrimes in banking sector</td>
<td>-Employee collusion</td>
<td></td>
</tr>
<tr>
<td>Digital piracy</td>
<td>-Intentions and willingness to pay (WTP)</td>
<td></td>
</tr>
</tbody>
</table>

The persons who are usually spent more time in the internet engaged with three ‘cyber deviance’ like 'software piracy, online harassment and computer hacking’ and shown low self control behavior, as shown in Figure 2. [46-48] Next factor of cybercrime victimization is the availability of personal information in Social Networking Sites (SNS), which has an impact on privacy and security of the victims. [49] Then, unauthorized ‘access to computer systems’ has influenced on ‘espionage and data theft’, malicious software and malware, and political freedom in a country has impacted in the malware infections in their routine activities. [50] Subsequently, lower social status; socioeconomic, psychosocial and geopolitical aspects; smoking, drinking and binge drinking; pornography; sexual promiscuity and hostile masculinity; minor daily stressors and immigrant status, urban residence, unemployment, living without parents and less active offline social life are other causes of cyber deviance. [51-57]

Therefore, cyber deviance and victimization caused to incur financial loss, anti-women sexual aggression, physical damage to industrial contamination, Internet Gaming Disorder (IGD) and psychological distress. [39, 50, 55, 58, 59]
Next form of cybercrime is crypto market, 'a type of website use encryption to protect the users' keeping anonymous. 'Silk Road', for example, is a website through which illicit drugs are traded to the consumer beyond the eyes of law enforcement agents and work like an alternative to the traditional illicit drug market. This crypto market consumes a large share of global trade. Greer et al.[61] supported that sex trafficker's use online for advertisement as well as alluring the victims. Turing to other forms of cybercrimes, it recognized cyber stalking, sexting, online child sexual abuse, and cyber hate, which are prevalent in the cyberspace. As causes of cyber stalking is breakup of relationship, sexting are lack of awareness of legal consequences, impressing and flirting with partner and peer pressure[64], coercion to woman by male counterparts in different way like 'persistent requests, anger, and threats' and treat sexting as 'a joke'.[32] Then, online child sexual abuse constituted with three elements like cyberspace, possession and extortion. Hence, cyber hate is another severe form of cybercrime which disseminate hateful and antagonistic content through World Wide Web. [67]

**DISCUSSION**

This research recognized that Routine Activity Theory (RAT) has an implication in finding the causal relation with cybercrimes like malware infections, and cyber-theft victimization. Holt and Bossler[68] supported RAT, however, opposite view persist that online environment in all cases not accessible. The identified causes of cyberbullying, cyber stalking, sexting and online child sexual abuse are attitude of adolescents, lower self control of both males and females, impulsive and risky traits of perpetrators, psychopathic behaviors of youth, social inequality, age, gender, father's age and family income, school delinquency, lack of safety warning websites, spend more time in the internet, less active offline social life, unauthorized access to computer, geopolitical aspects, unemployment, and available personal information in SNS like Facebook. [24] However, Slonje and Smith[70] supported that ‘the person carrying out cyberbullying may be less aware or even unaware of the consequences caused by his or her actions’.

In online fraud, older members of the society mostly involved and victim’s own-self aggravated the victimization by providing information to the fraudster,
where love and money acted as a catalyst. Furthermore, the availability of personal information in SNS; unauthorized access to computer systems; lower social status; socioeconomic, psychosocial and geopolitical aspects found as causal factor of computer-based deviance. In crypto market, illicit drugs are traded with the help of a website called 'Silk Road' to make safer communication between drug traders and consumers. Cyber hate is also a new trend of cybercrime to spread hateful comments in the internet. Hence, follow up strategy, warning, personnel risk assessment, sanction and educational programs identified as preventive mechanism for cybercrime.

**CONCLUSION**

Cybercrime is predominantly a crime based on cyberspace where any person may be victimized in any parts of the world. Mostly cyberbullying, online fraud, cyber deviance, crypto market, cyber stalking, sexting, online child sexual abuse, and cyber hate are the major heads of cybercrime. While the identified causes of cybercrime are pro-cyberbullying attitude, psychopathic behaviours, social inequality, more use of cell phone and Internet, strong emotions, greed, lack of awareness, weak policing and international cooperation, and availability of personal information. Whereas warning of cyber-victimization, personnel risk assessment, sanction and educational programs will be the appropriate remedial measures of cybercrime. These findings of causes, classes and remedial measures will contribute in the cybercrime scholarship. However, the current study is not beyond the limitation of empirical observations, what will be the future endeavour of finding reporting mechanism of cybercrime to law enforcement agent.

**Authors’ Contributions**

First author, Abu Taher Muhammad Abdullah has produced this research work for publication as a part of his dissertation. While second author, Israt Jahan has conceptually constructed this paper and edited the manuscript. Both the authors wrote this article and revised it.

**REFERENCES**


How to cite this article: Abdullah ATM, Jahan I. Causes of cybercrime victimization: a systematic literature review. *International Journal of Research and Review*. 2020; 7(5): 89-98.