Challenges of Cyber Policing in Response of Cybercrime to Reduce Victimization

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*

***Abstract*: This research investigated cyber policing challenges to reduce victimization in response to cybercrime with a systematic literature review method. Thematic analysis technique adopted to synthesize 111 articles of Scopus and ASSIA databases to find the theme 'challenges of cyber policing'. While 'Big Data' is an important hurdle to cybercrime investigation for police and othe law enforcement organizations, as cyber criminals use images and social media texts in cyber offences. Then, recording of traditional crime fails to identify the digital fraud, commercial victimization, and gang culture which is huge challenge of effective cyber policing. Besides, transnational jurisdiction, 'Advaced Persistent Threats (APT), Brexit, interdisciplinary barriers, command responsibility, electronic evidence and lack of equipments and devices were identified as challenges of policing in cyberspace. However, future responsive policies to cybercrime recognized as proactive approach to identify this crime, gain digital specialism, national crime database, 'Swiss Model', and vigilatntes. Hence, this study is not beyond limitation of empirical observations, which will be the future initiative in the field.**

***Keywords*: Cybercrime, policing, challenges, transnational crime, victimization**

I.INTRODUCTION

Advancement of technology makes people more dependent on Internet which is a breeding ground of malicious activities like cybercrime. The invention of the World Wide Web in 1989 has expedited digital communication and interaction among the world population (Hunton, 2011). This phenomenon of the Internet across the globe is directly impacting upon and even underpinning many fundamental aspects of modern society and critical national infrastructures. Cybercrime is a pressing issue for national and international police organizations to respond to cybercrime, 'including the complex dynamics of cybercrime networks' (Harkin *et al*, 2018). In fact, cyber policing envisages huge challenges to reduce victimization.

Cybercrime victimization can 'materialize in the form of offences analogous to the real world, for instance, cyberbullying and online harassment, or through security risks that affect the computer itself, like malware infections, ransomware infections, and theft and misuse of personal data'. While cybercrime victimization leads to symptoms similar to those of post-traumatic stress disorder (Bergmann *et al*., 2018). In the advent of new developments in Informationa Communications Technologies (ICTs), cyber policing has become crucial in contemporary policing discourse. However, law enforcement to deal with cybercrime is still limited, especially in the online environment (Gilmour, 2014). Therefore, the current article will examine the key issues and challenges that cyber policing will come to face in response of cybercrime to reduce victimization in the online environment.

II. LITERATURE REVIEW

'Cybercrime' is often used as a global phenomenon of crime and other undesirable behaviours that involve the use of networked technology (Hunton, 2011). According to the UK's Association of Chief Police Officers (ACPO) "cybercrime" defines as "the use of networked computers or Internet technology to commit or facilitate the commission of crime" (Gilmour, 2014). Likewise, "cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" (European Commission, 2013:3). While cybercrime classified as traditional offences like fraud, forgery, and identity theft; content-related offences like on-line distribution of child pornography or incitement to racial hatred; and offences unique to computers and information systems like attacks against information systems, denial of service and malware (Gilmour, 2014). In other word, cybercriminals are misusing computer and are utilising techniques like spamming, phishing, viruses, malicious code, hacking, denial of service attacks, network intrusion and the distribution and supply of illicit data to commit acts of both criminal and undesirable behaviour. For instance, cybercrime can be extended with the concepts of cyber warfare and cyber terrorism, industrial espionage and disinformation ranging from information warfare to propaganda and political attack. However, cybercrime is a major challenge in determining and tackling of these diverse criminal activities, the difficulty and complexity law enforcement face in their daily affairs (Hunton, 2011).

Cyberpolicing produce particularly unique staffing challenges as cyber competence is harder to acquire, and expertise in other units is less immediately transferable into the cyber realm; cyberexpertise has a shorter lifespan; there is an evident 'brain drain' from cyber units; and career progression within specialist units is particularly a complex problem. While these unique staffing challenges need to address by police organizations across the globe to appreciate in order to optimise their prospects for forming effective specialist cyber-crime units (Harkin *et al.*, 2018). Another challenge is the low priority given to the training of intelligence officers, particularly in strategic criminal intelligence and predictive analysis (Kowalick *et al.*, 2018). Law enforcement agencies are facing challenges of digital forensic analysis is to ensure access to the entire dataset including those segments that are stored online (Naqvi, 2018). Law enforcement is faced with an extensive range of challenges such as the lack of a single crime scene that can span several jurisdictions, each having different legislation, investigation processes and standards of acceptable evidence (Symantec, 2009). Collaborative partnerships with telecommunication companies, the computer industry and internet service providers are critical in assisting police to remain responsive to the challenge (Wilkinson, 2010). The final challenge is the 'reassurance' problem in policing cybercrime (Wall, 2017).

While 'political insurgency, terrorism, cybercrime, and drugs and people trafficking as a transnational networks' format criminals are imposing threat to the safety and security of the citizen of country (Mette Eilstrup Sangiovanni Section Editor, 2005:12). According to Furnelb and Warren (1999) cyber terrorists other than traditional terrorist they are emphasising technology to collect information, recruit hackers and embezzled money from the financial institution as well as individuals which in the long run restrict people movement due to fear of victimization. However, cryptographic technologies strictly maintain by US but unregulated use of this technology by terrorists is constantly threatening of terrorist attack like a double edge blade one way bombing physically and other way destroy defence mechanism causing national insecurity throughout the world (Furnelb and Warren, 1999:28-32). On the other hand, Shelley (2003:310) argues some citizens show sympathy to terrorists as their goals and objectives are coincided with the terrorists which expedite the victimization of mass people.

According to Wall (2001:9) transnational nature of cybercrimes creates various problems to the law enforcement (Broadhurst and Chang, 2012). For instance, police has to think on their decisions for detection and arrest for the cybercrime offenders from outside national jurisdiction which is not cost-effect but in local case police can use their resources in an efficient way. In these situations police has to face difficulties for setting their strategies when jurisdiction of committed offences, offenders, victim and impact of offences are in other location. Furthermore, this trans-jurisdictional dilemma has been created confusion regarding law application as offence committed of the other location which law will be applicable criminal or civil laws, which can differ on places that leads to escape of the offenders obstructing victim's safety and security. While Hunton (2010:385) states that 'mainstream law enforcement authorities must have the ability to combat ever increasing internet based crimes and other unwanted behaviours. In addition, law enforcement investigators should have insights about cybercrime nature and identification of digital evidence of cybercrimes before sending for 'technical examination'. However, Hunton (2010:385) argues trans-jurisdictional phenomena create problem for the investigators of cybercrime in the broader scenario of global cybercrime.

Apart from some peculiar criminological features unique to crime committed in cyberspace, 'the basic challenge for policing now is to grips with the concept of cyberspace—vibrant, resilient, secure or otherwise' (Sampson, 2014). However, very few researches have been done on the challenges exerts from cybercrime.Therefore, this article will examine the present and future cahallenges for cyber policing in response to reduce cubercrime victimization.

III. METHODS

The current 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). Literature search conducted using the Scopus and ASSIA (Applied Social Sciences Index and Abstracts) databases from 2014 to 2018 time scale. Successive terms were used 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)

Some inclusion criteria were followed to retrieve full articles (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 analysed and extracted results. However, 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.

In total, 270 articles were selected from Scopus (n=120) and ASSIA (n=150) databases (**Table 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 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. Finally, 111 articles were fixed for the analysis of this review and 26 articles were excluded.

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

Selection Process	Numbers (n)
Records identified through Data base searching from Scopus (n=120) and ASSIA (n=150)	n=120+150=270
Similar Articles	n=14
Records after similar articles removed	n=270-14=256
Records excluded	n=256-137=119
Records screened	n=256-119=137
Finally articles excluded	n=137-111=26
Full-text articles screening	n=137-26=111
Studies included in systematic review	n=111

A systematic literature review method followed for this study (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'.

Key analysis has been done through thematic analysis method to assess the police responses to minimise the victimization of cybercrime after carefully reviewing sources (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' (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 (Braun and Clarke, 2006). Few findings were produced in tabular and graphs format to show the richness of the findings in this research. Besides some sorts of findings were discussed elaborately to have an in-depth insights of the logics that provided in the searched articles regarding cyber policing challenges to respond against cyber-victimization.

IV. RESULTS

In this paper challenge of cyber policing theme has been discussed to know the trajectories of cybercrime victimization. Challenges for countering cybercrime faced by police and other law enforcement agencies depicted in the **Figure 1** that mentioned in the searched articles in this study by the researchers. The most important drawback for cybercrime investigation is the 'Big Data' which is simultaneously a challenge and opportunity in this modern information technology era (Smith *et al.*, 2017). Where Big Data is the 'volume, variety and velocity of data' that "can be collected, stored and analyzed" to generate criminal behaviours for criminal justice practice like images and social media texts particularly used by cybercrimes perpetrators with their locations. The burgeoning digital media and recording device proliferates data of the social events which is underpinning the cybercrime like cyberbullying, piracy and hacking as well as facilitating protection, detection and investigative information for analyzing criminal manipulation and community mobilisation. For example, "Facebook has over 936 million active users that generate 2.7 billion “Like” actions and 300 million photos per day" (Smith *et al.*, 2017: 266). It argued that the current mechanism of recording traditional crime fails to identify the changing pattern of crime like digital fraud and in some extent commercial victimization and gang phenomena which challenged for effective cyber policing (Marlow, 2014). For instance, people are unaware of digital fraud victimization or amount of loss incurred is so small, they will not willing to report to the police fearing of bureaucratic burden and query, which is a challenge for recording cybercrimes to initiate police investigation. In addition, banks’ willingness to protect their reputation by reimbursing clients for losses and fail to bring offence to attention of police and other law enforcing agents.

Policing of cybercrime envisaged challenge in allocation of their forces and resources in combating organised crimes based on the prosecutions and sentences as it is difficult to separate general crimes and organised crimes; where organised crimes denote criminal activities motivated by profit, 'online pedophile rings', drug dealing, trafficking, prostitution and cybercrimes (Kirby *et al.*, 2016; **Figure 1**). Cybercrimes pose jurisdictional challenges to police as its transnational nature where offences may commit in one country, offenders reside in another and during occurrence may be other country (Brown, 2015; Beek, 2016; Meyer, 2017). It supported, for instance in the UK, the cost of serious and organised crime at least £24 billion which included cybercrime with other crimes (Jarvis and Earis, 2015). Subsequently, it argued though organised crime groups (OCGs) exist around centuries but in modern era their activities more transnational and virtual while they can commit cybercrime across national border instantly with a keyboard button press (Jarvis and Earis, 2015).

Another challenge of policing cybercrimes found in the articles of this study is 'Advanced Persistent Threats (APT)'-state-sponsored espionage groups (Lemay *et al.*, 2018; **Figure 1**). These groups use cyber attacks for spying purpose and breaches security of others country like health insurance companies, entertainment groups, critical infrastructure and even democratic institutions to make news and damage for other countries. For example, the recent "hacking of the

Democratic National Committee and indicting by the FBI of Chinese military personnel for cyber economic espionage" are pronouncing the severity of cybercrimes. In addition, new actors of APT like India and Pakistan joined the ranks of the Western powers, China and Russia in the field of online based espionage and their proficiency to hide make investigation and build idea about their future activities challenging for police and other law enforcing agents (Lemay *et al.*, 2018). Furthermore, European Union (EU) and UK cybercrime policing would face great challenge after Brexit (Ambos and Bock, 2017). Where European Criminal Law and Justice are influencing the criminal law of the Member States based on 'neutralisation, conforming interpretation, assimilation, approximation, mutual recognition and institutionalisation' techniques. While the European Police Office (Europol) is responsible for collection, analysis and exchange of information, coordination, organization and execution of investigations among the Member States for combating cybercrime which will be difficult after Brexit between EU and the UK (Ambos and Bock, 2017).

Interdisciplinary barrier is an impediment for cyber policing in the cyberspace where cyber security demands to have knowledge on "computer science, computer engineering, psychology, information technology, ethics, and criminal justice" by the criminal justice agents to combat cybercrimes effectively (Payne, 2016; **Figure 1**). As criminal justice does not have all the answers how to combat against cyber offenders which required knowledge of biology, computer science, policy, and women's studies otherwise cyber policing will be in stake. Next challenge for cybercrime fighting is identification of command responsibility in the cyber world (van Sliedregt, 2016). Where command responsibility is referred superior or commander criminally responsible for failing to prevent or punish crimes committed by subordinates, while accumulates military and non-military superiors. It is difficult to recognize the source and who make a cyber attack for the virtual nature of cyberspace as well as the subordinates who have communication with attackers, and it is responsibility of commanders to identify it or punish otherwise the commander will be liable (van Sliedregt, 2016).

Corporal punishment against cyber criminals is a challenge to ensure human rights of the offender in case of criminal justice systems (Muaygil, 2016). It was a heated debate regarding physicians' involvement in the state-sanctioned corporeal punishment mechanism. For instance, Saudi blogger who sentenced for 1000 lashes that administered 50 at a time every Friday over a period of 20 weeks for insulting Islamic clerics and government officials on his website under 'tazir' crime category where discretion of the judges are applicable. Before execution of this corporeal punishment doctors would assume the responsibility of evaluating the man's physical fitness to withstand the lashings. These are the challenges for Saudi Arabia's international and legal commitments and membership in the United Nations Human Rights Council (UNHRC). Besides, physicians are in dilemma for moral ethics and religious obligation whether they will participate in the sate-sanctioned corporeal punishment (Muaygil, 2016). In other word, online researches about cybercrime on disable people are facing various challenges (Alhaboby *et al.,* 2017). While cases of cyber-victimization reported against people with disabilities are cyber harassment, cyberbullying, cyber-disability hates crime and cyber sexual solicitation. The challenges which identified were online identity, gate keepers' responses, social media use and addressing 'diversity through promoting inclusivity' of the disable people. Therefore, police faced challenges for lack of essential equipments and devices for fighting cybercrimes online as well as time constraints as they have to respond to more serious acquisitive crimes which demands urgent response (Broll and Huey, 2015).

This study revealed the importance and challenges of electronic evidence in cybercrime cases in the court judgements, where electronic evidence is the data related with electronic devices whether it is created, stored, manipulated or transmitted in a digital form (Sa'di *et al.,* 2015; Sun *et al.,* 2015).This evidence can be stored and retrieved from hard disks or memory banks of electronic devices like computers and Smartphones, whereas for its fragile nature electronic is prune to damage, destruction or it can be altered which pose a question of its authenticity bearing low or no weightage before the court thus undermining the prosecution's or the plaintiff's case. In terms of cybercrimes, it is a 'technical challenge' for police and other criminal justice agencies personnel regarding understanding of electronic evidence, and its preservation and extraction process, and the relevant law of electronic evidence and cybercrimes. Based on this evidence, court judgement of cybercrime related offences will be different and judges could avoid misjudgement (Sa'di *et al.,* 2015; Brown, 2015; Sun *et al.,* 2015). Besides, digital evidence is better than defendants' confession and seized material evidence. However, for example, cybercrime court judgements occupy approximately 60% of total judgements in Taiwan (Sun *et al.,* 2015).

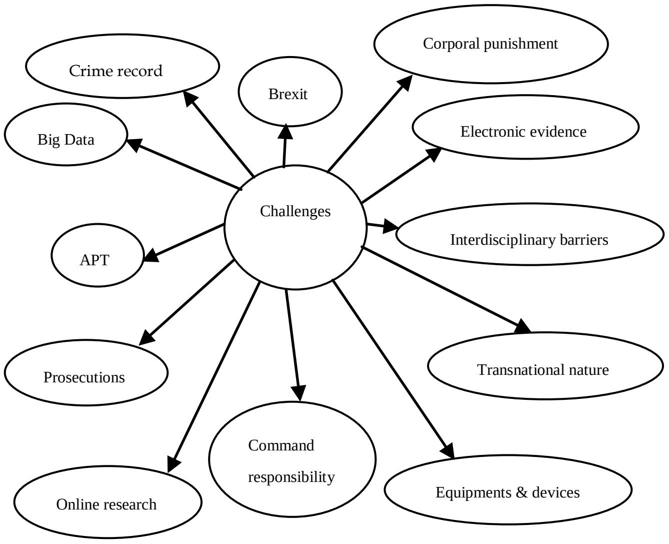

Figure 1: Challenges faced by police and other law enforcing agencies in protection, detection and prosecution of cybercrimes

In response to cybercrime, there are various techniques and mechanism found in the research articles of this study that should adopt by the police and other criminal justice agencies to combat future challenges as depicted in the **Figure 2**. It was suggested that 'digital specialism' is a vital tool to counter cybercrime which will help to investigate cybercrime where digital technologies are imparting role as an intersectional that is from healthcare, politics and education to sex, policing and warfare and transformative medium in the crime and justice arena (Smith *et al*., 2017). Subsequently, criminal justice agents should have to accommodate with digital device and infrastructure along with community participation to fight cybercrime in the virtual world. Whilst it found that present policy and practice of recording crime will produce incomplete scenario of overall cybercrimes, then 'proactive approaches' are inevitable to 'identify crime levels' as an important counter measures of cybercrime management (Marlow, 2014). For instance, waiting for report from bank about online fraud or financial loss will not provide actual victimization figure which need new proactive mechanism to develop between the police, the banks and other partner agencies to specify trends and sequences of cybercrimes.

Another finding asserted 'three simple criteria to identify organised crime offenders like serious crime, specific offence types and co-offending' (Kirby *et al*., 2016). For example, the UK national offender database used these criteria to distinguish each crime from others particularly organised type cybercrimes. In addition, it focused "offence based" data set in lieu of the “offender based” data set that usually evolved from proactive police investigations provides in depth overview of crime pattern. While criminal age, criminal recidivism and offence type will help to develop understanding of the cybercrimes which in the long run could be used to take more effective, preventive, detective and investigative strategies for countering cybercrimes by police (Kirby *et al.*, 2016). It supported that policy makers and regulators need to take a more rigorous and person-centred approach to rule making in respect of social media rather than the fear-based blanket prohibitions that have applied to date to combat cybercrimes in favour of disable people (Bates *et al.*, 2015). For instance, social care staff should allow making friend the disable people in the Facebook to uphold their feelings about humanity and dignity.

European Criminal Law and Justice built on some criteria among the Member States such as neutralisation, conforming interpretation, assimilation, approximation, mutual recognition and institutionalisation to facilitate criminal justice organisations to fight cybercrimes which could be an example for other regions of the world like Asia, Africa and South America to work combindly in their region against ubiquitous nature of cybercrimes (Ambos and Bock, 2017). After Brexit 'Swiss Model' could be followed to maintain future EU-UK relation particularly in cooperation and coordination in the Criminal Justice Systems which will build a strong cybercrime fighting platform (Meyer, 2017). Subsequently, it revealed that Swiss Government follow ‘‘bilateraler Weg’’ where they maintain cooperation with EU's supranational and transnational law enforcing organization through international treaties and through autonomous adaptation they update their laws accordingly with the recent up gradation of EU laws by keeping their autonomous entity. In terms of police cooperation, Switzerland maintain an agreement with the neighbouring countries of EU members states on legal framework for police cooperation by establishing cooperation centres in the border region and remarkably, for instance, the Swidish Initiative with EU is the Convention Implementing the Schengen Agreement of 14 June 1985. In case of cybercrime fighting, Switzerland is working with EU's Joint Investigation Team, Europol and Eurojust to share information regarding online fraud and other cybercriminals through accessing their databases with the help of bilateral agreements (Meyer, 2017).

This research identified that criminal justice systems should incorporate "criminal justice science" for better understanding the multi-disciplinary nature of criminal justice field where knowledge on computer, biology, forensic and gender studies will be achieved by the police personnel, judges and prosecutors to produce conclusive evidence for cybercrimes before court for trial of cyber offenders to reduce cybercrime victimization (Payne, 2016). While commanders’ responsibility could be identified with the help of International Criminal Court (ICC) ruling where commanders must assisted to make them liable for committing cybercrimes by their subordinates with the help of anonymous hackers particularly in the cyberwar as commanders recruit some agents to facilitate the cyberwar (van Sliedregt, 2016). Furthermore, third party should involved in the cybercrime fighting realm for successful criminal justice administration, as the police and the court rely heavily on their testimonies at the pre-trial and trial stages to dispense justice (Ndubueze and Igbo, 2014). Where third party referred the cyber-cafe managers, for instance, Nigerian law enforcement authorities strengthen cyber security through more strategic partnership with cyber-cafe mangers and internet service providers to ensure the security of cybercrime victims. In addition, Presidential rhetoric where they address the importance of cybercrime in their speech influenced police, people and policy maker (Hill and Marion, 2016). However, other improved technique should consider like incorporation of cyber policy with national regulation (Park *et al*., 2018), form new commission as USA (Gest, 2018), analysis of online threats (Awan and Zempi, 2016) and socio-technological inclusion that is social vigilantism (Lindsay, 2017) and School Resource Officers’ engagement like USA and Cnada (Wright, 2016).

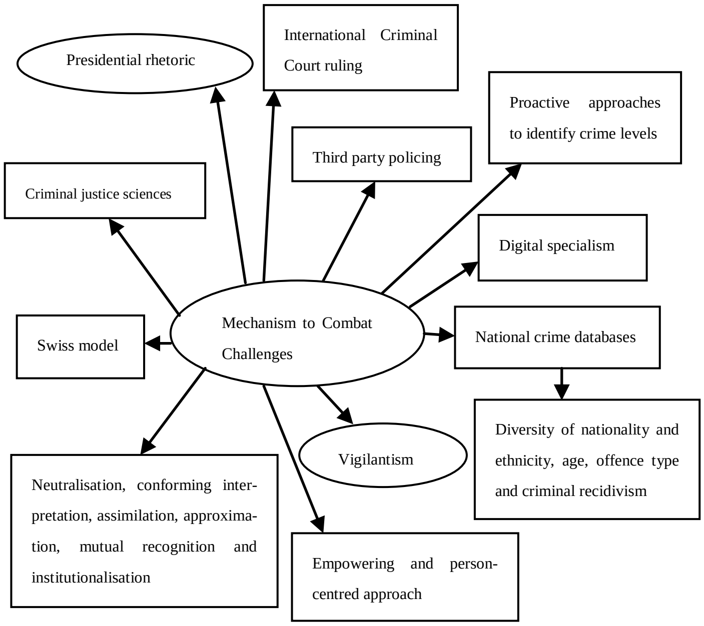
Presidential rhetoric
International Criminal Court ruling
Proactive approaches to identify crime levels
Third party policing
Criminal justice sciences
Digital specialism
Mechanism to Combat Challenges
Swiss model
National crime databases
Diversity of nationality and ethnicity, age, offence type and criminal recidivism
Vigilantism
Neutralisation, conforming inter-pretation, assimilation, approxima-tion, mutual recognition and institutionalisation
Empowering and person-centred approach

Figure 2: Mechanisms for combating cybercrime by law enforcement agent to face future challenges

V.DISCUSSION

Cyber policing mostly encounter transnational challenge to respond against cybercrime to minimize victimization of the public. Because it creates obstacle to lodge any case, specify a palce of occurrence, and arrest of an offenders, as cybercrime may takes place from any where and in any palce (Jarvis and Earis, 2015). While Kowalick *et al*. (2018) supported that police should have the ability to disrupt the attack of transnational organised crime at its source, or at a transit point (Kowalick *et al*., 2018). However, police and other law enforcement authority in the investigation of cybercrime should consider issues such as 'the global distribution of potential volatile and transient digital evidence, the transnational challenges of law enforcement processes, practices and legislation, and the likely extent or continuation of victim harm' (Hunton, 2011b). Other major challenges police face to respond cybercrime are 'Big data', crime recording system, Brexit for UK-EU, APT, electronic evidence, interdisciplinary barriers, and lack of essential equipments and devices. However, Wall (2017) argues 'mesh technologies' will probably join with digital 'devices' to develop lateral networks; while self-deleting communications, such as 'Tiger texts or Snapchat' will eradicate evidence before it can be captured.

However, this article recognized few counter measures to adopt by cyber police to curb the cybercrime victimization. Digital specialism for cyber policing will be an important instrument to investigate cybercrime in the cyberspace (Smith *et al*., 2017). While recording of cybercrime is an impediment to combat cybercrime, then proactive approaches are essential to identify the crime patterns, causes and legal measures for this crime (Marlow, 2014). After Brexit UK can follow the strategy of Swiss Government to maintain their relationship with EU to exchange information, policy, intellingence amongst law enforcement agencies for cybercrime affairs in particular (Meyer, 2017). Besides, cyber policing organizations could engage third party like cyber-cafe managers, train the staffs in criminal justice science, include social vigilantism in the cyberspace, and emphasie national cybercrime regulation to control the cyber criminals to minimize the cyber-victimization. These findings supported by other research as international cooperation requires combating this kind of crime. Sates should hold conventions to adopt effective legal framework to fight and restrict the progress of cybercrime worldwide. Cooperative mechanisms are needed to coordinate and unify joint efforts and to modernize means of combating cybercrime using the latest techniques (Al Azzam, 2019). However, the effectiveness of cyber policing activities depends on staffing as well as the establishment of cross-border cooperation and cooperation with private actors within the state (Borko *et al*., 2019). Hence, fighting cybercrime need to 'execute effective operations; law enforcement has to possess significant understanding of computer technology and to follow the latest developments in the area of network security' (Bojarski, 2015).

VI.CONCLUSION

Advancement of technology brings blessings and curses simultaneously which impart challenges to police and other law enforcement organizations to reduce cybercrime victimization.While transnationality of this crime impose huge impediment of investigation, prosecution, and implementation of legal frawork in a certain jurisdiction. Furthermore, huge data, volatile evidence, lack of expert staffs and equipments are major stumbling block of fighting cybercrime by police. However, digital specialism with proactive approaches of policing will lead to minimize the challenges of cyber policing to reduce victimazation. In addition, international cooperation is essential to control this phenomenal technology based crime to underpin a tool for combating cybercrime for the nations. This research will contribute in the existing literature to shape the cybercrime response scholarship. But this study is not beoynd the limitation of empirical observations, which will be the future research endeavor to find the mechanism used by cyber policing organizations to combat cybercrime.

AUTHOUR'S 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]. Al Azzam, Farouq Amhad Faleh (2019). "The adequacy of the international cooperation means for combating cybercrime and ways to modernize it".JANUS.NET e-journal of International Relations, Vol. 10, N.º 1, May-October2019,pp.66-83.

[2]. Alhaboby, Z. A., Barnes, J., Evans, H., & Short, E. (2017).

Challenges facing online research: Experiences from research concerning cyber-victimisation of people with disabilities. *Cyberpsychology, 11*(1Special Issue)

[3]. Ambos, K., & Bock, S. (2017). Brexit and the European criminal justice system - an introduction. *Criminal Law Forum, 28*(2), 191-217.

[4]. Awan, I., & Zempi, I. (2016). The affinity between online and offline anti-muslim hate crime: Dynamics and impacts. *Aggression and Violent Behavior, 27*, 1.

[5]. Bates, P., Smith, S., & Nisbet, R. (2015). Should social care staff be facebook friends with the people they support? *The Journal of Adult Protection, 17*(2), 88-98.

[6]. 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.

[7]. Bojarski, K. (2015). Dealer, hacker, lawyer, spy. modern techniques and legal boundaries ofcounter-cybercrime operations.The European Review of Organised Crime,pp.25-50.

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

[9]. Borko, A., Nehodchenko, V., Volobuieva, O., Kharaberiush, I., & Lohvynenko, Y. Fighting against Cybercrime: Problems and Prospects in Ukraine and the World (2019). Journal of Legal, Ethical and Regulatory Issues, 22(2S). 1–5.

[10]. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3, 77–101.

[11]. Broadhurst, R. and Chang, Y.C. (2012). Cybercrime in Asia: trends and challenges. *Asian Handbook of Criminology*, p.1-26.

[12]. 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.

[13]. 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.

[14]. 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.

[15]. 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.*

[16]. European Commission (2013). Cybersecurity Strategy of the European Union: AnOpen, Safe and Secure Cyberspace. Brussels: European Commission.

[17]. Furnelb, S.M. and Warren, M.J. (1999) 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?', *Computers & Security*, 18 :28-34.

[18]. Gest, T. (2018). What could a new crime commission accomplish? *Criminology and Public Policy, 17*(2), 497-511.

[19]. Harkin, D., Whelan, C. and Chang, L. (2018). 'The challenges facing specialist cyber-crime units: an empirical analysis'. *Police Practice and Research*, 19(6), pp. 519-536.

[20]. Hill, J. B., & Marion, N. E. (2016). Presidential rhetoric on cybercrime: Links to terrorism? *Criminal Justice Studies, 29*(2), 163-177.

[21]. Hunton, P. (2010). Cyber Crime and Security: A New Model of Law Enforcement Investigation. *Policing: A Journal of Policy and Practice*, Volume 4(4), pp.385–395.

[22]. Hunton, P. (2011a). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. Digital Investigation, 7:105-113.

[23]. Hunton, P. (2011b). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Compute r law & Security review, 27 (2011) 61e67

[24]. Jarvis, P., & Earis, R. (2015). Participating in the activities of an organised crime group: The new offence. *The Criminal Law Review,* (10), 766.

[25]. Klettke, B., Hallford, D.J. and Mellor, D.J. (2014) Sexting prevalence and correlates: A systematic literature review, *Clinical Psychology Review*, 34: 44–53.

[26]. Kirby, S., Francis, B., Humphreys, L., & Soothill, K. (2016). Using the UK general offender database as a means to measure and analyse organized crime. *Policing, 39*(1), 78-94.

[27]. Lastdrager, E.E. (2014) Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, **3**:9.

[28]. 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.

[29]. Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers and Security, 72*, 26-59.

[30]. 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.

[31]. Lindsay, J. R. (2017). Restrained by design: The political economy of cybersecurity. *Digital Policy, Regulation and Governance, 19*(6), 493-514.

[32]. Marlow, A. (2014). Thinking about the fall in crime. *Safer Communities, 13*(2), 56-62.

[33]. Mette Eilstrup Sangiovanni Section Editor (2005) Transnational Networks and New Security Threats, *Cambridge Review of International Affairs*, 18:1, 7-13.

[34]. Meyer, F. (2017). The "swiss model" as an option for the future UK-EU relationship. *Criminal Law Forum, 28*(2), 275-299.

[35]. Muaygil, R. (2016). The role of physicians in state-sponsored corporal punishment. *Cambridge Quarterly of Healthcare Ethics, 25*(3), 479-492.

[36]. Naqvi, S. (2018). Challenges of Cryptocurrencies Forensics: A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals. ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security.pp.1-5.

[37]. Ndubueze, P. N., & Igbo, E. U. M. (2014). Third parties and cyber-crime policing in Nigeria: Some reflections. *Policing (Oxford), 8*(1), 59-68.

[38]. Park, O. B., Im, H., & Na, C. (2018). The consequences of traumatic events on resilience among South Korean police officers. *Policing, 41*(1), 144-158.

[39]. Payne, B. K. (2016). Expanding the boundaries of criminal justice: Emphasizing the "S" in the criminal justice sciences through interdisciplinary efforts. *Justice Quarterly, 33*(1), 1-20.

[40]. Phil Kowalick, David Connery & Rick Sarre (2018). Intelligence-sharing in the context of policing transnational serious and organized crime: a note on policy and practice in an Australian setting, Police Practice and Research, 19:6, 596-608.

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

[42]. 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.

[43]. Sa'di, M. M., Kamarudin, A. R., Mohamed, D., & Ramlee, Z. (2015). Authentication of electronic evidence in cybercrime cases based on Malaysian laws. *Pertanika Journal of Social Science and Humanities, 23*(October), 153-168.

[44]. Sampson, F. (2014). Cyberspace: The new frontier for policing? Cyber Crime and Cyber Terrorism Investigator's Handbook, pp.1-10.

[45]. Shelley, L.I.(2003) 'Organized Crime, Terrorism and Cybercrime' in A. Bryden and P. Fluri (eds.) *Security Sector Reform: Institutions, Society and Good Governance* . Nomos Verlagsgesellschaft: Baden-Baden. pp. 303-312.

[46]. 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*.

[47]. Smith, J.A., Mccullough, R., Critchlow,C. and Luke, M. (2017) Proposing an Initiative Research Methodology for LGBTQ+ Youth: Photo-Elicitation and Thematic Analysis, Journal of LGBT Issues in Counseling, 11:4, 271-284.

[48]. Stan Gilmour (2014). Practitioner's insight-Policing Crime and Terrorism in Cyberspace: An Overview. The European Review of Organised Crime, 1(1), 143-159.

[49]. Sun, J., Shih, M., & Hwang, M. (2015). Cases study and analysis of the court judgement of cybercrimes in Taiwan. *International Journal of Law, Crime and Justice*, *43*(4), 412.

[50]. Symantec. Symantec global internet security threat report, trends for 2008, vol. XIV. Symantec Corporation; 2009. Published April 2009.

[51]. van Sliedregt, E. (2016). Command responsibility and cyberattacks. *Journal of Conflict and Security Law*, *21*(3), 505-521.

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

[53]. Wall, D. S. (2017). TOWARDS A CONCEPTUALISATION OF CLOUD (CYBER) CRIME**.** Conference Paper · May 2017.

[54]. Wilkinson, S. (2010). The Modern Policing Environment, in, G. Bammer (ed.) Dealing with uncertainties in policing serious crime. Canberra: ANU E Press.p.213.

[55]. Wright, M. F. (2016). Cyber victimization and psychological adjustment difficulties among adolescents. *Policing*, *39*(3), 536-550.