International Journal of Research and Review
Vol.7; Issue: 5; May 2020
Website: www.ijrrjournal.com
Review Article *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Causes of Cybercrime Victimization: A Systematic Literature Review

Abu Taher Muhammad Abdullah[1], Israt Jahan[2]

[1]MA Criminology, School of Sociology and Social Policy, University of Nottingham, UK.
[2]MA 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'. [2] 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. [4] 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". [5] 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. [3] 'Computer crime or cyber crime is a form of crime where the Internet or computers are used as a medium to commit crime'. [6] 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'. [5]

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'. [7] 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.[8] Conversely, 'Ngo and Paternoster [9] 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. [10] While Doring [10] 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.* [11] 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. [6] 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. [2] 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 [28]; social inequality [29]; age, gender, father's age and family income [30]; breakfast skipping [31]; cell phone and Internet [32,33] 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**.

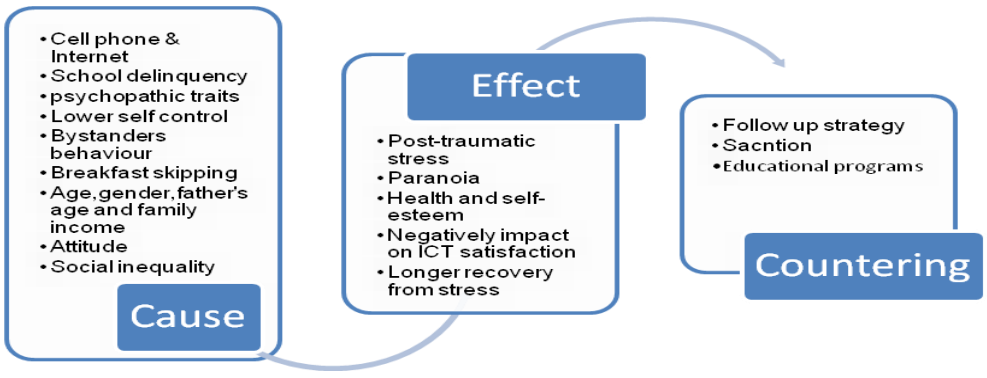

Figure 1: Cause & effect relationship with Cyberbullying and victimization

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 naiveté*'. 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 1: Nature of online fraud as a severe form of cybercrime

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

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]

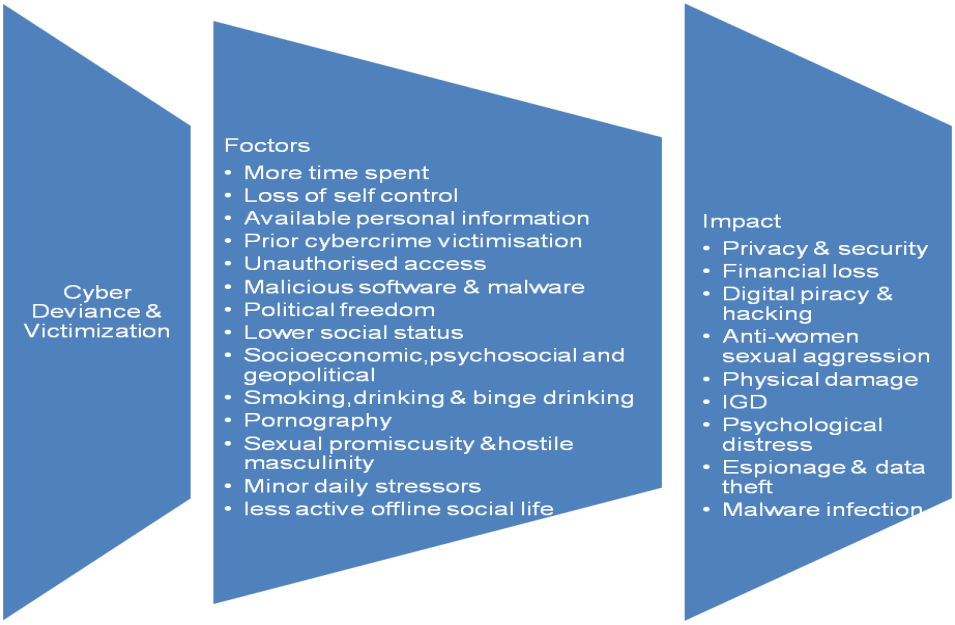

Figure 2: Process of various cybercrime deviance and victimization

Next form of cybercrime is *crypto market*, 'a type of website use encryption to protect the users' keeping anonymous. [60] '*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, [62] and *sexting* are lack of awareness of legal consequences, [32,63] impressing and flirting with partner and peer pressure [64]; coercion to woman by male counterparts in different way like 'persistent requests, anger, and threats' [65] and treat sexting as 'a joke'. [32] Then, *online child sexual abuse* constituted with three elements like cyberspace, possession and extortion. [66] 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, [50] and cyber-theft victimization. [45] Holt and Bossler [68] supported RAT, however, opposite view persist that online environment in all cases not accessible. [69] 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. [35] 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. [51] 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

1. Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? Cyberpsychology, Behavior, and Social Networking, 21(2), 84–90.
2. Meško, G. (2018). *On Some Aspects of Cybercrime and Cybervictimization. European Journal of Crime, Criminal Law and Criminal Justice, 26(3), 189–199.*
3. Kamruzzaman, M., Islam, M. A., Islam, M.S., Hossain, M. S. and Hakim, M.A. **(**2016). Plight of Youth Perception on Cyber Crime in South Asia American Journal of Information Science and Computer Engineering. Vol. 2, No. 4, pp. 22-28.
4. Ilievski, A. (2016). An Explanation Of The Cybercrime Victimisation: Self-Control And Lifestyle/Routine Activity Theory. Innovative Issues and Approaches in Social Sciences, Vol. 9, No. 1,pp.30-47.
5. Catherine D. Marcum and George E. Higgins Cybercrime in, Krohn, M. D., Hendrix, N., Penly Hall, G., & Lizotte, A. J. (Eds.). (2019). *Handbook on Crime and Deviance. Handbooks of Sociology and Social Research.*
6. Shabnam, N., Faruk, M. O. and Kamruzzaman, M. (2016). Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students. Social Sciences. Vol. 5, No. 1, pp. 1-6.
7. Kranenbarg, M. W., Holt, T. J. & van Gelder J.L. (2019).Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and TraditionalOffending-Only, Victimization-Only and the Victimization-Offending Overlap, Deviant Behavior,40:1, 40-55.
8. Song, H., Lynch, M.J. and Cochran, J.K. (2015). A Macro-Social Exploratory Analysis of the Rateof Interstate Cyber-Victimization. *American Journal of Criminal Justice*.1-20.
9. Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5,773–793

10. Doring N.M. (2009). 'The Internet's impact on sexuality: A critical review of 15 years of research'. *Computers in Human Behavior*. Vol. 25, Issue 5, pp.1089-1101.
11. Cooper, A.L., Delmonico, D.L., Griffin-Shelley, E., and Mathy, R.M. (2004). Online sexual activity: An examination of potentially problematic behaviors. *Sexual Addiction & Compulsivity*, 11, 129–143.
12. Cohen, L. E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.
13. Clough, J. (2015) *Principles of Cybercrime*. 2nd ed. Cambridge: Cambridge University Press.p.524.
14. Liberati, A., Altman, D.G., Tetzlaff, J., Mulrow, C., Gøtzsche, P.C., Ioannidis, J.P.A., Clarke,M., Devereaux, P. J., Kleijnen,J. and Moher, D. (2009) The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. PLoS Med 6(7): e1000100.
15. Ramirez, R., and Choucri, N. (2016). Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, 4, 2216-2243.
16. Klettke, B., Hallford, D.J. and Mellor, D.J. (2014) Sexting prevalence and correlates: A systematic literature review, *Clinical Psychology Review*, 34: 44–53
17. Lastdrager, E.E. (2014) Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science,* **3**:9.
18. Booth, A., Papaioannou, D. and Sutton, A. (2012) *Systematic Approaches to a Successful Literature Review*. London: Sage.p.279.
19. Rousseau, L.D.M., Manning, J., and Denyer, D. (2008) Evidence in management and organisational science: assembling the field's full weight of scientific knowledge through syntheses. *Academy of Management Annals*, 2:475-515.
20. Sidebottom, A., Thornton, A., Tompson, L., Belur, J., Tilley, N. and Bowers, K. (2017) 'A systematic review of tagging as a method to reduce theft in retail environments'. Sidebottom *et al. Crime Sci. (2017) 6:7*.
21. Castleberry, A. and Nolen, A.(2018) Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*, pp.1-9.
22. Lawless, B. and Chen, Y.W. (2018) Developing a Method of Critical Thematic Analysis for Qualitative Communication Inquiry, *Howard Journal of Communications*, Vol.0,No,0,pp.1-15.
23. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 77–101.
24. Munnelly, A., Farrell, L., Martin O'Connor, & McHugh, L. (2018). Adolescents' implicit and explicit attitudes toward cyberbullying: An exploratory study using the implicit relational assessment procedure (IRAP) and self-report measures. *The Psychological Record, 68*(1), 1-10.
25. Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2014). Exploration of the cyberbullying Victim/Offender overlap by sex. *American Journal of Criminal Justice, 39*(3), 538-548.
26. Beran, T., Mishna, F., McInroy, L. B., & Shariff, S. (2015). Children's experiences of cyberbullying: A Canadian national study. *Children & Schools, 37*(4), 207.
27. van Geel, M., Toprak, F., Goemans, A., Zwaanswijk, W., & Vedder, P. (2017). Are youth psychopathic traits related to bullying? Meta-analyses on callous-unemotional traits, narcissism, and impulsivity. *Child Psychiatry and Human Development, 48*(5), 768-777.
28. Bastiaensens, S., Vandebosch, H., Poels, K., Van Cleemput, K., Desmet, A., & De Bourdeaudhuij, I. (2014). Cyberbullying on social network sites. an experimental study into bystanders' behavioural intentions to help the victim or reinforce the bully. *Computers in Human Behavior, 31*(1), 259-271.
29. Görzig, A., Milosevic, T., & Staksrud, E. (2017). Cyberbullying victimization in context: The role of social inequalities in countries and regions. *Journal of Cross - Cultural Psychology, 48*(8), 1198-1215.
30. Beyazit, U., Şimşek, Ş., & Ayhan, A. B. (2017). An Examination Of The Predictive Factors Of Cyberbullying In Adolescents. *Social Behavior and Personality, 45*(9), 1511-1522.
31. Sampasa-Kanyinga, H., & Willmore, J. (2015). Relationships between bullying victimization psychological distress and

breakfast skipping among boys and girls. *Appetite, 89*, 41-46.
32. Korenis, P., & Billick, S. B. (2014). Forensic implications: Adolescent sexting and cyberbullying. *Psychiatric Quarterly, 85*(1), 97-101.
33. Holt, T. J., Fitzgerald, S., Bossler, A. M., Chee, G., & Ng, E. (2016). Assessing the risk factors of cyber and mobile phone bullying victimization in a nationally representative sample of Singapore youth. *International Journal of Offender Therapy and Comparative Criminology, 60*(5), 598.
34. Barboza, G. E. (2015). The association between school exclusion, delinquency and subtypes of cyber- and F2F-victimizations: Identifying and predicting risk profiles and subtypes using latent class analysis. *Child Abuse & Neglect, 39*, 109.
35. Bolimos, I. A. & Choo, K. R. (2017). Online fraud offending within an Australian jurisdiction. *Journal of Financial Crime, 24*(2), 277-308.
36. Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2016). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology, 9*(2), 205-216.
37. Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave?*Justice Quarterly, 33*(5), 890-911.
38. Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers and Security, 45*, 58-74.
39. Lathrop, A. J., & Stanisz, J. M. (2016). Hackers are after more than just data: Will your company's property policies respond when cyber attacks cause physical damage and shut down operations? *Environmental Claims Journal, 28*(4), 286-303.
40. Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? an assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*(3), 287-300.
41. Jackman, M. & Lorde, T. (2014). Why buy when we can pirate? The role of intentions and willingness to pay in predicting piracy behavior. *International Journal of Social Economics, 41*(9), 801-819.
42. Umlauf, M. G., & Mochizuki, Y. (2018). Predatory publishing and cybercrime targeting academics. *International Journal of Nursing Practice, 24*.
43. Cunningham, M. R., Jones, J. W., & Dreschler, B. W. (2018). Personnel risk management assessment for newly emerging forms of employee crimes. *International Journal of Selection and Assessment, 26*(1), 5-16.
44. Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues: In cybercrimes, cybercriminals and their policing, in crime, law and social change. *Crime, Law and Social Change, 67*(1), 3-20.
45. Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice, 41*(3), 583-601.
46. Lee, B. H. (2018). Explaining cyber deviance among school-aged youth. *Child Indicators Research, 11*(2), 563-584.
47. Li, H., Luo, X. R., Zhang, J., & Sarathy, R. (2018). Self-control, organizational context, and rational choice in internet abuses at work. *Information and Management, 55*(3), 358-367.
48. Donner, C. M. (2016). The gender gap and cybercrime: An examination of college students' online offending. *Victims & Offenders, 11*(4), 556.
49. Martinez, F. R. C., Candelaria, A. D. H., Lozano, M. A. R., Zúñiga, A. R. R., Peláez, R. M., & Michel, J. R. P. (2017). After click the submit button, control over personal information and privacy is lost: A case study in Mexico. *RISTI - Revista Iberica De Sistemas e Tecnologias De Informacao,* (21), 115-128.
50. Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology, 62*(6), 1720-1741.
51. Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology, and Law: An Interdisciplinary Journal of the Australian and New Zealand Association of Psychiatry, Psychology and Law, 24*(3), 323-338.

52. Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47*, 44.
53. Chan, S. F. & La Greca, A.M. (2016). Cyber victimization and aggression: Are they linked with adolescent smoking and drinking? *Child & Youth Care Forum, 45*(1), 47-63.
54. Montgomery-Graham, S., Kohut, T., Fisher, W., & Campbell, L. (2015). How the popular media rushes to judgment about pornography and relationships while research lags behind. *The Canadian Journal of Human Sexuality, 24*(3), 243-256.
55. Baer, J. L., Kohut, T. & Fisher, W. A. (2015). Is pornography use associated with anti-woman sexual aggression? re-examining the confluence model with third variable considerations. *The Canadian Journal of Human Sexuality, 24*(2), 160-173.
56. Wright, M. F. (2015). Cyber victimization and perceived stress: Linkages to late adolescents' cyber aggression and psychological functioning. *Youth and Society, 47*(6):789.
57. Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology & Crime Prevention, 16*(2), 203.
58. Wichstrøm, L., Stenseng, F., Belsky, J., Tilmann, v. S., & Beate, W. H. (2018). Symptoms of internet gaming disorder in youth: Predictors and comorbidity. *Journal of Abnormal Child Psychology*, , 1-13.
59. Hsieh, Y., Hsi-Sheng, W., Hsiao-Lin, H., Shen, A. C., Jui-Ying, F., & Ching-Yu, H. (2018). The effects of peer victimization on Children's internet addiction and psychological distress: The moderating roles of emotional and social intelligence. *Journal of Child and Family Studies,*1-12.
60. Martin, J. (2014). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice: CCJ, 14*(3), 351.
61. Greer, B. T., Cotulla, G., & Seddighzadeh, H. (2016). Should sex traffickers be subject to sexually violent predator laws? *Journal of Criminal Psychology, 6*(3), 121-133.
62. Lee, B. H. & O'Sullivan, L.F. (2014). The ex-factor: Characteristics of online and offline post-relationship contact and tracking among canadian emerging adults. *The Canadian Journal of Human Sexuality, 23*(2), 96-105.
63. Gámez-guadix, M., Almendros, C., Borrajo, E., & Calvete, E. (2015). Prevalence and association of sexting and online sexual victimization among spanish adults. *Sexuality Research & Social Policy, 12*(2), 145-154.
64. Strohmaier, H., Murphy, M., & Dematteo, D. (2014). Youth sexting: Prevalence rates, driving motivations, and the deterrent effect of legal consequences. *Sexuality Research & Social Policy, 11*(3), 245-255.
65. Thomas, S. E. (2018). "What should I do?": Young Women's reported dilemmas with nude photographs. *Sexuality Research & Social Policy, 15*(2), 192-207.
66. Açar, K. V. (2016). Sexual extortion of children in cyberspace. *International Journal of Cyber Criminology, 10*(2), 110-126.
67. Burnap, P. & Williams, M. L. (2016). Us and them: Identifying cyber hate on twitter across multiple protected characteristics. *EPJ Data Science, 5*(1).
68. Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30, 1-25.
69. Yar, M. (2006) *Cybercrime and Society*. London: Sage.p.185.
70. Slonje, R. and Smith, P.K. (2008) Cyberbullying: Another main type of bullying? Scandinavian Journal of Psychology, 2008, 49:147–154.

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.

******