Global Scientific JOURNALS

GSJ: Volume 8, Issue 4, April 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

WHAT ARE THE POLICE RESPONSES TO SEVERITY OF CYBERCRIME FOR VICTIM'S SAFETY AND SECURITY?

By ABU TAHER MUHAMMAD ABDULLAH

Abu Taher Muhammad ABDULLAH is currently working as Additional Superintendent of Police, District Police, Thakurgaon, Bangladesh. Recently, Mr. ABDULLAH completed MA Criminology from University of Nottingham, UK, PH-+880-1743653571. E-mail: atmabdullah77@yahoo.com

ABSTRACT

This study explored police responses to severity of cybercrime with a systematic literature review. After searching Scopus and ASSIA databases, 111 articles were thematically analyzed to find police responses to cybercrime. While most of the articles were originated from Anglo-American region (n=85), maximum articles followed empirical research (53.16%), and cyberbullying was common of different cybercrimes. In response to scamming, fraud and hacking, detectives are predominantly working in the cyberspace. School resource officers, especially in USA and Canada, are responsible to maintain code and conducts of the schools for students who commit cyberbullying in the school premises. Australian police adopt 'victim-oriented approach' to respond online fraud, where they use financial intelligence to identify advance fee fraud and romance fraud victims. In particular, police respond to cybercrime through investigation, detection and intervention by adopting 'target hardening', collect intelligence from 'fusion centers', and 'special unit' to secure online theft victimization. Besides, 'Story telling', 'three stage investigative models', 'Korean Desk' and public-private cooperation were identified as investigation strategies. However, police officers cannot patrol in cyberspaces, even though supranational police organizations are active to control cybercrime. Police officers believed that awareness amongst the youth is the key response to cybercrime. Furthermore, this research on police response to cybercrime will enrich existing literature, but not beyond limitation of empirical observation. This will impact future research endeavor in the field.

Key Words
Cybercrime, Policing, Cyberbullying, financial fraud, online fraud, Cyber-victimization

Introduction

Modern world is the realm of information and technological advancement. While technology shapes everyday business and influence social life as a blessing and curses simultaneously, where 'crime follows opportunity' that provides the basis of cybercrime (Clough, 2015: i). At the advent of internet, globalization gets momentum to disappear economic, social and political boundaries (Solak and Topaloglua, 2015). According to International Telecommunication Union (ITU) statistics of 2016, 3,385 million world populations are using internet and increasing day by day (ITU, 2018). With the help of internet service provider, online banking, e-commerce and social networks expedite economic growth as well as build a good relationship worldwide. Unfortunately, this online space is becoming a breeding ground for malicious activities which emerged new dimensional crime that is cybercrime and its severity, meaning intensity, is a great concern for academia, organisations, global governments, police departments and intelligence units (Arpana and Chauhan, 2012).

In the last two decades, as technological leapfrogging hackers exploit this opportunity for their monetary gain, anonymous setting in the internet helps them to expand their network to make partners to organise to commit financial fraud and online fraud like identity theft, credit card theft and bank account details theft (Paquet-Clouston *et al.,* 2018). Besides, cyber piracy, larceny and cyber pornography are also committed in the internet (Lu *et al.*, 2006). This internet network not only increases the victim's number but also increase the offenders (Broadhurst and Grabosky, 2005:31). These severities seek more police attention as police is the main law enforcing agents. The current research is an endeavour to find how police respond against the severity of victim's safety and security focusing on the strategies of controlling cybercrime.

Literature review

Cybercrime is the 'computer crime', 'Information Technology Crime', 'hi-tech crime' and 'digital crime' which refers two types of crimes, like offences targeted computer and its network to gain unauthorized access to system, programmes and data called 'cyber-dependent' crimes, while other category is the traditional one such as theft, fraud and forgery where computer system, network and technology use to commit these crimes called 'cyber-enabled' crimes (Goodman and Brenner, 2002; Clough, 2015:10-11). While Gillespie (2019) argues that cybercrime is a type of computer crime. Likewise, it has been argued that 'digital' and 'hi-tech' crime are taken place without connection to the internet whereas 'e-crime' and 'cybercrime' need the connection (Hunton, 2009: 529). Whether Thomas and Loader (2003:3) provide a working definition for law enforcing agencies to resolve the controversy regarding the definitional aspect of cybercrime as 'computer-mediated activities' occurs

in the 'electronic networks' globally which considered either illegal or illicit among the parties. Hence, cybercrime may be of crime which prohibited by law or deviance that breaches social norms. Thus, 'sexually explicit speech and imagery' in online are an example of deviance (Yar, 2006:9).

While internet facilitate new dimension of 'social interactions' as well as extended criminal activities to victimise people like 'paedophile networks' (O'Connell, 2000), 'hate-related propaganda' (Whine, 2000), 'financial crimes' (Neumann, 1995), and 'forging of hyper-criminal networks'. Hence, Mackinnon (1997) argues 'online populations' are participated various 'quasi-criminal activities', for instance, 'verbal abuse', 'defamation', 'harassment', 'stalking and in extreme cases "virtual rape" (Williams, 2001:152-153). These deviant behaviours are usually treated simple misbehaviour as considering "virtual" element, in contrast to, "real-world affairs". However, Williams (2001:152-153) substantiated this argument as virtual and real divide help to escape the accountability of online offenders in the question of cybercrime victims' safety and security.

Levi (2001:44) argues that computers and internet 'democratize criminal opportunities' for online access to the financial and defence sectors which is not possible physically. While Tuttle (2017:4-7) states an example of financial cybercrime where hackers has taken away $81 million from Bangladesh Bank as cyber criminals modify, add or delete entries of the business process like deliveries and invoicing ultimate result is the payment goes to incorrect party. Besides, Brenner (2007) argues hacker may get 'unauthorized access to a computer' network without ill motive but if they get once an access will take 'credit card' information or "deface" websites. In addition, 'online fraud may happen through various medium like 'e-mail, social networking' like 'chat or dating websites, and online trading sites' (Finch, 2007). As hacking and online fraud have a relation, for example, credit card details could be achieved by hacked web servers. Consequently, multiple victimization may happen as scams where individual 'identity or account details' can be stolen and financial institutions, 'government agencies or service provider' may be deceived (Hutchings, 2013: 93-114). In fact, 'ad-hoc associations' between unknown individuals are facilitated by the internet in the cyberspace to victimize people (UNDOC, 2010).

Cybercrime is a global issue which is a great concern for the countries around the world along the international organisations like UN, G-8, EU, and the Council of Europe particularly for law enforcement and prosecutions of cybercrimes, when law enforcing agents are trying to execute existing law in the criminal activities in the cyberspace (Goodman and Brenner, 2002: 139). While Clough (2015: 23-26) argues since early 1980s international bodies have led to build a legal framework to combat cybercrime but failed. However, the 'Council of Europe Convention on

Cybercrime', also called Budapest Convention, is the 'first binding multinational instrument to address issues of cybercrime' activated on July 1, 2004. Hence, the United Nations Office on Drugs and Crime (UNODC) also agreed, this planned legislation has great influence on fighting against severity of cybercrime, though it is a regional initiative (Clough, 2015: 23-26).

Wall (2001:169) argues misunderstandings of internet that it cannot be oversee and there is lawlessness to fight severe form of cybercrimes which provides some extent of 'moral holiday' for the law enforcement authority and other criminal justice agents. For example, these misconceptions are trans-jurisdictional and fear of commercial and political exploitation in combination of media sensation which misguided people about internet. Whereas Saini *et al.* (2012) argue privately owned information technology companies are trying to make happy customers not to worry about transnational crime. Besides, human rights organisations are against strict control and monitoring of cyberspace. In fact, these misunderstandings and misconception leads to fighting cybercrime severity more complex to ensure safety and security of cybercrime victims. However, researches on police response against severity of cybercrime very scarce which justify the current research.

Methods

Literature search

This study conducted in accordance with the evidence-based guidelines for systematic reviews set forth in the 'PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses)' statement to ensure quality (Liberati *et al.,* 2009). An electronic literature search conducted using the Scopus and ASSIA (Applied Social Sciences Index and Abstracts) databases from 2014 to 2018 time scale. Successive terms in each search added sequentially in time, as the search was revised during the initial paper selection process in the following way (Ramirez and Choucri, 2016):

- (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)

In case of 'cybercrime' search term, there was variation in terminology like 'cybercrime', 'cyber crime' and 'cyber-crime' in the research articles for both databases which noted in this study and searched following those terms (Ramirez and Choucri, 2016:2230). Finally, 'cybercime' term kept for this research as it is internationally recognized in the UN and Cybercrime Conventions (Clough, 2015:10-11). For completeness of search, more terms were looked in addition, such as cybercrime victim, cyber security, policing cybercrime, police response, victim's security, victim's safety, cyber

policing, cyber domain, cyber war, cyberbullying, cyber physical, cyber safety, cybernetics, sustainability, surveillance, cyber stalking, online, digital, internet, web server, network, virtual world, social networking, internet abuse and cyberspace (Ramirez and Choucri, 2016).

Inclusion and exclusion criteria

Full articles retrieved only based on some inclusion criteria (Klettke *et al.*, 2014). While the focus provided on the severity of cybercrime and police responses to cybercrime. Then, priority was given to the journals that illustrated causal factors of cybercrime. After that, the articles related with police investigation process, multi agency initiatives and policy matters regarding cybercrime fighting in the internet were important criteria for literature search. Next, criminal justice matters related articles were also documented. Therefore, the articles were analyzed and extracted results.

Considering exclusion criteria, different traits were focused like the publications which were written other than English excluded for syntactical analysis (Lastdrager, 2014). 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.

The total number of articles found 270 from Scopus and ASSIA databases were 120 and 150 respectively (**Figure 1**). 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. From 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 from 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. Finally, 111 articles were fixed for the analysis of this review and 26 articles were excluded.

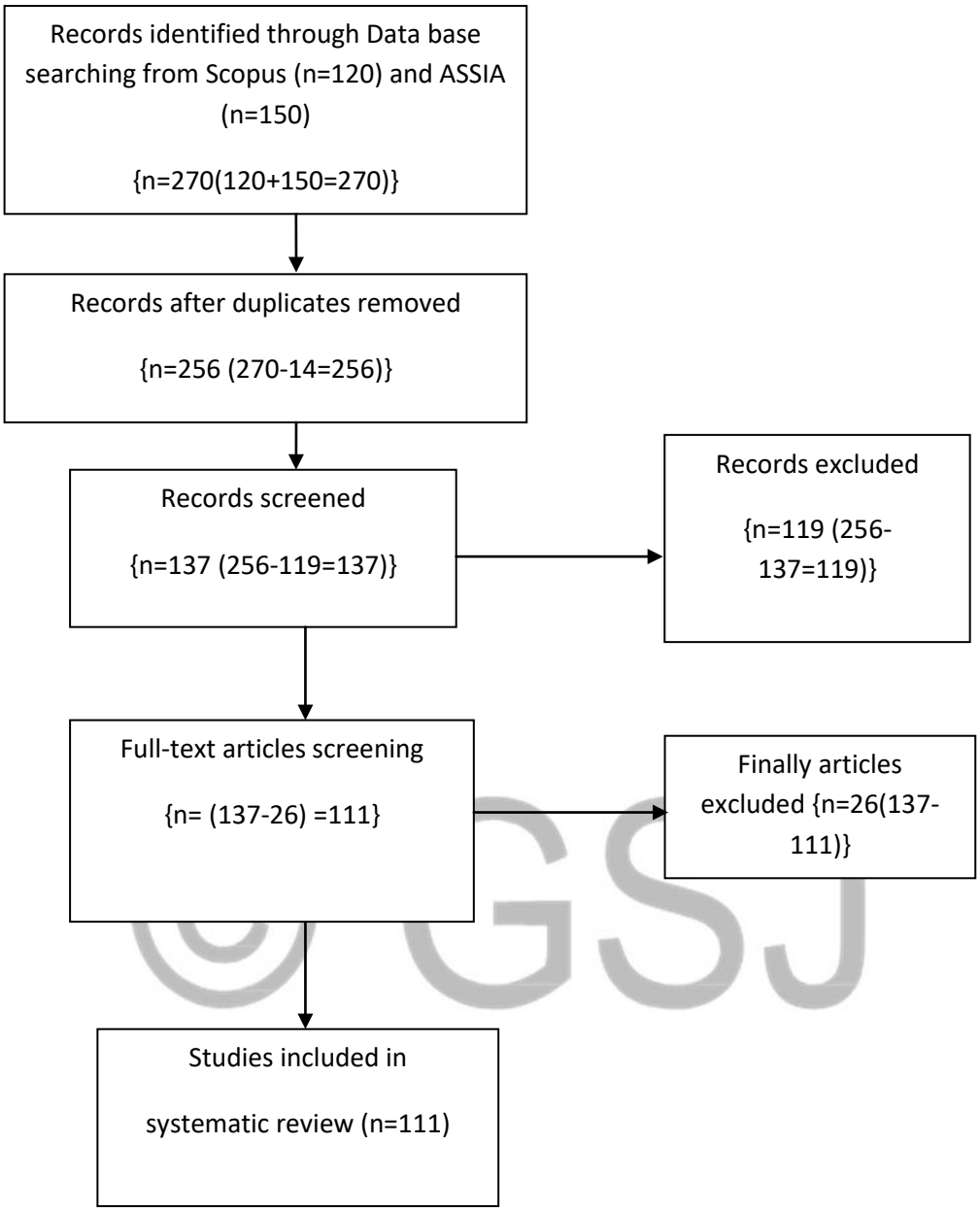

Figure 1: Flowchart of the articles selection of the review (Klettke *et al.,* 2014)

Research design

A systematic literature review method followed for this research (Booth *et al.*, 2012). As systematic literature review is the explicit 'accumulation, transparent analysis and reflective interpretation' of previous research findings and outcomes of 'a specific questions' (Rousseau *et al.*, 2008). This research conducted based on the four criteria, such as search, appraisal, synthesis and analysis which comprised a mnemonic 'SALSA' (Sidebottom *et al.*, 2017). Articles were search based on Scopus and ASSIS databases to collect information on 'causes', 'severity', 'policing' and 'criminal

justice' related with cybercrime. To this end, 'full text 111 articles' were selected based on predetermined 'inclusion and exclusion criteria'.

Data analysis

After carefully reviewing sources, key analysis has been done through thematic analysis method to assess the police responses to minimise the victimization of cybercrime (Riessman, 2008, p. 11; Castleberry and Nolen, 2018). 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' (Nowell *et al.,* 2017; Lawless and Chen, 2018). 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, as shown in **Table 1** (Braun and Clarke, 2006; Thorne, 2000:69). In this review, few findings were produced in graphs format to show the richness of the findings. Besides some sorts of findings were discussed elaborately to have an in-depth insights of the logics that provided in the searched articles regarding police responses to cybercrime severity.

Table 1: Number of themes found in the analysis (Cranwell *et al.*, 2016)

Name of themes	Number of sub themes
Causes and severity of cybercrime victimization	14
Responses of police and other criminal justice agencies against cybercrime	7
Challenges for cyber policing	3
Total	24

Results

Geographical distribution, research pattern and Kinds of cybercrime

The findings of this study indicated that the most of the research on cybercrime is Anglo-American origin that is 85 articles of 111. Most of the articles generated in the search were from European region 46 articles representing 41.44% of the search total, as shown in the **Figure 2** below. Whereas the lowest research articles found in the African region (n=3) comprising 2.701% of all articles. Interestingly, no article was found from the South American region on the cybercrime study which indicates that cybercrime has not been subject to academic research as yet. Though researchers

concerned about the cybercrime in the Asian region where 16 articles (14.41%) found, but their initiative like point on the tip of the ocean, as this region are mostly populous there may have chance more victimization of this crime. On the other hand, the researchers of the Australian area produced 6.31% (n=7) of the searched articles.

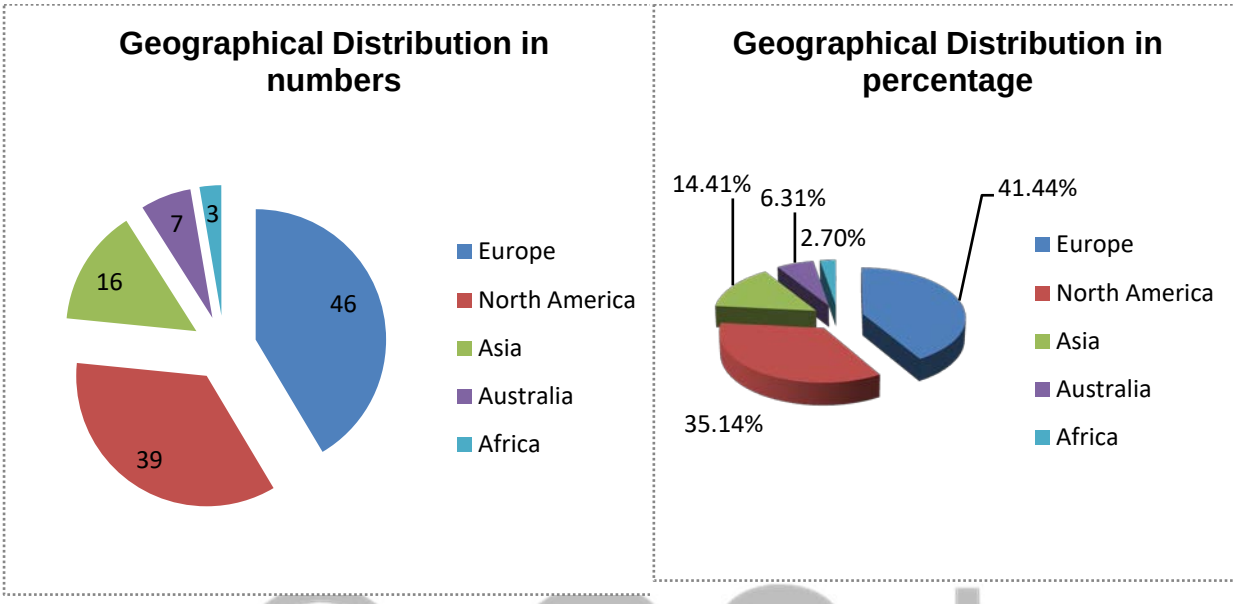

Figure 2: Geographical distribution of cybercrime research and researchers in the world

Regarding cybercrime research pattern, maximum research done depending on the primary data sources which comprises 53.16% (n=59), whereas the minimum research type is ethnographic research with 0.9% (n=1), as depicted in the **Figure 3**. It indicates that researchers are interested to find the causes cybercrime victimization, victims position in committed offence whether they are really victims of cybercrime or their acts contributed to the victimization, offenders stand in cybercrime commission, responses of police and other criminal justice agencies to cybercrime, and investigation process of cybercrime by police based on the survey either face-to-face interview or online questionnaire survey on victims, parents, police, prosecutors, prison officers, lawyer or social care staffs and in possible case contact with offenders. While the second most research tendency amongst cybercrime researchers is secondary research which constituted 44 articles (39.64%). Of the 111 articles of this study where researchers are interested to test the theory, research done based on secondary sources from the official data, police cases and records, data from various online based research organisations and campaign (See **Figure 3** below). Besides, others research pattern followed by cybercrime investigators are case study and meta-analysis comprising 4 (3.60%) and 3 (2.70%) articles respectively amongst the articles fixed for the present study.

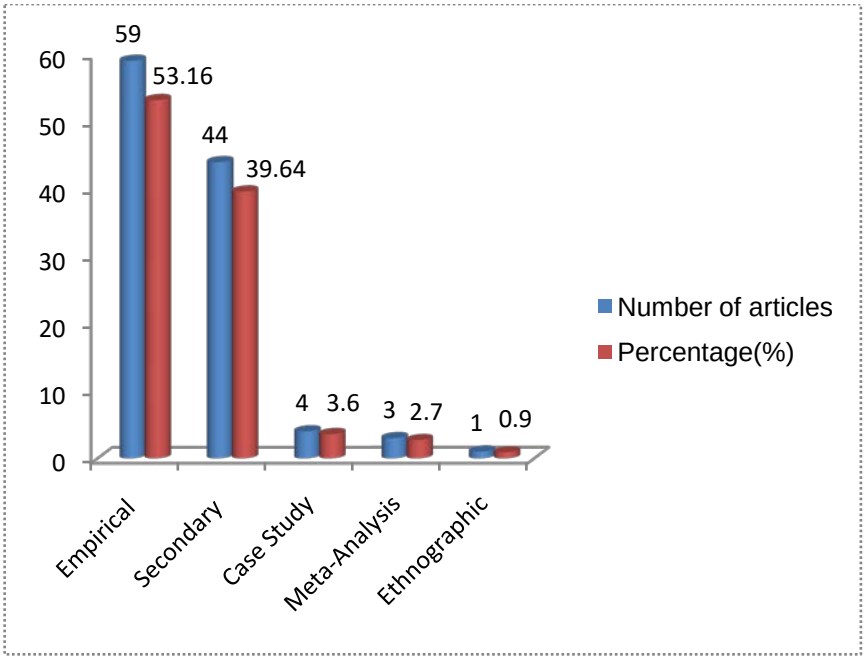

Figure 3:Existing cybercrime research pattern

Cyberbullying was prevalent of the articles reviewed comprising 19 articles amongst various kinds of cybercrime. Where cyberbullying considered as 'bullying that done by electronic means like text messages, emails, online chartrooms or social networking sites' primarily prominent in adolescents people (Wolke *et al.,* 2017). Next, 15 articles found for computer-based cyber deviance category where research related 'software piracy, online harassment and computer hacking' included. Fraud category like online fraud or financial fraud comprised 10 articles occupied 3rd positioned. Other categories of cybercrime found for review are cyberstalikng (n=4), sexting and online sexual victimization (n=4), online child sexual abuse (n=3) and online illicit market called crypto market (n=3).

Responses of police to cybercrime

In this article, theme on police response has been discussed to show the trajectories of police responsive mechanism to combat against cybercrime. Though supranational police organizations are established, but the main police actors in the realm of cybercrime fighting depend largely on the detectives as police officers cannot patrol in cyberspaces particularly scamming, fraud and hacking (Beek, 2016). It is supported by another finding that police and school resources officers are not considering cyberbullying as a crime rather they thought it is 'reactive and unnecessarily punitive' (Broll and Huey, 2015). While school resource officers are 'sworn police officer' with uniformed and armed, whose responsibilities are patrolling to the school premises, investigation of criminal complainants, minimizing disruption and duties imposed by the school authorities for dealing with

students, who violate code and conducts of the schools, for example, these officers are found in USA and Canada. In addition, police officers believe that cyber-policing duties could be possible within the existing laws for controlling cyberbullying behaviors that cross into criminal territory. To this end, police officers perceived that education is the potential response to cybercrime as young generation commits this crime by using computers beyond the ambit of criminal justice system (Broll and Huey, 2015).

While Australian police responded to cybercrimes like online fraud with a mechanism named 'victim-oriented approach' (Cross, 2016:125). In this approach, police use financial intelligence to identify potential victims of advance fee fraud and romance fraud, who are sending money to West African countries, and deliberately police send letter to the targeted victims to intervene from sending money. This review identified three Australian projects, namely Project Sunbird (West Australian Police and West Australian Department of Commerce), Operation Disrepair (South Australian Police), and the National Scams Disruption Project (Australian Competition and Consumer Commission), which were initiated in collaboration with police and consumer protection agencies (Cross, 2016:130). Five stage processes followed, such as, the first one, police with intelligence identified five West African countries-Nigeria, Ghana, Togo, Sierra Leone and Benin; then, commerce department send a letter to the potential victims who are going to send money in those countries explaining the reason of suspicion of fraud. If the victims continue to send money after three months, second letter is usually issued. Next, in the third stage, commerce department liaises with bank, remittance agencies and relevant organizations to block account to identify offenders and probable victims. After that, fourth stage is intelligence related, where victims are targeted, who make contact with the offenders to gather information. Finally, in the last stage, police engaged for investigation targeting local offenders and if required referred to national and international police agencies for help. Australian Competition and Consumer Commission (ACCC) followed these five stages themselves and when required help, then seek local police assistance as they are empowered by legal instruments. Thus, Australian police follow the tertiary crime prevention technique such as eliminating influences, focusing on individuals or groups at risk and finally focusing the offenders who already committed cybercrimes or aims to commit (Cross, 2016).

Next, police and other criminal justice agencies response to online fraud is "target hardening", which is long-established proactive method used by law enforcement agencies for decades to provide safety and security of the cybercrimes victims by informing the tricks, tactics and methods employed by online fraudsters to avoid being targeted (Bolimos and Choo, 2017). In addition, investigators of online fraud found 'addict symptomology' like drug addiction, while they are victimized by the scammers and lost money, they cannot believe that they are victimized as the drug addicted person

who needed rehabilitation like drug users. For this, fraud victims need to build a good cooperation with law enforcement agency to facilitate arrest the culprits physically (*ibid*.303-305). Then, fusion centers act as an important stem for law enforcement agencies to get information about cybercrimes (Carter *et al.*, 2017). For instance, the USA has been created 78 fusion centers after 1/11 terrorist attack which are working nationwide at present to share intelligence with law enforcing organizations on terrorist, cybercriminals and traditional crimes offenders. In fact, new specialized units of police, for example, 'the Metropolitan and City of London police fraud squad' in the UK work to protect risks of fraud like identity theft, card theft, data breach and hacking scandals (Levi, 2017).

Furthermore, storytelling recognized as a technique to investigate, detect and arrest of the scammers in advance fee fraud case (Beek, 2016). Here, investigators are pretending as a victim to produce fictitious tale to make believable to the criminals, though police, fraudsters and victims have to struggle to create story as real one. For instance, detectives of CID (Criminal Investigation Department) of Ghanaian Police got success by telling storey to persuade the suspect scammers to meet physically, and arrest them (*ibid*.307). While 'three stage investigative models' for computer integrity crimes are followed by police, which include hacking, malware distribution and denial of service attacks are targeted networks and computers, for example, in Finland local police district has the capacity for computer forensics analysis though variation in cybercrimes exits in different districts (Leppänen and Kankaanranta, 2017). Here, first, the entire pre-trial examination of cybercrimes are conducted by a computer forensic investigators; then, two individual investigators conduct computer forensic and tactical investigation separately where occasional investigators engaged in tactical investigation, and for the last one, computer forensic investigation is done by computer forensic investigators while tactical investigations performed by centrally designated investigators.

'Korean Desk' in the Philippines, an example of international cooperation, identified in this research (Kim, 2018). While cybercrime is transnational in nature in terms of victims, perpetrators and evidence location, which need pragmatic approach to cybercrime, in combination of police, government agencies, private sector and international organizations (Brown, 2015). Concomitantly, cybercrime investigators should possesses some forensic investigative skills like 'soft'-communicative, intuitive skills and strategy, and 'hard'-forensic imaging, hardware and structured data analysis skills (Brown, 2015:65-66). In addition, it found that 63% child pornography offenders were referred to SAFE Network Inc. (SAFE) by probation officer obeying the court order for assessment of problematic online sexual offending behavior, and after assessment police investigation on this cybercrime initiated, and then, sent for treatment following 'court mandate' by probation officer (Price *et al.*, 2015). Hence, cybercrime investigation depends on police officers'

rational choice, where cost and benefit analysis is an important factor with case nature, which immensely influence the police officers intention to work in cooperation with private investigators (PIs) (Lee and Yun, 2014).

Discussion

The significance of the findings of regional distribution, research pattern, and cybercrime classification indicates how much people and authorities are concerned about the severity of cybercrime. However, no article was found from China, though they have over 750 million internet users (Broadhurst and Grabosky, 2003:31; ITU, 2016). Police responded to cybercrime like scamming, fraud and hacking (Beek, 2016) with the help of detectives due to regular patrolling in the cyberspace is not possible. Although mentality of police officers and school resource officer against cyberbullying found that it is not a serious crime and action taken for this would be reactive and punitive. However, opposite view also noted as school officials struggle to track cyber-bullies for its jurisdiction which occurred in cyber-space and the perpetrators know it to 'side-step of school intervention'.

Furthermore, pro-active method like "target hardening" used by police to inform the tricks, tactics and methods applied online fraudsters to avoid being victimized (Bolimos and Choo, 2017). Likewise, Australian Police followed 'victim-oriented approach' (Cross, 2016); in the USA, police use fusion centre to share intelligence with law enforcement agencies on cybercriminals (Carter, *et al*, 2017). Mostly used strategies were ‘storytelling technique’, ‘three stage investigative models’, ‘Korean desk’, and private investigators to respond to control cybercrime. However, ‘cybercrime units have proliferated over time and are on the path to becoming a normative aspect of policing’ (Willits and Nowacki, 2016).

Conclusion

Severity of cybercrime is ubiquitous and a great concerns from general public to all governments of the world. As police is the main law enforcing agent they have to respond this issue first. However, police are facing problem for patrolling in online, but police responded to cybercrime with the help of various investigation, detection and intervention strategies from government initiative to private investigators. This review was an initiative to examine police responses to cybercrime underpinning on previous literature. But it was not without limitation, and to overcome this limitation future endeavour of police focused empirical research would expect to examine, how people could be incorporated police response to cybercrime.

References

Arpana, M. and Chauhan, M. (2012). PREVENTING CYBER CRIME: A STUDY REGARDING AWARENESS OF CYBER CRIME IN TRICITY. *International Journal of Enterprise Computing and Business Systems*, Vol.2(1): 2230-8849,[Online].Available at: http://www.ijecbs.com, [Accessed 03/09/2018]

Beek, J. (2016). CYBERCRIME, POLICE WORK and STORYTELLING in WEST Africa. *Africa, 86*(2), 305-323. doi:10.1017/S0001972016000061

Bolimos, I. A. & Choo, K. R. (2017). Online fraud offending within an Australian jurisdiction. *Journal of Financial Crime, 24*(2), 277-308. doi:10.1108/JFC-05-2016-0029

Booth, A., Papaioannou, D. and Sutton, A. (2012). *Systematic Approaches to a Successful Literature ReviewI.*London:Sage.p.279.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 77–101.[Online]Available at: doi:10.1191/ 1478088706qp063oa,[Accessed 21/06/2018]

Brenner, S.W. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime Online* (pp.12-28).Devon: Willian Publishing.

Broadhurst, R. and Grabosky, P. (2005). Cyber-crime: The Challenge in Asia. Hong Kong: Hong Kong University Press.p.434.

Broll, R. & Huey, L. (2015). "Just being mean to somebody isn't a police matter": Police perspectives on policing cyberbullying. *Journal of School Violence, 14*(2), 155-176. doi:10.1080/15388220.2013.879367

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55-119. doi:10.5281/zenodo.22387

Carter, J. G., Carter, D. L., Chermak, S., & Mcgarrell, E. (2017). Law enforcement fusion centers: Cultivating an information sharing environment while safeguarding privacy. *Journal of Police and Criminal Psychology, 32*(1), 11-27. doi:http://dx.doi.org/10.1007/s11896-016-9199-4

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,[Online]Available at: https://doi.org/10.1016/j.cptl.2018.03.019,[Accessed 21/06/2018]

Clough, J. (2015). *Principles of Cybercrime*. 2nd ed. Cambridge: Cambridge University Press.p.524.
Cohen, L. E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Cranwell, J., Britton, J. Bains, Manpreet (2016). "F*ck it! Let's get to drinking – poison our livers!": a thematic analysis of alcohol content in contemporary YouTube music videos. *International Journal of Behavioral Medicine,* Vol.24, Issue 1, pp 66–76, [Online].Available at : http://eprints.nottingham.ac.uk/34671/8/art%253A10.1007%252Fs12529-016-9578-3.pdf,[Accessed 28/06/2018]

Cross, C. (2016). Using financial intelligence to target online fraud victimisation: Applying a tertiary prevention perspective. *Criminal Justice Studies, 29*(2), 125-142. doi:10.1080/1478601X.2016.1170278

Finch, E. (2007). The problem of stolen identity and the Internet, in Y. Jewkes (Ed.), *Crime Online* (pp.12-28).Devon: Willian Publishing.

Gillespie, A.A. (2019). *Cybercrime: Key Issues and Debates*.2nd ed. Oxon: Routledge.p.390.

Goodman, M.D. and Brenner, S.W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, Volume 10, Issue 2, SUMMER, Pages 139–223, https://doi.org/10.1093/ijlit/10.2.139

Hunton, P. (2009). The growing phenomena of crime and the internet: A cybercrime execution and analysis model'.*25 Computer and Law and Security Report 528-535*, in J. Clough (2015) *Principles of Cybercrime*. 2nd ed. Cambridge: Cambridge University Press.p.524.

Hutchings, A. (2013). 'Hacking and Fraud: Qualitative analysis of online Offending and Victimisation', in K. Jaishankar and Ronel, N. (2013)(eds.) *Global Criminology: Crime and Victimization in a Globalized Era*. London: CRC Press.p.93-114.

ITU (International Telecommunication Union) (2018). 'New data visualization on Internet users by region and country, 2010-2016', [Online].Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default, [Accessed 30/08/2018]

Kim, K. H. (2018). The Korean desk in the Philippines: Facilitating collaboration in international criminal justice. *Policing, 41*(1), 159-174. doi:10.1108/PIJPSM-05-2016-0067

Klettke, B., Hallford, D.J. and Mellor, D.J. (2014). Sexting prevalence and correlates: A systematic literature review, *Clinical Psychology Review*, 34: 44–53
Lastdrager, E.E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science,* **3**:9.

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,[Online]. Available at: https://doi.org/10.1080/10646175.2018.1439423,[Accessed 21/06/2018]

Lee, C., & Yun, I. (2014). Factors affecting police officers' tendency to cooperate with private investigators. *Policing, 37*(4), 712-727. Retrieved from http://ezproxy.nottingham.ac.uk/login?url=https://search.proquest.com/docview/1634006814?accountid=8018

Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology & Crime Prevention, 18*(2), 157-175. doi:http://dx.doi.org/10.1080/14043858.2017.1385231

Levi, M. (2001). "Between the Risk and the reality falls the shadow", in D. S. Wall (2001)(ed.) *Crime and the Internet*. London: Routledge.pp.44-58.

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. doi:10.1007/s10611-016-9645-3

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,[Online].Available at:doi:10.1371/journal.pmed.1000100, [Accessed 28/08/2018]

Lu, C.C., Jen, W.Y., Chang, W. and Chu, S. (2006). Cybercrime & Cybercriminals: An Overview of the Taiwan Experience. *JOURNAL OF COMPUTERS*, VOL. 1, NO. 6,pp.1-8.

Mackinnon, R.C. (1997). "Punishing the persona: Correctional Strategies for the Virtual Offender", in S. Jones (ed.), *Virtual Cultures: Identity and Communication in Cybersociety*, London: Sage.

Neumann, P. (1995). *Computer Related Risks*, Reading, Mass.: Addison-Wesley, in D. S. Wall (2001)(ed.) *Crime and the Internet*. London: Routledge.p.221.

Nowell, L.S., Norris, J.M., White, D.E. and Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods,*Vol.16: 1–13,[Online].Available at: DOI: 10.1177/1609406917733847 journals.sagepub.com/home/ijq,[Accessed 15/06/2018]

O'Connell, R. (2000). *Through the Looking Glass: a perspectives of child sex iconography in cyberspace,* paper presented at the British Society of Criminology Conference, Leicester University, in D. S. Wall (2001)(ed.) *Crime and the Internet*. London: Routledge.p.221.

Price, M., Lambie, I., & Krynen, A. M. (2015). New Zealand adult internet child pornography offenders. *Journal of Criminal Psychology, 5*(4), 262-278. Retrieved from http://ezproxy.nottingham.ac.uk/login?url=https://search.proquest.com/docview/1713503018?accountid=8018

Paquet-Clouston, M. and Décary-Hétu, D. & Olivier Bilodeau (2018). Cybercrime is whose responsibility? A case study of an online behaviour system in crime, *Global Crime*, 19:1, 1-21,[Online].Available at: https://doi.org/10.1080/17440572.2017.1411807

Ramirez, R., and Choucri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. *IEEE Access,* 4, 2216-2243.

Riessman, C.K. (2008). Narrative methods for the human sciences, London: Sage Publications.p.253.

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, [Online].Available at: https://www.tandfonline.com/doi/abs/10.1080/19416520802211651,[Accessed 21/06/2018]

Saini, H., Rao, Y. S. and Panda, T.C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)*. Vol. 2, Issue 2, pp.202-209, www.ijera.com,

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*, [Online]Available at: DOI 10.1186/s40163-017-0068-y, [Accessed 28/08/2018]

Solaka, D. and Topaloglua, M. (2015). The Perception Analysis of Cyber Crimes In View of Computer Science Students, 4th WORLD CONFERENCE ON EDUCATIONAL TECHNOLOGY RESEARCHES, WCETR-2014, *Procedia - Social and Behavioral Sciences*,182 :590 – 595,[Available at: www.sciencedirect.com,[Accessed 03/09/2018].

Thomas, D. and Loader, B. D. (2006). *Cybercrime: Law enforcement, Security and Surveillance in the information age*. London: Routledge.p.300.

Thorne, S. (2000). Data analysis in qualitative research. *Evidence Based Nursing*, 3: 68-70 [Online]. Available at: https://ebn.bmj.com/content/3/3/68.short, [Accessed 21/06/2018]

Tuttle, H. (2017). The 2017 Cyber risk Landscape. *Risk Management*, Vol. 64, Iss. 1:4-7, [Online]. Available at: https://search.proquest.com/docview/1870564461?pq-origsite=gscholar, [Accessed 28/08/2018]

United Nations Office on Drugs and Crime (UNODC) (2010). *The Globalisation of Crime: A Transnational Organised Crime Threat Assessment,* Sales no.E.10.IV.6, United Nations Publication United Nations Office on Drugs and Crime (UNODC) (2013) *Comprehensive Study on Cybercrime.*

Wall, D. S. (2001). (ed.) *Crime and the Internet*. London: Routledge.p.221.

Whine, M. (2000). "Far Right Extremists on the Net", in D. Thomas and B. D. Loader (2006) *Cybercrime: Law enforcement, Security and Surveillance in the information age*. London: Rutledge.p.300.

Williams, M. (2001). 'The language of Cybercrime', in D.S. Wall (2001) (ed.) *Crime and the Internet*. London: Routledge.pp.152-166.

Willits, D. and Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies*, Vol. 29(2):41,[Online].Available at: https://opensiuc.lib.siu.edu/cgi/viewcontent.cgi?article=1012&context=ccj_articles,[Accessed 26/02/2020]

Wolke, D., Lee, K., & Guy, A. (2017). Cyberbullying: A storm in a teacup? *European Child and Adolescent Psychiatry, 26*(8), 899-908. doi:10.1007/s00787-017-0954-6

Yar, M. (2006). *Cybercrime and Society*. London: Sage.p.185.