American-Eurasian J. Agric. & Environ. Sci., 15(Tourism & Environment, Social and Management Sciences): 09-17, 2015
ISSN 1818-6769

DOI: 10.5829/idosi.aejaes.2015.15.s.202

Cyber Stalking: Social Issues of Harassment on Internet

[1]Murshamshul Kamariah Musa, [1]Zuhairah Ariff Abd Ghadas,
[1]Nazli Ismail and [2]Mohd Shahril Nizam B Md Radzi

[1]Faculty of Law and International Relations, Universiti Sultan Zainal Abidin,
Kuala Terengganu, Terengganu, Malaysia
[2]Faculty of Entrepreneurship and Business, Universiti Malaysia Kelantan,
City Campus, Pengkalan Chepa, Kota Bharu, Kelantan, Malaysia

Abstract: The borderless nature of Internet and its easy access to cyberspace has provided a low-cost but high-connectivity ways for criminals to reach victims. This resulted in a rise of crimes which make use of the Internet as a medium, such as fraudulent scams, child sexual exploitations and a new concern cyber stalking. Cyber stalking has been labelled as the crime of the nineties due to its nature which utilises the latest technological telecommunications as a mean to perpetrate such act. Cyber stalking, similar to stalking, involves threatening or harassing behaviours by one individual against another, with the exception that this particular act makes full use of the internet. Compared to offline stalking, cyber stalking has caused more intense stress and trauma on the victim. This paper is an introductory research and aims to identify the characteristics of cyber stalking, how it is committed and whether there exist any legislations in Malaysia in comparison to jurisdictions such as the USA and UK, which addresses this new breed of crime. As an initial legal study on cyberstalking, the methods used are by way of doctrinal analysis of statutory provisions, judicial decisions and relevant government policies.

Key words: Cyber stalking · Cybercrime · Online harassment · Computer Crimes Act 1997 (Malaysia) · Communication and Multimedia Act 1998 (Malaysia)

INTRODUCTION

Cybercrimes are crimes, which are perpetrated by making use of the computer or the information and communication technology (ICT) including the Internet. Most of these types of crimes have it roots in the real world; such as fraudulent swindles, theft, gambling, child exploitation and pornography. Rapid advancement in technology and communication has also contributed to a rise in cyber stalking, a crime originating from stalking.

The phrase cybercrime, computer crime and Internet crime are use almost interchangeably. It has been described as an illegal act which makes use of the computer itself, its systems or its application. Regardless of the term used, the perpetrator of a computer or cybercrime essentially requires knowledge of the workings of a computer and its system, even if only at the minimum level. The term 'computer crime' sometimes seems to be restricted only to crimes where the computer itself is paraphernalia for the commission of the crime which can occur both online and offline [1]. The term 'cybercrime' on the other hand, seems to suggest a much wider perspective of the crimes committed. The perpetrator is not only making use of a computer but also the world communication system – the Internet as a medium or place for executing an illegal act. The effect of the crime is more horrifying due to the borderless nature of the internet and the possibility of apprehending a criminal is now almost an impossible task as such crime occurs online. Surin suggests that when the term 'computer-related crime' is used the scope of definition expanded to cover not only computer-related activities which are criminal in nature in the legal sense but also antisocial behaviours which is not considered as transgressing the law [2].

Corresponding Author: Murshamshul Kamariah Musa, Faculty of Law and International Relations, Universiti Sultan Zainal Abidin, Kuala Terengganu, Terengganu, Malaysia.

Computer crime could reasonably include a wide spectrum of criminal activities, issues and offences. It may be in the form of intrusion into the computer systems (data stealing, planting of viruses, creating back doors or changing user names and passwords) or in the form of password sniffing, computer sabotage, or identity theft. These types of actions jeopardize the security of a computer system and the data stored by its users. In this limited sense, cyber stalking is also a type of computer crime as it makes full use of the computer in its commission.

Cybercrime is used [3] to refer to any crime, (inclusive of those that do not really substantially rely on the computer for its commission); which involves computers and networks. This type of crime makes full use of the internet by misusing, manipulating or abusing information that exists in the virtual realm of technology [4].Some writers [5] classify cybercrimes into three broad categories; namely crimes committed against the property of another, against the human body and cyber terrorism. Cybercrimes which targeted the property of another can be theft (of information, money, property or services); fraud, forgery, mischief (either with malice or not) by sending computer viruses, cyber vandalism and cyber trespass. Types of cybercrimes afflicted on the body of a person includes distribution of pornographic materials and related activities, such as cyber harassment or cyber stalking. Cyber terrorism, on the other hand, is usually a type of organized crime, which is commonly politically motivated [6]. In all these three broad categories of crime, the culprits will utilize and abuse whatever information gathered by making full use of the cyber space. It can becommitted via computers or any of the telecommunications systems which are themselves a computer system such as phones linked to a computer satellite systems and even global positioning systems (GPS) [7].

Definition of Cyber Stalking: There is no standard or universally accepted definition of cyber stalking. Cyber stalking in reality is a type of stalking but committed in the virtual world. Bocij and McFarlane posit that the terms cyber stalking and internet harassment could be used interchangeably as both involve “an element of threat or aim to cause distress to the victim” [8]. In order to grasp the meaning of cyber stalking it would be more appropriate to understand what is ‘stalking’ in the first place.

Stalking connotes a series of acts and behaviours inflicted by one, against another person, causing fear and worry on the victim. Stalking might starts quite harmlessly, so subtlety that the victim might not be aware of it happening at its earliest stage. As a crime, stalking does not requires the presence of a physical element but concentrate more on the mental element; whether the conduct intimidate or arouse the victim’s fear andapprehension [9]. Among stalking acts might include - repeated following and loitering, unwanted contact in any forms of communication, observation of the victim’s behaviour, interfering with property and even contacting family and friends of the victim inappropriately [10]. Stalking occurs in real time in the real world and always results in physical confrontation between the stalker and the victim, one way or the other. Legally, stalking is recognised as a crime only a few decades ago. The seriousness of this offence was after a series of incidents in the nineties, involving celebrities like Madonna and Jodie Foster and the incident, which eventually led to the death of young actor Rebecca Schaeffer in 1989 in California [11]. In essence, stalking encompasses a pattern of repeated, frequently intrusive behaviours which exist at a continuing severity that intimidate and cause fear in the victims [12].Different jurisdictions provide different definitions of this offence.

The main distinction between harassment and stalking lies in the time period of its occurrence. Harassment may occurs only once and for a short time; but in in stalking, the harassment would continue for a longer period, ranging from a few weeks’ time to a few years. The intention of the perpetrators and the original motivation for their behaviour also differs. In harassment, the perpetrator’s intention is just to scare the victim, for the fun of it, or to ensure that the victim would behave according to the way that the perpetrator wants. However, in stalking the intention is to frighten, terrorize or even injure another person physically, emotionally or reputation wise. Though both cyber stalking and cyber harassment might involve using the same tactics and techniques, in cyber stalking, the perpetrator will start by relentlessly pursuing his or her victim online. It probably might result into an offline confrontation. A cyber harasser might moves on and forgets about his victim after a while; but a cyber-stalker might leave his or her victim for a while but will always relentlessly returns to the victim, from time to time [13].In cyber stalking, the stalker is not in direct presence of his or her victim but rather follows or creeps up to the victim online, monitoring the victim’s activities on the virtual world, gathering information and at the same time making threats and other forms or verbal intimidation. It then escalated into a form of unwanted contact that intrudes on a person’s privacy and causing fear to the victim [14].

Benschop defines cyber stalking as "the repeatedly harassing or threatening of an individual via the Internet or other electronic means of communication" [15]and Bocij further suggested that it can be committed by individuals, groups of individuals or organisation to harass one or more individuals [16]. Among types of behaviours which constitutes cyber stalking, are spamming, transmission of threats and false accusation, damage to data or equipment, theft of data and identity, computer monitoring, solicitation of minors for sexual purposes and also any form of aggression online [17]. The Malaysian Computer Emergency Response Team (MyCERT) [18]describes cyber harassment as covering a wide range of offensive behaviour committed online against another, which are intended to threaten and disturb and divides them into bullying, stalking, sexual, religious and racial harassment. Cyber stalking is described as harassment done via electronic communications, wherein the stalker hides behind anonymity of the Internet to stalk a victim, targeting a victim with threatening messages. There seems to be significant overlapping characteristics between the classes of cyber harassment listed by MyCERT [19] compared to those offered by other writers.

It is reiterated that though there seems to be no specific legal definition of cyber stalking, most writers [20] recognizes the fact that this type of crime is committed by making use of technology's new and powerful tools and its devastating effect are similar, if not greater than conventional or offline stalking. It is an act which intrudes the privacy of a legal person and violates a person's right to life, liberty and security [21].

Types of Cyber Stalking: Due to the vast distances or geographical differences between the victims and the perpetrators cyber stalking is not going to result into physical violence, as long as it stays on the 'virtual world'. However, if by any chance, the cyber stalker decided to launch into offline stalking, the result might even turn to murder, as in the case of actress Rebecca Schaeffer. Nonetheless cyber stalking, would still inflict the same distressing effects on a victim as in offline stalking, be it physical, emotional and psychological consequences. Given the global coverage of the internet, the distress caused by cyber stalking might even be greater.

Cyber stalkers are clever at making use of variety of techniques and methods to stalk their victim. A cyber stalker usually follows a victim's online activity either for gathering of information, initiating contact, making threats or engaging in other forms of verbal intimidation, either through emails, network access, social network web pages/guestbook, personal chat services (for example Facebook, ICQ, Twitter, MSN messenger), chat rooms, Web discussion groups (for example Usenet, bulletin boards), electronic dating services and Internet games sites.The popular usage of these social networks has regulated the term stalking as a non-threatening normal act of social browsing, where it is used to imply to a process of gathering information of an individual based on one's online profile [22]. However, it is submitted that the crime of cyber stalking needs to be differentiated from mere social browsing or creepy behaviour especially when it has escalated into an intrusion and threat on a person's privacy.

Ogilvie categorises three primary ways by which cyber stalking is conducted depending on the how the usage of the Internet being exploited. She lists them as email stalking, Internet stalking and computer stalking [23].

- Email stalking is one of the most common forms of harassment and it represents the closest replication of traditional stalking by letter. It can be by issuing unsolicited emails, comprising of hate, obscene or threatening mail, spamming (high volumes of electronic junk mail which might force the computer to shut down) or sending viruses, which are sent in a repetitive manner with the intent to intimidate. It can also be done at regular or random intervals by the cyber stalker without the need to be physically presence at the computer terminal, by adopting sophisticated programs to that effect. The effect is an uninvited and arguably threatening incursion into the privacy of an individual. The reasons are often due to attempts to initiate or repair a relationship, or to threaten and traumatize a person. The perpetrators are easily traceable. A number of cases from the United States demonstrate how this type of stalking occurs, such as the case of *People v. Costales* [24] and *State v Gandhi*[25].Nonetheless, the free availability of anonymizer and anonymous remailers which are free and easily uploaded over the Internet might result in a high degree of protection available for protection of stalkers who wanted to conceal their tracks.
- Internet stalking is more public as the cyber stalker comprehensively uses and utilizes the Internet to slander and endanger the victims. The cyber stalker can make use of Internet bulletin boards or chat rooms, by posting controversial or sexually enticing

message under the name, phone number or email address of the victim. The other Internet users are deceived to harass or threaten the victim based on that false information given by the cyber stalker. Stalking by proxy occurs when the cyber stalker make use of third party either relatives or friends of the stalker or even a stranger, to intimidate the victim. A typical example is when the stalker impersonates the victim on the Internet, giving false messages that the victim is interested in sexual favours causing those who are interested in such activities to contact the victim with lustful remarks or when those people starts knocking on the victim's door! Minimal effort combined with lack of direct contact between the cyber stalker and the victim makes it difficult for the law enforcers to identify, locate and arrest the offender. It is most disturbing that internet stalking can cross over to the real world. It might be followed by threatening phone calls, vandalism of property, threatening mail or even physical attacks, an electronic precursor to real world behaviour. A UK case *R v Debnath* [26]provides a good illustration on how this type of stalking occurs.

- Computer stalking requires the cyber stalker to be more computer savvy than the other two earlier categories as the perpetrator exploits the makings of the Internet and operating system of a computer to assume control of the targeted victim's computer. A personal Windows based computer connected to the Internet can be identified. A stalker using this method can communicate directly with their victim as soon as the victim's computer connects in any way to the Internet. Once the cyber stalker assumes control of the victim's computer, the only defensive mechanism for the victim is to disconnect and relinquish their current Internet address. An incident cited is where a woman received a message from the cyber stalker stating that he is going to get her and he opened the woman's CD-ROM drive in order to prove that he has control over her computer.Vasiu and Vasiu cited other occurrences such as electronic spying on victims using malware, the usage of keylogger programs to observe victims' Internet usage and tracking of victim's movements using Global Positioning System (GPS) technology [27].

In conclusion, we can say that cyber stalking can be in various forms, but it still shares the most important characteristic with offline stalking i.e. the desire to exert control over their victims and engage in almost similar types of behaviour to achieve this.

Cyber Stalking in Malaysia: CyberSecurity Malaysia [28] statistical report indicates that almost 2000 incidents were reported to them in third quarter of 2012, whereby 63 cases were from cyber harassment. This number had decreased 3.33 % from the previous second quarter in the same year [29].The report also mention that, cyber harassment incident generally involved cyber stalking, cyber bullying and threat done via email and social networking sites such as Facebook, Yahoo Messenger, Twitter and Skype. These social networking sites are popular avenues for cyber harassment. Even though there was a lower rate of cyber harassment incident reported for a certain period, such reduction does not really signify a reduction in its actual occurrences. The reason being, most of cyber stalking incidents are usually unreported as the victim can opt out of the victim cycle by adopting a new internet identity or even abstaining from any internet activities for long period, thus cutting off any unwanted and prolonged contact with cyber stalker. This is evident as the figures in Table 1 indicated an increase in the number of cyber harassment incidents in the year 2013 [30].

Most online harassment incidents committed in Malaysia as reported to CyberSecurity (through MyCERT) Malaysia, involved harassment committed via web blogs,forums or social networking sites. As popular networking channels on internet, the harasser posted false or misleading information on blogs and web forums against a particular individual or organisations. Other harassing behaviours include threatening or defamatory emails and SMS messages sent to the victims with malicious intention. Cyber Security upon receipt of such

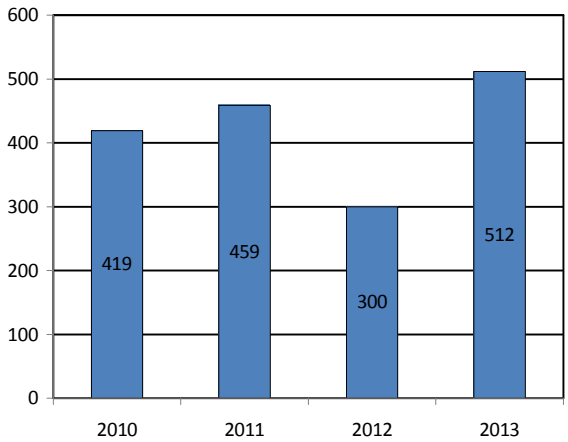

Table 1: Reported Cyber Harassment Incidents in Malaysia: Year 2010-2013
Source: MyCERT Incident Statistics 2010-2013 at www.mycert.org.my

complaints from the victim would notify the respective ISP providers where the blogs or forums were hosted for removal of such information. Though CyberSecurity acts as a monitoring body for detection of potential threats in the cyber world, it was not armed with any penal provisions. Any complaints notified to it will be dealt by CyberSecurity together with the relevant ISP providers and the law enforcement agencies [31].

Generally in addressing a cyber or computer related crime, the Computer Crimes Act 1997 is used in tandem with other Acts such as the Communication and Multimedia Act 1998, the Digital Signature Act 1997 and also the Penal Code (Act 574). Most of the types of cyber or computer related crimes which occurred in Malaysia and reported to CyberSecurity comprises of spamming, phishing, hacking and denial of services. Harassment via internet, as mentioned earlier constitutes only 2.67% of the total case of cyber-crimes reported [32]. Nonetheless, as shown in Table 1, the figures indicates a rise in the reported number of harassment incidents which necessitates the existence of appropriate legal framework to tackle the issue.

The Malaysian Legal Framework: In many developed countries, where the usage of ICT are commonplace, anti-stalking laws have been promulgated, which cater to the issue of cyber stalking either explicitly or impliedly. The United States of America, had, by the year 1999, some form of stalking law in all its 50 states [33], perhaps under different names such as criminal harassment or criminal menace. The Violence against Women Act 2000, legislated at federal level in the USA includes cyber stalking in its interstate stalking statutes. However, as this is the only federal law on anti-cyber stalking, each state has to further define the criminal act. As a result, in different jurisdictions the definition also varies to a certain extent. Some states have even revised their laws to regulate computer based harassment while others worded their anti-stalking law wide enough to cover both online and offline behaviours [34]. Similar laws to regulate stalking have also been promulgated in Canada, England, Wales and Australia [35].The United Kingdom addresses incidents of online harassment under provisions of Protection from Harassment Act 1997 and the Malicious Communication Act 1998, which are generally used to regulate traditional harassment cases.

Unlike USA and Australia, Malaysia does not have a specific anti-stalking law in its penal legislation. The Malaysian Penal Code, Act 574 does not contain any specific provisions which concentrate on the issue of stalking or harassment. A suggestion has been put forward by Anita Abdul Rahim and Nazura A. Manap [36]that a cyber-harasser or stalker may be prosecuted under Section 503 of the Malaysian Penal Code for making a criminal intimidation or under Section 507 where such criminal intimidation is done by anonymous communication. Section 503 provides:

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.

The main requirement that needed to be proved is that the threat must have caused alarm to the victim either to his body, property or reputation. The wordings of the section does not restrict to only physical threat but can be interpreted to those threat committed via Internet. Nevertheless, compared to threat by physical confrontation,it is quite difficult to prove that such online threat has caused alarm to the victim, either to his/her wellbeing or property. It would again depend on the peculiarity of the facts in each case. If such criminal intimidation was done anonymously, once caught,the culprit may be prosecuted under Section 507[37]. The punishment for such action is provided for under Section 506 [38] of the Code.

To create a safe cyber environment, Malaysia has set up a set of regulatory framework by 2002 which addresses cyber challenges issues, not only in integrity, security and privacy of information but also issues of intellectual property rights affecting trade. These laws are the Computer Crimes Act 1997, the Digital Signature Act 1997, the Telemedicine Act 1997, Copyrights(Amendment)Act 1997, Communications and Multimedia Act 1998 andOptical Disc Act 2000 [39]. For the purpose of this article, only the Computer Crimes Act 1997 and the Communications and Multimedia Act 1998 are analysed in order to ascertain whether it contains any provisions pertaining to cyber stalking either explicit or impliedly. A cursory look on these Acts seems to suggest that there are no clear cut provisions on online harassment.

The Malaysian Computer Crimes Act 1997 (the CCA) was passed in Parliament in March 1997 and enforced on 30th June 2000. Its main purpose was to provide for regulations pertaining to the misuse of computers. It is based on the United Kingdom Computer Misuse Act 1990 but with some modifications. However, it mostly governed

crimes involving unlawful access to data in a computer and its misuse [40]. The Preamble to the Act provides that it is to regulate offences relating to the misuse of the computers. These computer related crimes includes hacking, virus attack, as well as unauthorised interception of programs and data over computers, their systems or networks. The ultimate aim of this Act is to provide a safe environment for online transaction (particularly financial transactions) by deterring computer crimes and protection users' privacy [41]. Section 2 of the CCA defines computer as:

> *"an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility"*

This definition covers activities relating to automatic processing and transmission of data using the computer systems and networks. As part of the regulatory framework governing cyberspace, the CCA mainly protect the users against four types of offences as provided under Section 3 (unauthorised access to computer material), Section 4 (unauthorised access with ulterior intent), section 5 (unauthorised modification to content) and section 6 (unauthorised communication of codes and passwords) of the CCA. These sections [42] nonetheless are more related to hacking, phishing and identity theft rather than to be used for cyber stalking incidents.

The Communications and Multimedia Act 1998 (the CMA) primarily regulates the existing telecommunications industry and 'allow for the smooth convergence within the communication and multimedia industry'. It is part of the legal and regulating framework on the infrastructure of cyber laws in Malaysia. In line with it, a Commission on Multimedia and Communication was instituted to police and implement the Act under the Malaysian Multimedia and Communications Commission Act 1998. Again, similar to the CCA, cyber stalking is not specifically or directly address under the CMA. However it is submitted a provision, under the CMA which touches on the issue of online harassment, Section 211(1), can be used to tackle cyber stalking. The section states:

> *"No content applications service provider, or other persons using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person"*

The punishment of any person who contravenes the section i.e. maintain an indecent or offensive content is provided for under Section 211(2) of the same Act which carries a maximum fine not exceeding RM50,000 or imprisonment for a maximum term of one year or a combination of both upon conviction. It should serve as a deterrent to would be cyber stalkers who intend to manipulate any content for the purpose of harassing his victim.

Another provision which can be used to criminalise the act of online harassment is Section 233(1) of the CMA. The sections provides that the use of any facilities or services to transmit content which is 'obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass' another person would amount to a criminal offence. Such offence is punishable under Section 233(3) with a fine not exceeding RM50, 000 or one year imprisonment or both. It is submitted that the aforesaid provisions which prohibits online publication of illegal content and improper use of the internet are the most appropriate provisions to cater to cyber stalking incidents in Malaysia.

In short, we can safely argue that besides the two above stated provisions under the CMA, Malaysia's existing legal and regulatory framework does not have comprehensive provisions to address the issue of stalking or cyber stalking. In fact if the law must be resorted to in combating any cybercrime, one has to resort to the provisions of the Penal Code of Malaysia (the law on criminal actions) to find the relevant ruling. Even though some traditional laws have been revised or amended to address the commission of a cybercrime and online environment, Malaysia still needs a long way to go on the possibility of tackling cybercrimes effectively compared to our English counterpart either in the USA or United Kingdom. There exist vast rooms of improvement towards that goal.

CONCLUSION

Information technology evolves very fast and similar evolution might applies to cybercrimes. Empirical evidence gathered shows that cyberstalking is a serious cybercrime, occurring worldwide and is growing day by day as the numbers of Internet users increases [43].

There is a need for a mechanism to curb the rise of the cybercrimes, mainly through a legal infrastructure. In this paper, it is observed that Malaysia still lack of specific legislation to deal with cybercrimes. As an immediate action, the laws which are available via various legislation should be put into use to tackle cyberstalking [44].Nonetheless, it is time for the existing Penal Code or any penal provisions in various acts in Malaysia to take cognisant of the new breed of cybercrimes and include them in the definition of traditional crime as practised in the United Kingdom and United States. It is also suggested that a specific legislation could be enacted to supervise each category of cybercrime committed against the public, be it against their bodies, properties or for the public safety [45]. This would ensure that a cybercriminal can be properly prosecuted and the process of proving or disproving a crime committed in the virtual world is properly regulated with adequate punishment.

REFERENCES

1. The computer can either be the target, or use as a weapon or a medium of storage and the knowledge on computer technology is essential. See N.A. Mohamed and R. Maskat, 2004. Computer Crime: The Malaysian Approach. In the Proceedings of the International Conference on Electrical Engineering and Informatics. Institut Teknologi Bandung, Indonesia, pp: 364.
2. Surin, A.J., 2006. Cyberlaw and Its Implications. Pelanduk Publications Sdn Bhd., pp: 83.
3. Though many writers seem to use the word almost to mean the same, when the term ‘cyber’ is used it usually denotes the usage of cyberspace and the issue of jurisdiction arises. See further for instance the works of S.L.Y. Aun and L.L.B.H. London, 2005. An Introduction to Cybercrimes: A Malaysian Perspective.Available: http://www.mae/e.net/articles/ ekom2005.pdf (February 6, 2012); S.W. Brenner, 2001. Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law. Murdoch University Electronic Journal of Law, 8(2); R. Broadhurst, 2006. Developments in the Global Law Enforcement of Cyber-Crime. Policing: An International Journal of Police Strategies and Management, 29(3); A. Gupta, 2010. Cyber Crime in Present World.
4. Vello, R., 2006. Information Technology and Litigation: A General Introduction to Computer Crime, Information Security and Computer Forensics. Malayan Law Journal, no.5, p lvi.
5. Abdul Rahim, A. and N. Abdul Manaf, 2004. Jenayah Berkaitan Komputer: Perspektif Undang-Undang Malaysia. Dewan Bahasa and Pustaka, pp: 7-30. Also see D.I. Bainbridge, 2008. Introduction to Information Technology Law, 6th Edition. Pearson Education Limited; K.M. Rogers, 2011. The Internet and the Law. Palgrave Mcmillan.
6. Abdul Rahim, A. and N. Abdul Manaf, 2004. Jenayah Berkaitan Komputer: Perspektif Undang-Undang Malaysia. Dewan Bahasa and Pustaka, pp: 7-30.
7. Singh, B. and A. John, (not dated). Internet Crimes. Malayan Law Journal Free Online Articles. Availablehttp://www.lexisnexis.com.my/free/articles /beldue2.html (5 Sept 2006).
8. Bocij, P. and L. McFarlane, 2003. Cyber stalking: The Technology of Hate. The Police Journal, 76(3): 205.
9. Ogilvie, E., 2000. Stalking: Policing and Prosecuting Practices in Three Australian Jurisdictions. Australian Institute of Criminology Trends and Issues Series, pp: 2.
10. McEwan, T.E., P.E. Mullen and R. MacKenzie, 2007. Anti-Stalking Legislation in Practice: Are We Meeting Community Needs?. Psychiatry, Psychology and Law, 14(2): 207-209.
11. Baer, M., 2010. Cyberstalking and the Internet Landscape We Have Constructed. Virginia Journal of Law and Technology, 15(154): 155.
12. Ogilvie, E., 2000. Stalking: Policing and Prosecuting Practices in Three Australian Jurisdictions. Australian Institute of Criminology Trends and Issues Series, pp: 2.
13. Cyber stalking and cyber harassment explained available at http://www.wiredsafety.org/ cyberstalking_harassment/cs0.html (5 Sept 2008).
14. Hanewald, R., 2008. Confronting the Pedagogical Challenge of Cyber Safety. Australian Journal of Teacher Education, 33(3): 2.
15. Benschop, A. and translated by C. Menting, 2011. Cyberstalking: Menaced on the Internet. Socio Site available at http://www.sociosite.org/ cyberstalking_en.php(20 July 2011).
16. Bocij, P., 2002. Corporate Cyberstalking: An Invitation to Build Theory. First Monday, 7(11): 37.
17. Bocij, P., 2002. Corporate Cyberstalking: An Invitation to Build Theory. First Monday, 7(11): 38.

18. MyCERT was established in 1997 and operates under Cyber Security Malaysia as a point of reference for the internet community in Malaysia to deal with computer security incidents. The organisation provides assistance to the victims and works together with law enforcement agencies such as the Royal Malaysian Police, Securities Commission and Bank Negara Malaysia. MyCERT also has close collaborations with Internet Service Providers (ISP), computer security incident response teams and various computer security initiatives worldwide. See details on the functions of this organisation at www.mycert.org.my.
19. See http://www.mycert.org.my/eb/serves/report_incidents/cyber999/main/detail/799/index/html (29 May 2014) under Definition of Incidents.
20. See also the comments of the following writers on the connection between advancement of the Internet and cyber stalking; D. Harvey, 2003. Cyberstalking and Internet Harassment: What the Law Can Do., In the Proceedings of the NetSafe II: Society, Safety and the Internet Conference. Auckland, New Zealand; M.L. Pittaro, 2007. Cyber Stalking: An Analysis of Online Harassment and Intimidation. International Journal of Cyber Criminology 1(2); N. Geach and N. Haralambous, 2009. Regulating Harassment: Is the Law Fit for the Social Networking Age. Journal of Criminal Law, pp: 73.
21. Vasiu, I. and L. Vasiu, 2013. Cyberstalking Nature and Response Recommendations. Academic Journal of Interdisciplinary Studies, 9(2).
22. See Fitzgerald, B., (2012, July 5). Facebook Study Explains Why We Still Spend So Many Hours Stalking Each Other. The Huffington Post. Available at http://www.huffingtonpost.com/2012/07/04/facebook-study-shows-we-u_n_1644061.html; N. O'Neill, (2011, April 5). 7 Ways to Spot a Chronic Facebook Stalker. AllFacebook. Available at http://allfacebook.com/chronic-facebook-stalker_b37856
23. Ogilvie, E., 2000. Cyber stalking http://www.aic.gov.au (5 Sept2006).
24. 2d Crim. No. B215915 (Court of Appeals of California, Second District, Division Six, 2010), wherein the victim received a large number of disturbing emails from a Michigan person, who is a stranger to her after she used a MySpace account to market her music.
25. 989 A.2d 256, 2010. the victim met the accused through a mutual friend. In the course of their relationship which had took a bad turn, the accused send sexually graphic and threatening emails containing the details of accused's desire to have sex with the victim.
26. [2006] 2 Cr App R (S) 169. The accused has committed a series of harassing conduct against the victim whom she had a one-night stand and of whom she had mistakenly belief had transmitted a venereal disease to her. She started sending emails to the victim's fiancé, under the guise of the victim's friend telling about the sexual incident. She also sends emails to the victim's employer, pretending to be the victim admitting that he was harassing the accused. Not only that, she registered the victim on a database for person with sexually transmitted disease, on a gay American prisoner exchange website and set up a website which contains false article alleging homosexual practices by the victim. She also paid hackers to divert victim's email to one of her accounts.
27. Vasiu, I. and L. Vasiu, 2013. Cyberstalking Nature and Response Recommendations. Academic Journal of Interdisciplinary Studies, 9(2).
28. This is an organization under the Ministry of Science, Technology and Innovation Malaysia (MOSTI). It started out in 1997 as MyCERT-Malaysian Computer Emergency Response Team. In 2001 it is known as NISER (National ICT Security and Emergency Response Center) and was entrusted as a monitoring body for the network infrastructure of the country in line with the country's policy to ensure a smooth and safe ICT networking system throughout the country under the MSC agenda. In 2005, it became a company limited by guarantee under MOSTI and given the task as a national cyber security agency in 2006. In 2007 it was renamed as CyberSecurity Malaysia and given additional mandate in order to ensure the safety of ICT networking in the country. It works in collaboration with other Computer Emergency Response Teams (CERT) around the world to foster cooperation and coordination in incident prevention of cyber threats. See www.cybersecurity.org.my.
29. See e-Security Vol 32(Q3/2012), pp: 2-7. This journal published by CyberSecurity Malaysia under patronage of (MOSTI) and can be viewed online at www.esecurity.org.my also through www.cybersecurity.org.my.

30. Data retrieved from My CERT, however the Incident Report cover five types of cyber harassment which are cyber bullying, cyber stalking, online sexual harassment, religious and racial online harassment. The Reports does not focus only on cyber stalking as the only type of harassment.
31. Refer to www.cybersecurity.org.my and www.mycert.org.my for further information on the functions of these two agencies in tackling cyber security incidents.
32. See report by CyberSecurity published in their official bulletin e-Security, Vol.32 (Q3/2012) at www.esecurity.org.my.
33. See an interesting report prepared by the Attorney General of USA to the Vice President Al Gore in August 1999, Cyber Stalking: A New Challenge for Law Enforcement and Industry at http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (5Sept2006).
34. Miller, C., 2006. Cyber Stalking and Bullying – What Law Enforcement Needs to Know. Available www.officers.com (2 Sept 2008). See also I. Vasiu and L. Vasiu, 2013. Cyberstalking Nature and Response Recommendations. Academic Journal of Interdisciplinary Studies, 9(2). Section 2261A of Title 18 of the United States Code penalizes cyber-stalking as much as physical stalking, with imprisonment for a minimum one year period.
35. On stalking laws for Victoria, Queensland and South Australia, refer to article by E. Ogilvie, 2000. No. 176: Stalking: Policing and Prosecuting Practices in three Australian Jurisdictions. Australian Institute of Criminology. Available http://www.aic.gov.au (2 Sept 2008).
36. See Abdul Rahim, A. and N. Abdul Manaf, 2004. Jenayah Berkaitan Komputer: Perspektif Undang-Undang Malaysia. Dewan Bahasa and Pustaka, pp: 66-70 for detail discussions.
37. Section 507 of the Penal Code: Whoever commits the offence of criminal intimidation by an anonymous communication, or by having taken precautions to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment for a term which may extend to two years, in addition to the punishment provided for the offence by section, pp: 506.
38. Imprisonment up to 2 years with a fine, or if it caused hurt or destruction of property of the victim, impeaching the chastity of a woman, the term of imprisonment can be up to 7 years plus fine.
39. Kuppusamy, M. and A.S. Santapparaj, 2006. Cyber-Laws in the New Economy: the case of Malaysia. Asian Journal of Information Technology, 5(8): 885-887.
40. For detail discussion of the effect of this Act, see Hamim, Z., 2004. The Legal Response to Computer Misuse in Malaysia-The Computer Crimes Act 1997. UiTM Law Review, pp: 210-234.
41. Kuppusamy, M. and A.S. Santapparaj, 2006. Cyber-Laws in the New Economy: the case of Malaysia. Asian Journal of Information Technology, 5(8): 885-887.
42. In all these sections, the criminal act is obtaining information or data from a computer without authorization.
43. Aa, S., 2011. International (Cyber) Stalking: Impediments to Investigation and Prosecution. The New Faces of Victimhood, pp: 191-213.
44. The Penal Code, the Computer Crimes Act 1997, the Communications and Multimedia Act 1998, to be read together, with other relevant acts such as Women Protection Acts 1973, on the issue of phonographic or prostitution, Defamation Act on the issue of libel and slander etc.
45. Abdul Rahim, A. and N. Abdul Manaf, 2004. Jenayah Berkaitan Komputer: Perspektif Undang-Undang Malaysia. Dewan Bahasa and Pustaka, pp: 94-95.