Copyright © 2018 International Journal of Cyber Criminology – ISSN: 0973-5089
January – June 2018. Vol. 12(1): 316–332. DOI: 10.5281/zenodo.1467931
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Cloaked By Cyber Space: A Legal Response to the Risks of Cyber Stalking in Malaysia

Zaiton Hamin[1] **& Wan Rosalili Wan Rosli**[2]
Universiti Teknologi MARA, Malaysia

Abstract

Cyber stalking generally involves unwarranted, repeated and threatening conduct of the offender via the Internet or social media platforms, which causes fear, distress or alarm to the victim. A qualitative study on the perception of cyber stalking and the adequacy of the anti-stalking law to regulate such crime in Malaysia is somewhat scarce. Hence, this paper seeks to examine cyber stalking risks and the sufficiency of laws to govern such crime and the legal protection afforded to victims. This paper adopts a qualitative methodology, where the data is obtained from eighteen semi-structured interviews conducted with various stakeholders, including the regulators and enforcement officers. Secondary data involves cyber legislation, the Penal Code, and online sources. The findings suggest that cyber stalking risks are often manufactured by the victims, which lead to individual responsibility towards managing and mitigating such risks. The findings have significant implications for lawmakers to either enact specific laws on cyber stalking or amend the Penal Code to include such crime.

Keywords: Cyber stalking, risks, risk society theory, anti-stalking legislation, secondary victimization.

Introduction

In the current electronic era, new offences exist such as cyber bullying, cyber harassment and cyber stalking, which can be committed via information and communication technology (ICT). Such crimes which are committed in cyberspace have extensive social, political and economic implications and may ultimately challenge traditional criminal laws. The International Telecommunications Union (ITU) Key ICT Indicators for the World Statistics, reported that as at October 2017, individuals using the Internet have increased to more than 830 million people (ITU, 2017). The recent Internet World Statistics (2018) reported that 48.7 percent of Internet users in the world originate from the Asian region. Moreover, the same 2018 Report stated that in 104 countries around the world, more than 80 percent of the youth population is online. This explosion ICT usage has led to hybrid crimes, in which cyber stalking or cyber harassment is one of

[1] Associate Professor, Faculty of Law, University Teknologi MARA, Shah Alam, Selangor, Malaysia. Email: zaiton303@salam.uitm.edu.my
[2] Senior Lecturer, Faculty of Law, University Teknologi MARA, Shah Alam, Selangor, Malaysia. Email: rosalili@salam.uitm.edu.my

them. Wall (2005) suggests that hybrid crimes are crimes where the Internet has opened up new opportunities for existing criminal activities. Such crimes are crimes that can be committed with or without the Internet, but it increases in severity through the use of information technology such as cyber stalking, which could transcend from cyberspace to the real world and vice versa (Norden, 2013).

In the global context, the extant literature on stalking and cyber stalking has been published (Meloy, 1999; Medlin, 2002; Lamplugh, 2003; Ngo, 2013). Research on traditional stalking showed that several trends and characteristics of crime are emerging. For example, rather than older people, younger persons are vulnerable to the risk of becoming victims of stalking. (Aa, 2011; Purcell, Pathe' & Mullen, 2002). Stalking is also generally accepted to be a widespread problem with serious social, psychological, medical and economic impediments (Owen, 2016; Fox, Nobles & Fisher, 2011). Literature also suggests that as opposed to traditional stalking, the research on cyber stalking is not as extensive as the former and is relatively small (Mutawa, 2016; Noble, Fox & Fisher, 2014; Reyns, Henson & Fisher, 2015; Tavani & Grodzinsky, 2002). Early literature on cyber stalking can be found in the late 1990's (Elison & Akdeniz, 1998). However, it is only in the last five years that research on cyber stalking victimization has started to progress (Reyns, Henson & Fisher, 2015). Early and more recent literature agrees that cyber stalkers use technology to hide their identities and to use the anonymity of the Internet to quickly target their victims without the need for any physical contact (Mutawa, 2016; Reyns, 2014; Ashcroft, 2001).

The recent legal literature on cyber-stalking focuses mainly on the effectiveness and the implications of the anti-stalking laws. For instance, Knight (2014) asserts that in the United States, offenders would often contact their victims after their prosecution and as a result, the recidivism rate of stalking and cyber-stalking increases to sixty percent. Other jurisdictions such as the UK and New Zealand enacted their anti-stalking laws in 1997 in the form of the Protection from Harassment Act 1997 and the New Zealand Harassment Act 1997 respectively. These statutes cover both criminal and civil harassment (CCPL, 2013). Singapore followed the UK's footsteps by criminalising cyber stalking and created the Protection from Harassment Act in 2014 (Hamin & Wan Rosli, 2016). The anti-stalking laws in the UK, Singapore, and the United States offer various protections for the stalking victims such as protection order, injunction, damages and restraining orders (Middlemiss, 2009; Cheong, 2014).

The extant literature on cyber stalking indicates that the veil of anonymity attracts stalkers to stalk their victims in cyberspace (Reyns, 2011; Heinrich, 2015; Middlemiss, 2014). Leong and Morando (2015), Heinrich (2015), Reyns (2011) and Tavani and Grodzinsky (2002), suggest that cyber stalkers can operate anonymously or pseudonymously while online, and they can stalk one or more individuals from the comfort of their home without having to venture out into the physical world to commit such crimes. Studies have shown that women are most likely to be stalked rather than men in traditional stalking and cyber stalking, which implies that such crime, is mainly a gender-motivated crime towards women committed by men (Godwin, 2003, Medlin, 2002, Reyns, 2010, Nobles, 2013).

The Malaysian literature on the criminalisation and the legal protection available for cyber stalking victims is rather scarce. Recent available studies indicate that the traditional criminal law in the Penal Code and cyber law in the shape of the Communication and Multimedia Act 1998 are the legal responses to cyber stalking in Malaysia (Hamin & Wan

Rosli, 2017). Other local literature highlights the unwillingness of female cyber stalking victims reporting on the crimes inflicted upon them by the police (Haron, 2010). Furthermore, Cyber Security Malaysia states that the problem posed by cyber stalking is peripheral as the actual number of the victims is higher because not all victims are willing to come forward with their reports (Cyber Security Malaysia, 2010). The recent statistics compiled by the Malaysian Computer Emergency Response Team (MyCERT) on cyber harassment incidences in Malaysia shows the numbers have tripled in the last ten years (MyCERT, 2017). The latest figure of such crimes reported by MyCERT for the first half of the year 2018 involves 142 cases. This indicates an increase in the number of cases as 560 cases were reported in 2017 and 529 cases in 2016. However, there is a lack of qualitative study on the perception of cyber stalking and the adequacy of the anti-stalking law to regulate such a crime. As such, this paper seeks to examine the perspective into such a crime and identify the sufficiency of anti-stalking law and the legal protection afforded to cyber stalking victims in Malaysia. Hence, this paper intends to fill in the gaps in the legal literature and research on anti-cyber-stalking law.

Literature Review

The advent and pervasiveness of technology have resulted in a broad range of activities including simultaneous sharing of information, pictures, making comments, instant messaging to friends and families and also engaging in social media (Leong & Morando, 2015). With such technological development, the magnitudes of cyber harassment and cyber stalking are rather extensive (Leong & Morando, 2015). Early literature defines stalking as a crime involving acts or behaviors of pursuit which is done over time that is threatening and potentially dangerous towards the victim (Meloy, 1998). Similarly, Thomas (1993) argues that the main elements of stalking involve the repetitive and threatening conduct of the offender.

Cyber stalking that has emerged from the conventional stalking may now be committed through any technological devices that can be connected via the Internet (Heinrich, 2015). The literature suggests that such a crime has evolved tremendously in terms of the technological medium of the crime commission and the types of illegal activities involved. Such a crime may be committed via the Internet involving unsolicited communication through emails, chat rooms, smart phones, mobile applications, SMS, social networking sites, and forums. The nature of stalking could range from repeated, threatening, or malicious information sharing or in extreme cases the luring or enticing of victims into dangerous liaisons (Reyns, 2015). Similarly, Piotrowski (2012) argues that cyber stalking involves the repeated and persistent attempt by one individual (the stalker), to harass another person (the victim), using the Internet or another open network. Local literature such as Haron (2010) divides the nature of the activities of cyber stalking into four types involving harassing, threatening, intimidating and impersonating the victim. Smoker and March (2017) contend that with the development of technology coupled with the susceptibility for uninhibited behavior within the online environment, cyber stalking has become a norm due to the availability of greater avenues of communication and open access to information.

The literature suggests that the architecture of the Internet allows cyber stalkers to operate anonymously or pseudonymously while online, and they could stalk one or more victims from the comfort of their homes. For instance, Dhillon, Challa, and Smith (2016)

contend that because of the anonymity of the Internet environment, cyber stalking has taken a new form with an unprecedented scope. Through various technological applications, stalkers could stalk multiple victims simultaneously even when the victims reside in different states and countries from the stalkers (Hamin & Wan Rosli, 2017; Tavani & Grodzinsky, 2002). Cyber stalkers could easily acquire personal information about their victims due to the availability of such information that is readily accessible from electronic databases via online search engines (Heinrich, 2015). In most cases, the victims would never discover the true identity of their cyber stalkers (Bocij & McFarlane, 2002).

Recent literature focuses on the trans-nationality of such crime in which cyber stalking is considered as a trans-border crime. Jaishankar (2011) highlights that cyber stalking can also happen to victims that live in states and countries that are geographically distant from the stalkers. According to Dillon, Challa and Smith (2016), cyber stalking ignites jurisdictional issues as it is a cross-border crime. Prior qualitative studies focus on technologies in intimate partner stalking (Reyns, 2015), the impact of social network technology in the commission of cyber stalking (Haron, 2010) and qualitative analysis on the cyber stalking legislation in the UK (Maple, 2011) and the United States (Hazelwood, 2013).

Extant literature suggests that the impact of cyber stalking may be more dangerous and prevalent than traditional stalking. Such impact may be due to the various crime stimuli of the Internet that provide tremendous opportunities to utilise advanced computer programs (Aa, 2011; Mutawa, 2016). Cyber stalkers face no difficulties in finding their victims which can be done with a click of a button. The chances of being confronted with their actions are negligible as they would conceal their identities, alter critical data, move and delete information within seconds and destroy the evidence (Aa, 2011). Rawlinson (2015) explains that in Australia, 98 percent of domestic violence victims have also experienced cyber stalking. Al-Khateeb and Epiphaniou (2016) argue that more than 38 percent of cyber stalking victims fear that the offensive behavior of the offenders online would develop into a face-to-face confrontation. Tokunaga and Aune (2015) suggest that the threat of cyber stalking has become imminent and state that about 20 percent to 40 percent of Internet users are victimized through cyber stalking. The US Bureau of Justice Statistics (2017) reports that within a year, an estimated 14 in every 1,000 persons aged 18 or older may become victims of cyber stalking.

The Risks of Technological Crime

The variety of the risks of victimization of cyber stalking has also been documented. For instance, Perry (2012) explains that the first risk is the physical danger to the victim through digital footprints in which the cyber stalkers could obtain the victim's current location and commit physical assault or even murder. Secondly, there is the risk of contact information whereby the cyber stalker could find the contact details of the victim's home, work, family and even friends (Perry, 2012). Thirdly, through data gathering, the cyber stalker could gain more information about the victim and could deceive the victim through social engineering. Similarly, Paladin (2016) states that cyber stalkers could always gather their data to be able to have access to personal information about the victims and immediately act upon it directly or indirectly using people who are close to the victim. Fourthly, the cyber stalker could gather sufficient information about the victim and commit identity theft (Perry, 2012). Lastly, the cyber stalker could take over the victim's

account and use it to harass the victim personally and financially; for example, by penetrating into the victim's bank account and sending a false e-mail (Perry, 2012). The use of Spyware that is readily available nowadays, at a meager price or even with a free download on the Internet has enabled the stalkers to track their victims and gather information on them (Paladin, 2012).

Risk Society Theory

Giddens (1990) explains risk society as a society increasingly preoccupied with the future and safety that generate a notion of risks. Beck (1992) a principal writer of the risk society theory defines risk society as a systematic way of dealing with hazards and insecurities induced and introduced by modernization. Beck (1992) and Giddens (1990) approached the risk society theory from the perspective of modernity, in which a society is seen to be vastly more dynamic than any previous society and lives in the future rather than the past. Beck (1992) also defines modernisation as surges of technological rationalisation and changes in work and organisation, which include changes in lifestyle and forms of love, societal characteristics and ordinary biographies. Other changes include a change in structures of power and influence in the ways of political repression and participation in views of reality and norms of knowledge. Giddens (1990) further explains that the risks in modern societies multiply with the increasing complexification of governance and technological control, and in the societal systems of production and consumption.

Both sociologists argue that humans have always been exposed to a level of risk such as natural disasters that are perceived to be caused by non-human forces. Giddens (1990) and Becks (1992) suggest that in modern society, humans are exposed to new risks such as pollution and crime which is the result of the modernisation process. Giddens (1990) defines these two types of risks as external risks and manufactured risks. Manufactured risks are identified as a high-level human agency involved in producing and mitigating such risks.

The risk society has since evolved into a world risk society, which involves the masses. Such a world risk society has led to an increase in online relationships with those who are physically absent (Castells et al., 2002). Social relations are generated online and have become globalised with friends from all over the world. The public is aware of the risks that come with the changing climate of globalisation such as cyber stalking, identity theft, cyber fraud, and cyber pornography. Beck (1992) contends that there is a strange paradox in modern society whereby risks are increasing due to technology and advancement of science rather than being abated by technological progress. The world risk society carries a high degree of risks which is so enormous that it transcends time and place on a global scale where the control of risks seems impossible (Jackson et al., 2004). The ultimate risks in cyber crime are that one is unaware of the risks which occur with a single click of a mouse (Jackson et al., 2004). Cyber risk mitigation would involve equipping oneself with weapons of software and knowledge as in a virtual environment; the perpetrator uses the cloak of anonymity to hide effectively (Jackson et al., 2004). Technological changes have led to the shifting of ways of communication, where rather than meeting face-to-face technology has minimised the gap between people across the world with just a single click of a mouse (Jackson, 2002). The world risk society and technological developments have led to the increasing vulnerability towards human-made risks (Giddens, 1999).

Regulating Cyber Stalking

In the current Malaysian legal landscape, the law that governs cyber stalking is the Penal Code and the Communication and Multimedia Act 1998 (hereinafter the CMA 1998). Section 503 and section 506 of the Penal code which provide for criminal intimidation may also govern cyber stalking. Criminal intimidation is committed when a person threatens another with any injury to his person with the intent to cause alarm to that person. The punishment for criminal intimidation under section 506 is imprisonment for a term that may extend to two years or fine or both. To date, 11 cases of criminal intimidation have been prosecuted in the courts, but none of these cases involve stalking or cyber stalking.

In the Singaporean case of PP v Colin Mak Yew Loong (2013, Unreported), the defendant had been sending the victim threatening e-mails and voice messages for more than six years. The harassment included threats of violence by using an AK-47 rifle and a lead pipe. The perpetrator was charged with criminal intimidation and was sentenced to three years of imprisonment and fined SGD5000. This case took place during the pre-implementation of the Protection from Harassment Act 2014 (PHA 2014) in Singapore. If the case were decided in Malaysia, the same decision would apply since criminal intimidation in Singapore is *in parimateria* (the same subject) with section 503 of the Malaysian Penal Code. However, if the case were decided post-PHA 2014, the defendant would have been charged with cyber stalking under section 7 of the PHA 2014 whereby on conviction the accused would be liable for a fine not exceeding SGD 5,000 and imprisonment not exceeding the term or twelve months or both. If the harassment towards the victim continues, the accused may also be charged with a subsequent offense with a maximum fine of SGD 10, 000 or a maximum jail term of two years or both.

Section 233 of the CMA 1998 governs the improper use of network facilities or network services. A person who commits an offense under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding one year or both. A person can also be further fined one thousand Malaysian Ringgit for every day during which the offence continued after the accused is convicted. However, no such cases relating to cyber stalking have ever been prosecuted under this section. The only case that was reported in this section involved the case of Rutinin b Suhaimin v PP (2014) 5 MLJ 282 whereby the accused published the comment that 'Sultan Perak sudahgila !!!!!' (Sultan of Perak is crazy!!!!!) via his Internet account. The decision, in this case, was overturned by the higher court as there was evidence that the accused's account could have been accessed by other persons as his IP line was on continuous login the entire day on the day the crime was committed. Despite the utility of section 233 in governing cyber stalking, it does not provide the necessary protection for the victims under the protection order, restraining order, injunction and civil remedies which are provided under the Protection from Harassment Act 1997 (PHA1997) in England and Wales. Also, this section does not identify or define the acts and behaviors that constitute cyber stalking or provide any instances of the impact of the stalkers' behavior on the victim such as those provided under section 2A and 4A of the PHA 1997.

Methodology

In focusing on cyber stalking as a risk to be managed and observing the adequacy of the current law and legal protection for victims, this research employed a qualitative analysis. This methodology was chosen as it would provide a greater understanding of the social

phenomena to gain an in-depth, intense and a holistic overview of the study (Silverman, 2013). Hence, such a methodology would enable the researcher to explore the views of the respondents on the criminalisation and the legal protection of victims of cyber stalking in Malaysia. For this paper, the findings were based on data collection via primary and secondary data, and this stage was divided into two phases. The first phase of the data collection involved reviewing all the relevant literature on the subject matter via library-based search (Bell, 1987) on cyber stalking and the gendered nature of the crime. The primary sources included the Communication and Multimedia Act 1998 and the Penal Code while the secondary sources include textbooks, academic journal articles, government reports, newspaper articles and online databases and sources.

The second phase of the data collection involved fieldwork, in which the primary data was mainly generated from face-to-face semi-structured interviews with eighteen respondents. In-depth interviews are used in this study to capture the respondents' perception and perspectives that are able to reconstruct the meanings attributed to their experiences and events (Scheibelhofer, 2008). Such interviews with the respondents are crucial to obtaining more detail answers when giving their views and opinions (Scheibelhofer, 2008). According to Bryman (2007), the in-depth qualitative interviews would be the most appropriate method for collecting the data for the present study as this research is interested in knowing and understanding the respondents' point of views. The interview method was chosen as it provided the researcher with the opportunity to explore the respondents' opinions of an issue in depth, rather than to merely test their knowledge on the subject matter or to only categorize their information (Matt, 2000).

A total number of eighteen respondents were interviewed in this study. Out of these, three respondents were police officers from the Cybercrime Unit of the Royal Malaysian Police, two officers from Cyber Security Malaysia, two members from the Bar Council Malaysia, two deputy public prosecutors, two legal practitioners who specialises in cyber law and one member of the WAO, two officers from the Multimedia and Communication Commission and one cyber stalking victim. This study is mainly interested in the respondents' narratives on their perception of cyber stalking and the laws governing cyber stalking. The reliability of these narratives was strengthened via an independent triangulation with the semi-structured interview data obtained from two officers from the Ministry of Communication and one officer from the Multimedia and the Ministry of Women, Family and Community Development respectively. Out of the eighteen interviews, twelve were men and six were women. Bertaux (1981) and Guest, Bunce, and Johnson (2006) suggest that fifteen respondents would be the minimum sample size for such qualitative research to reach the point of saturation. The number of samples is based on the contention of Crouch and McKenzie that twenty respondents in a qualitative study help build and maintain a close relationship and improve open and frank exchange of information (Crouch & McKenzie, 2006).

The sampling method in this research incorporated a purposive sampling, which means that the respondents were selected because they were likely to generate pertinent data for the research (Crouch & McKenzie, 2006). The chosen respondents represent various stakeholders that have been identified and selected based on their occupational roles as they have a portfolio very close to the research topic and are believed to be able to provide relevant data. Access was gained through email, telephone and also through the gatekeepers within the relevant institution. All the potential respondents were given a set

of interview questions at the time of access to help them decide whether or not to participate in the research.

In this research, the time spent on the fieldwork and such interviews was two months. Each interview lasted between twenty-five minutes to an hour at the respondents' workplaces. Prior to the interview session, the objectives of the research and other information were explained in simple language to every respondent. Such information included why they were being interviewed, what would be done with the information they provided and what are the potential outcomes of the research. The interview began with informal discussions by selecting a topic of interest and once a relationship had been developed, the researcher started with the semi-structured interview questions to guide the discussion. Harvey (2011) states that establishing a rapport and a relaxed environment are crucial to collecting good quality data.

In relation to the ethical matters, this research did not have to go through the Ethics Committee of the University, given that no clinical trials are involved. The researcher, however, has taken due reasonable care and diligence in maintaining the importance of ethics while conducting this study. All the respondents have been given a fair opportunity and encouraged to raise any questions and concerns during the interview.

In analysing the primary data, all the interviews were digitally recorded, and their contents transcribed and analysed using the Atlas.ti version 8 qualitative research software. Such data analysis was conducted through thematic and content analysis, in which observations and interview transcripts from the semi-structured interviews were examined (Seidman, 2006). The process consisted of creating codes and categories, taking into account the themes and then analysing the respondents' perceptions and experiences, along with the existing literature review. Once the codes were added to the project in Atlas.ti, the code was approached deductively and then linked to the important segments in the data. As the data were coded deductively, the researcher had also come across new themes and ideas; hence, the researcher needed to code the data inductively (Jesson, 2011). The coding process was essential in segmenting the data segments relevant to each of the codes identified for the research. Once the list of codes was generated, it contained both the deductive codes as well as the inductive codes.

Semantic validation through primary data quotation may be useful to verify the interpretations made within the content analysis. The descriptions of the respondents' views suggest the way in which the narratives of the perceptions of cyber stalking and the law governing such crime may constitute the construction of its realities. As such, despite the lack of generalisation of the findings, the data are deemed valid and reliable, presenting insights on how cyber stalking is a risk that needs to be managed and there are inadequacies in the current legal framework governing cyber stalking.

Findings

Cyber stalking as a Risk to be Managed

The research revealed that cyber stalking is perceived as a risk to be managed rather than a crime to be punished. The majority of the respondents believed that such risks were generated due to new ways of communicating and rapid technological changes that are occurring. A respondent commented that:

> I think the risk of cyber stalking is on the rise because of the way people are communicating now... through the online medium such as the SMS, WhatsApp, and other social media accounts.

Another respondent suggested that:

> It is how we use technology and now more technological platforms are available to communicate. Back in the old days, if I want to stalk you, I have to follow you physically.

Similarly, one respondent from a regulatory body commented that:

> Cyber stalking is a greater risk nowadays because of the influence of social media.

Manufacturing the risks

The findings revealed that the majority of the respondents believed that the victims might have contributed to the creation or manufacture of the risks of cyber stalking by having access to the Internet. One respondent commented that:

> When people have access to the Internet and create Facebook accounts, of course, there is a risk of cyber stalking.

Similarly, another respondent commented that:

> Cyber stalking risks may happen as more and more users are connected to the Internet… some may have good or even bad intentions when using the Internet.

The majority of the respondents suggested that another way in which the risk of cyber stalking was manufactured was through over sharing of personal information online or in social media applications. One respondent cited that:

> This risk of cyber stalking may exist due to our eagerness to share everything online...

Similarly, another respondent remarked:

> In this life and especially when communicating online, we cannot share everything with others... if what we share is harmful to us, it's best not to share!

Secondary Victimisation in Cyber Stalking

The findings suggested that on the perception of cyber stalking, there was ambivalence on the seriousness of cyber stalking. Despite understanding the nature of cyber stalking, the majority of the respondents were either unaware of the severity of the offense or were engaged in what could be considered secondary victimisation of cyber stalking. One respondent stated that:

> I believe that when someone sends you SMS or WhatsApp or e-mail message many times in a day threatening you, that is cyber stalking…it is a serious crime… but I'm not too sure how many Malaysian are experiencing this.

Minimizing the threat

Some of the respondents, in particular, the regulators, considered such an offence lightly and suggested that a simple solution could be used to tackle the issue. A respondent stated that:

> It's easy. What the victim needs is only to close her account. She could also create a new account and make sure that the stalker is no more in the friend's list.

Another respondent suggested that:

> If you just grow up and ignore the stalkers, you'll be OK…

Victim-blaming mentality

Some of the respondents blamed victims for exposing themselves to cyber stalkers. A respondent from the regulatory body remarked that:

> If you reveal everything to the public… then it's your problem…

On a similar assertion of victim-blaming, another respondent argued that:

> You would not reveal anything about yourself to the public in real life without cause, and similarly, there is no reason for you to do so to an anonymous individual on the Internet...

Gendered Nature of Crime

The findings revealed that the majority of the respondents thought that the perpetrators of the crime were not solely men and that they believed that both men and women were potential cyber stalkers. A respondent from the regulatory body remarked that:

> The stalkers can be anyone, not necessarily men…

Such a belief was apparent based on the equal percentage of Internet involving both genders. Another respondent from the same regulatory body suggested that:

> In Malaysia, our Internet users are almost 50-50...54/46 meaning we have equal number female and male users…I don't think the crime is limited to a specific gender because technology is gender neutral.

Adequacy of Law and Legal Protection for Victims

The findings suggested paradoxical views on the adequacy of the law and the legal protection for the victims of cyber stalking. A respondent from a legal firm remarked that:

> Cyber stalking is already a crime under the existing law… similar reliefs are available under the Domestic Violence Act, and under the Rules of Court 2012 and by common law (e.g., *quia*time injunctions) …

Another respondent also from a regulatory body highlighted that the current law is sufficient due to the availability of an existing legal framework involving four legislations that could govern cyber stalking. He commented that:

> We have the Defamation Act, the Sedition Act, Section 233 of the CMA and the Penal Code. So, all these laws may cover cyber stalking.

Despite such belief in the sufficiency of the current law, some respondents perceived that it is now suitable for Malaysia to have a specific anti-stalking law akin to Singapore and England and Wales. A respondent from a regulatory body commented that:

> We need to establish a specific anti-stalking law that is similar to the law and the legal protection available in the UK.

Governing the Risks of Cyber Stalking

The findings indicated that some of the respondents believed that cyber stalking risks need to be mitigated or governed to protect themselves online. Hence, they offered some possible modalities to mitigate or regulate the risk of cyber stalking such as lodging a police report, using technology to block the stalkers, creating awareness campaigns involving the regulators and imposing self-regulation when using the Internet.

Reporting to the police

The findings revealed that the majority of the respondents suggested that lodging a police report would be an appropriate response to the risk of cyber stalking. A respondent from a regulatory body remarked that:

> We advise the victims who reported to us to lodge a police report at any nearby police station… and they must provide all pertinent and relevant information to the police.

Technology as governing modality

Further means of mitigating the risk of cyber stalking would be through technology namely by use of password authentication, blocking technology and by using security software like Norton security software which prevents spyware from entering the victim's computer. A respondent stated that:

> Computer users are usually excited about a new IT application without taking care of online security and safety. One example of protection against cyber stalking is to block the stalker from your hand phone, Facebook, Instagram and Twitter accounts.

Awareness campaigns and education

The findings indicated that a top-down approach in the form of the awareness campaigns and exposure through education be made mandatory by regulators for computer users to minimize their risks of cyber stalking. One respondent for a regulatory body asserted that:

> We have conducted several road shows to make Malaysians aware of the risk of cyber stalking.

Similarly, another respondent agreed that creating awareness and exposing issues related to cyber stalking through education would be beneficial in the reduction of such risks. A respondent commented that:

> Mitigation of such risks and crime would involve educating computer users and creating awareness on the dangers of the Internet…

Individual responsibility

The findings suggested that individual responsibility and the preference for private justice are evident from the narratives of the respondents. Such responsibility would involve not only managing their risks of cyber stalking but also to assume some of the blame for the failure to manage such risks. The majority of the respondents perceived that computer users would have to protect themselves against such risks or crime as the regulators seemed to place such responsibility upon them. One respondent from a regulatory body commented that:

> Via education and awareness campaigns, we have emphasized that computer users must regulate their usage and protect themselves.

A similar view was expressed by another respondent who commented that:

> Computer users need to be aware of the risk of using computers … one involving cyber stalking and need to know how to protect against stalkers…

Discussion

The findings revealed that cyber stalking is a risk to be managed, which confirms Beck's risk-society theory that underlines the changes happening within contemporary social life such as technological changes, declining influence of customs and tradition and democratization of personal relations (Beck, 1992). The extant literature further suggests in the past decade, globalization and technological advances have led to the rampancy of cyber stalking (Perry, 2012; Paladin, 2016; Dhillon, Challa, & Smith, 2016; Hamin & Wan Rosli, 2017).

With regards to the manufacturing of risks by the victims, the findings suggested that victims have contributed to the creation of the risks of cyber stalking by over sharing personal information online and by having unlimited access to the Internet. These findings confirmed the literature on the rampancy of cyber stalking which may be due to the voluminous information available online (Leong & Morando, 2015; Heinrich, 2015; Reyns, 2015). The online environment also provides a conducive setting for cyber stalkers to prey on their victims (Smoeker & March 2017; Hamin & Wan Rosli, 2017).

The findings on the governance of the risks of cyber stalking suggested that reporting of cyber stalking ordeal to the authorities or police was favorable. However, such views are contrary to literature which indicates that victims do not usually report such crime immediately to the police (Patel, 2013; McNamara & Marsil, 2013). Such reluctance is attributed to the lack of positive response from the authorities (Hamin & Wan Rosli, 2017).

Furthermore, the findings indicate that other modalities of governance such as technology, awareness via campaign and education by regulators play significant roles in

governing such risk. This view confirms the literature that supports other governing modalities apart from the law that may be essential in governing such crime (Paladin, 2016; Hamin & Wan Rosli, 2017; Heinrich, 2015).

The narration of the findings above also suggests that mitigating the risks needs to be undertaken by victims of cyber stalking themselves. In the move towards a world risk society in which the magnitude of the risks is more significant, mitigation of risk is paramount to protect computer users from being victims of crime, in particular, cyber stalking (Jaishankar, 2011). Interestingly, the findings indicate that the regulators seemed to place individual responsibility onto computer users, in particular, the victim, in managing his or her risks. Also, victims were blamed for failure in managing their cyber stalking risks. Such perception is consistent with O'Malley's notion of "privatized prudentialism" and Garland's responsibilisation strategy which suggest that rather than formal criminal justice institutions, informal controls within the civil society should provide order and security (Garland, 1999).

With regards to secondary victimisation in cyber stalking, the findings indicated that there was inconsistency in the perception of cyber stalking. The said crime was perceived to be severe but on the other hand, the apathy shown to the victims was surprising. Evidence suggested that the majority of the respondents were not fully aware of the effects of cyber stalking. Interestingly, the nonchalant responses to such crime by closing the victim's account or ignoring the stalker further indicated lack of knowledge of the seriousness of the crime and its inherent dangers (Tokunaga & Aune, 2015; Rawlinson, 2015; US Bureau of Justice Statistics, 2017)

The above findings indicated that the majority of the respondents believed that cyber stalking was not a gender-motivated crime and that anyone could be a cyber stalker. Interestingly, such belief may be due to the equal percentage of Internet users between the genders in Malaysia and (MCMC, 2017). Such a view is contrary to the above-mentioned current literature which shows that men are the more likely perpetrator than women (The Bureau of Justice Statistics (2017); the British Office for National Statistics, 2015; Godwin, 2003; Reyns, 2012; Aa, 2012). Similarly, the findings seem to disprove the findings in the Strategy and Policy Directorate research (2014) that women are more vulnerable to the victimization of cyber stalking rather than men.

With regards to the adequacy of the law and legal protection for cyber stalking victims, the findings again indicated that paradoxical perception exists amongst the respondents. While some of the respondents believed that a specific law on cyber stalking was an illusion, there was also favoritism on a specific law modeled on that in England and Wales with some legal protections provided within. Such ambivalence on the adequacy of the law and its legal protection seemed to be contrary to the international and local literature mentioned above on the sufficiency of the law dealing with such crime (Hamin & Wan Rosli, 2017; Mutawa et al., 2016). However, one respondent lamented that even if there is a need for a specific law governing cyber stalking, the implementation would be challenging given the current social and legal landscape.

Conclusion

The findings reveal that cyber stalking is not merely a punishable crime but also a risk to be managed. Victims of such crime or risks are believed to be responsible for manufacturing such risk by having unlimited access to the Internet and by over sharing

personal information in social media applications. Apart from that, the findings indicate that secondary victimisation is in existence in which, threat minimisation and victim-blaming mentality are common. Also, contrary to the extant literature, the findings showcase that cyber stalking is not considered as a gendered crime. Importantly, the findings suggest the paradox of the sufficiency of the law and its attendant legal protection for the victims. Furthermore, it was found that other modalities such as reporting the matter to the authorities, exploiting technological software to block the stalkers and conducting awareness campaign are essential to governing the risks of cyber stalking. The findings also indicate that individual responsibility and the preference for private justice are evident corresponding to Garland's responsibilisation strategy and also O'Malley's privatised prudentialism.

The research has several implications for various stakeholders. Firstly, the lawmakers or the government should introduce specific provisions in the Penal Code. Alternatively, the government should create a new anti-stalking legislation which is more comprehensive, and which would provide adequate legal protection for victims akin to the laws in England and Wales and Singapore. Secondly, the regulators should enforce section 233 of the Communication and Multimedia Act 1998 to prosecute cyber stalkers. Victims of such crime should be afforded criminal law protection and should not be burdened with the individual responsibility to protect them. Lastly, the implication for computer users is that they need to implement bottom-up approach by adopting specific security measures via technology to minimise cyber stalking risks. Going beyond this qualitative research, future research could be conducted via mixed-method approach on the effectiveness of the current legal framework or a comparative analysis be made on the law in Malaysia and other jurisdictions such as England and Singapore or Australia in which the anti-stalking legislation is well established.

Limitations

In completing the study, there are several limitations faced by the researchers, particularly during the fieldwork. First, the access issue involving the approval and consent from the gatekeepers is the Ministry of Communications and Multimedia and the Ministry of Women, Family and Community Development, which took one month to obtain. Another limitation is the willingness of the respondents to participate in the semi-structured interviews. One interview was deferred several times due to the busy schedule of the respondent. Time management and planning with proper appointments with the respondents are crucial considerations in this research. Finally, the researcher acknowledges that a large number of interviews in the study certainly lead to the use of time and resources in the process of contacting the respondents, arranging the appointments, travelling, changing plans, transcribing the interviews and analysing the primary data. As Creswell (2013) points out, conducting qualitative research needs a strong commitment and demands time and resources for the researcher to concentrate in the field study as well as some other challenges especially when the study relates to human participants.

Acknowledgement

This work was supported by research grant FRGS/1/2016/SSI10/UITM/02/5 by the Research Management Centre, University Teknologi MARA, Shah Alam, Selangor.

References

Aa, S. (2011). International (cyber) Stalking. In: R. M. Letschert, & J. J. M. van Dijk (Eds.). *The new faces of victimhood: globalization, transnational crimes and victim rights* (pp. 191-213).

Al-Khateeb, H., & Epiphaniou, G. (2016). How technology can mitigate and counteract cyberstalking and online grooming. *Computer & Security Journal,* 14-18.

Bell, J. (1987). *Doing Your Research Project – A Guide for First-Time Researchers in Education and Social Science.* Philadelphia: Open University Press.

Bertaux, D. (1981). *From the Life-History Approach to the Transformation of Sociological Practice.* In: Biography and Society: The Life History Approach in the Social Sciences (pp. 29–45). London: Sage.

Beck, U. (1992).*Risk Society: Towards a New Modernity.* New Delhi: Sage. (Translated from the German Risikogesellschaft) 1986.

Bureau of Justice Statistics (2017). *Stalking and Cyberstalking.* Office of Justice programs. Retrieved from https://www.bjs.gov/index.cfm?ty=tp&tid=973.

Bryman, A. (2007). The Research Question in Social Research: What is the Role? *International Journal of Social Research Methodology, 10*(1), 5-20.

Bocij, P., & Mcfarlane, L. (2002). Online Harassment: Towards a Definition of Cyberstalking. *Prison Service Journal,* 139, 31-38.

Castells, M, & Pekka, H. (2002). *The Information Society and the Welfare State: The Finnish Model.* Oxford UP: Oxford.

Crouch, M., & McKenzie, H. (2006). The Logic of Small Samples in Interview-based Qualitative Research. *Social Science Information, 45*(4), 483-499.

Cybersecurity Malaysia (2010). *Cyberstalking a serious Threat.* Retrieved from http://cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1853/index.html.

Dhillon, G., Challa, C., & Smith, K. (2016). *Defining Objectives for Preventing Cyberstalking* (pp. 76-87). Presented at the IFIP International Information Security and Privacy Conference. Belgium: Springer International Publishing.

Giddens, A. (1999). Risk and Responsibility. *Modern Law Review, 62*(1), 1-10.

Giddens, A. (1990). *Consequences of Modernity.* Cambridge: Polity Press.

Godwin, M. (2013). *Cyber Rights: Defending Free Speech in the Digital Age.* The MIT Press: Cambridge.

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods, 18*(1), 59-82.

Hamin, Z., & WanRosli, W. R. (2017). Managing Cyberstalking in Electronic Workplaces, *Advance Science Letter*, *23*(8).

Hamin, Z., & Wan Rosli, W. R. (2017). *Scent of a Woman: The Gendered Crime of Cyberstalking.* Presented at the UUM International Legal Conference (UUM ILC 2017) (Indexed), UUM Sintok, Kedah, Malaysia.

Harvey, W. S. (2011). Strategies for Conducting Elite Interviews. *Qualitative Research*, *11*(4), 431-441.

Haron, H., & Yusof, F. (2010). *Cyberstalking: The Social Impact of Social Networking Technology.* Presented at the International Conference on Education and Management Technology (ICEMT 2010).

Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology*, 7(2), 155.

Heinrich, P. (2015). Generation iStalk: An Examination of the Prior Relationship between Victim of Stalking and Offenders. *Theses, Dissertations and Capstones*, Paper 917.

Internet World Statistics (2018). *Internet Users in the World by Regions*. Retrieved from https://www.internetworldstats.com/stats.htm.

International Telecommunication Union (2017). *ICT Facts and Figures 2017*. Retrieved fromhttps://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf.

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*. Florida: Taylor & Francis Group.

Jesson, J., Matheson, L., Lacey, F. M. (2011). *Doing Your Literature Review: Traditional and Systematic Techniques*. Cambridge: Sage. p. 9.

Knight, M. (2015). Stalking and Cyberstalking in the United States and Rural South Dakota: Twenty-Four Years after the First Legislation. *South Dakota Law Review,* 59 S.D.L.REV.392.

Lamplugh, D., & Infield, P. (2003). Harmonising Anti-Stalking Laws. *The George Washington International Law Review,* 34, 853.

Leong, L., & Morando, J. (2015). Communication in Cyberspace. University of Denver Sturm College of Law, *Legal Research Paper Series*. Working Paper No. 15-11.

Logan, T. (2010). *Research on partner stalking: Putting the pieces together*. Lexington, KY: University of Kentucky, Department of Behavioural Science & Centre on Drug and Alcohol Research. National Institute of Justice.

MCMC (2017). Internet Users Survey 2017. Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-Internet-Users-Survey-2017.pdf.

McNamara, C. L., & Marsil, D. (2012). The prevalence of stalking among college students: The disparity between researcher-and self-identified victimization. *Journal of American College Health,* 60(2), 168-174.

Medlin, A. N. (2002). Stalking to Cyberstalking, a Problem Caused by the Internet. *Law and the Internet*, Fall 2002 papers, Georgia State University College of Law, 140 Decatur St., Atlanta, Georgia 30303 http://gsulaw.gsu.edu/lawand/papers/fa02/medlin.

Meloy, J. (1998). *The Psychology of Stalking*. The Psychology of Stalking: Clinical and Forensic Perspectives. London: Academic Press.

Mullen, P., Pathé, M., Purcell, R. (2000). *Stalkers and their victims*. Cambridge: Cambridge University Press.

Mutawa, N., Bryce, J., Fanqueira, V., & Marrington, A. (2016). Forensic Investigation of Cyberstalking Cases Using Behavioural Evidence Analysis. *Digital Investigation, 16*, 96-103.

Ngo, F. (2014). Toward a Comprehensive Model on Stalking Acknowledgement: A Test of Four Models. *Crime & Delinquency, 60*(8), 1158-1182.

Nobles, M. R., Reyns, B. W., Fox, K. A., Fisher, B. S. (2014). Protection against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization among a National Sample. *Justice Quarterly, 31*(6), 986-1014.

Norden, S. (2013). *How the Internet has Changed the Face of Crime*. Masters of Science Thesis (unpublished).

Paladin. (2016). *Stalking and Harassment – A Shorthand Guide about Digital and Cyberstalking*. Retrieved from http://paladinservice.co.uk/wpcontent/uploads/2014/11/Digital-and-Cyber-Stalking-Toolkit.pdf.

Patel, P. (2013). *Rebalancing the Scale: Prioritizing Victims of Crime in the Criminal Justice System*. Retrieved from http://www.roadpeace.org/resources/REBALANCING_THE_SCALES.pdf.

Parsons, T. (1961). Theories *of Society; Foundations of Modern Sociological Theory*. Illinois: The Free Press of Glencoe.

Perry, J. (2012). *Digital Stalking: A Guide to Technology Risks for Victims*. Retrieved from www.digital-stalking.com.

Piotrowski, C. (2012). From Workplace Bullying to Cyberbullying: The Enigma of E-Harassment in Modern Organizations. *Organization Development Journal, 3*(4).

Pittaro, M. L. (2007). Cyberstalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology, 1*(2), 180–197.

Reyns, B. W., Henson, B. (2015). The Thief with a Thousand Faces and the Victim with None: Identifying Determinants for Online Identity Theft Victimization with Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology,* 1-21.

Scheibelhofer, E. (2008). Combining Narration – Based Interviews with Topical Interviews: Methodological Reflections on Research Practices. *International Journal of Social Research Methodology, 11*(5), 403-416. p. 405.

Sheridan, L., & Grant, T. (2007). Is Cyberstalking Different? *Psychology, Crime & Law, 13*(6), 627-640.

Seidman, I. (2006). *Interviewing as Qualitative Research*. New York: Teachers College Press.

Smoker, M., & March, E. (2017). Predicting perpetration of intimate partner cyberstalking: Gender and the Dark Tetrad, *Computers in Human Behaviour*, *72*, 390-396.

Silverman, D. (2013). *Doing Qualitative Research*. Los Angeles: SAGE.

Spence-Diehl, E. (2003). Stalking and Technology: The Double-Edged Sword. *Journal of Technology in Human Services, 22*(1), 5-18.

Spitzberg, B. H., & Cupach, W. R. (2007). The State of The Art of Stalking: Taking Stock of the Emerging Literature. *Aggression and Violent Behaviour, 12*, 64-86.

Tavani, H., & Grodzinsky, F. (2002). Cyberstalking, Personal Privacy and Moral Responsibility. *Ethics and Information Technology, 4*, 123.

Tokunaga, R. S., & Aune, K. (2015). Cyber-Defence: A Taxonomy of Tactics for Managing Cyberstalking. *Journal of Interpersonal Violence,* 1-25.

Thomas, K. R. (1993). How to Stop the Stalker: State Anti- Stalking Laws. *Criminal Law Bulletin, 29*(2), 124-136.

Wall, D.S. (2005) *The Internet as a conduit for criminals*. In A. Pattavina (Ed.) Information Technology and the Criminal Justice System, 77-98. Thousand Oaks, CA: Sage.