Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws

Duryana binti Mohamed

Ahmad Ibrahim Kuliyyah of Laws, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia

Keywords:
Malaysia cybercrime
Cyberlaw
Cybercrime control measures
Traditional law

ABSTRACT

Cybercrimes are increasing in Malaysia. According to a report the crimes jumped by 88 per cent in 2011 with 15,218 cases compared with 8090 in 2010. This report has caused a lot of concern from the Government and the public. At a glance, these crimes are like 'diseases' spreading throughout the country and causing damage to people, the economy and the country. Although various efforts have been taken and some are still ongoing, total prevention of cybercrime is very difficult. Combating the threat is very challenging since Malaysia is still lacking in many of the tools required including manpower and technology. But the efforts will continue. This paper discusses some of the efforts taken by the Government and other organisations to deal with these problems followed by an analysis on the application of cyberlaws and how these measures work together with the traditional law in tackling cybercrime cases.

1. Introduction

Cybercrimes continue to rise and have become one of the modern problems that threaten public security and economy of the country. These activities will continue to increase if no effort is taken to reduce or to prevent them. Many countries have made efforts to prevent these 'diseases' from spreading but total prevention seems to be impossible. Nevertheless, this does not deter Governments and other organisations from continuing their efforts to reduce such crimes from spreading to broader levels of society. One of the efforts taken by the Government of Malaysia has been to introduce cyber legislation and regulation. This paper discusses these efforts followed by an analysis of the application of cyberlaws and how the laws work together with the traditional laws in combating the threats of cybercrimes.

1.1. *Cybercrime and traditional crime: an overview*

Cybercrime is also known as high-tech crime or computer crime (Clifford, 2001; Wall, 2002). According to the Encyclopedia Britannica computer crime is 'any crime that is committed by means of a special knowledge or expert use of computer technology.' This means that computer crime is committed by a computer expert who uses his knowledge and skills to commit computer abuses and various types of cybercrimes. Nevertheless, this definition may change in future due to the evolution in information technology that may influence the scope of the definition (Eu Jin, 2004).

Generally, cybercrime involves unlawful activities committed in 'cyberspace' and the computer is used as a medium or tool to commit those crimes. These acts are sometimes known as 'Old Crimes, New Tools' since the crimes committed are originally old type (from the offline world) or traditional types of crime, but the techniques of committing such crime have been changed within the digital environment. One example of such crime is computer fraud which is committed by manipulating computer data belonging to others in order to dishonestly obtain or embezzle money or property, to cause loss (Allan & Salter, 1997).

Other types of fraud include misuse of Automated Teller Machine (ATM) cards, misuse of credit cards and electronic

0267-3649/$ – see front matter © 2012 Duryana binti Mohamed. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2012.11.005

fund transfers (Carter, 1995; Grabosky, 2005). The online transfer of money usually involves international syndicates which target internet users to deposit money for payment of something which does not exist (Ahzan, 2010).

Another type of cybercrime is known as 'New Crimes, New Tools' because the crimes involve a situation where the suspect uses the computer system to alter or modify certain data in that system. These crimes are committed against the computer system. They include sabotage, vandalism and electronic wiretapping or gaining illegal access by impersonating an authorised user or exceeding a person's authority (Bologna & Shaw, 2000). Other than these, spreading computer viruses, cyberwar, cyber terrorism, denial of service (DOS) i.e. by preventing others from making use of their system, internet pornography or cyber pornography, invasion of privacy such as access to personal information, software piracy such as an unauthorised replication of computer software, reprogramming, hacking, phishing or identity theft, cyber squatting, cyber stalking, mass web defacement and faring are all categorised as cybercrimes. In summary, these cybercrimes are evolving and will continue to evolve with new technology and versatile criminal minds.

On the other hand, traditional crimes are crimes committed without using the computer or electronic medium. These crimes are committed by an individual or a group of individuals either by way of abetment, conspiracy, giving false evidence, theft, fraud, assault and murder. These offences are mentioned in the Penal Code of Malaysia and certain statutory provisions. Street crimes are also part of the conventional crimes and they include snatch theft and robbery. According to a report these offences made up 17% of the overall crime index in 2008 (Karim, 2009).

1.1.1. *Cybercrime incidents and losses*

In Malaysia, the incidence of cybercrime started to attract public attention when hackers attacked the websites of the Malaysian Parliament and University Technology Mara in 2002. The hackers wiped out all information on the Parliament website and replaced the homepage with words in a foreign language. This attack is considered dangerous because it affected the government body and one of the public universities in Malaysia. Then, in 2004, many local websites were affected by web defacement activities which resulted in the emergence of cyber graffiti (New Straits Times, 2004; Sani, 2005). The impact of web defacement activities on sites which handle electronic transactions is said to be much greater than on information-based websites. Then, cyber attacks continued to grow and from the statistics in 2008, fraud recorded the highest number of cases (907) as compared to denial of service attacks (12). Until May 2009, system intrusion recorded the highest number of cases (624) and denial of service attacks increased to 14 cases. However, fraud and forgery cases had reduced to 331 cases. The lowest reported case in 2009 was for indecent content (6) (Mycert, 2008). In 2009, CyberSecurity Malaysia (the national cybersecurity specialist centre under the purview of the Ministry of Science, Technology and Innovation (MOSTI)) had received 3564 cases reported to the centre; an increase of 68%, compared with the same period in 2008 (The Star, 2010a). In 2011, a total of 15,218 incidents were reported via the Cyber999 Help Centre, which was an 88 per cent increase compared with 2010 when only 8095 incidents were reported (Kye Lee, 2012). The cybercrime cases reported to the RMP include Short Message System (SMS)/calling, ATM, parcel, Internet Banking/phone banking/FTT, phishing, e-commerce and abuse of network facilities under the Communications and Multimedia Act (CMA) 1998. According to the statistics of the Royal Malaysian Police the highest reported case in 2010 was crimes related to misuse of ATM and the highest loss amounting to RM20,786,906.62 was caused by syndicate activities on banking transactions. As of July 2012, love scams and fraudulent online purchases ranked highest among the 403 cases of cybercrimes reported within the first three months of the year. These incurred losses of RM16 million. According to Bukit Aman Cybercrime and Multimedia Criminal Investigation officer ASP Mohd Syafiq Jinuin Abdullah, the frequency of cybercrime cases had increased steadily, where about 6586 reports of such cases were lodged last year with RM34 million incurred in losses compared with 6238 cases involving RM18 million in 2010 (Bernama, 2012b).

Although there was a statement (Moores, 2004) that cybercrimes do not cause any physical violence and have low personal risk when compared with other crimes, cybercrime has the potential to cause financial damage and monetary loss that could threaten Malaysian businesses and the economy (Utusan Malaysia, 2004). This fact is supported in a statement issued by Tommy Seah, Honorary Group Chairperson of International Cybercrime and Forensic Examiner (ICFE) Group of Companies in April 2010. According to him, financial and cybercrimes were among the most prevalent economic crimes committed in Malaysia. The economic crimes constitute fraud, corruption and bribery, identity theft, money laundering, cybercrime, accounting and financial fraud. On the enforcement issue, he also said that 'it was important to ensure greater enforcement by the authorities and organisations in order for Malaysia to remain attractive to foreign investors' (Bernama, 2010a).

Early examples of loss can be seen back in 2003 when the United Kingdom suffered £60 million losses from cyber-related crimes and a police survey indicated that 83 per cent of Britain's largest companies had been victims of cybercrime costing them more than £195 million in business downtime, lost productivity and perceived damage to their brand or share price (BBC News, 2005). In October 2012, the Ponemon Institute conducted a study on *Cost of Cybercrime* in UK. The result has shown that cybercrime costs UK organisations an average of £2.1m a year each. The study also revealed that the cost of attacks on UK organisations range between £400,000 and £7.7m. It is submitted that this situation is quite alarming and needs proper security measures to handle it. The study also found that the most costly UK cybercrimes are those caused by malicious insiders, denial of service attacks and malicious code. The 2012 study also revealed the average annual cost of cybercrime incurred by US organisations. It is the highest of the countries studied i.e. at $8.9m or £5.5m, which represents a 6% increase over the average for 2011, and a 38% increase over 2010 (Ashford, 2012). In August 2008, eleven people in Boston, US were charged in connection with data breaches or credit card fraud at nine major retailers. According to the authorities the crimes were the largest Federal hacking and

identity theft case ever which involved the theft and sale of more than 41 million credit and debit card numbers. While in Malaysia, more than RM116 million in damages had been incurred in the last two years due to online crime (Cheng, 2012).

In short, the above threats can cripple computer networks and systems. Therefore, in order to prevent huge losses to business and damage to the integrity of any corporation, efforts must be made to curb these activities (Yunos and Nasir, 2003). The companies, for example, must protect their integrity by setting up policy-based content security which deals with matters on productivity, online threats, compliance and legal liability (Durbin, 2004; Hamin, 2003). There must also be effective mechanisms to prevent and detect cybercrime activities on all networks in order to avoid attacks like denial of service attacks (DOS). This is because without effective protection, such crimes could threaten the security of the country and threaten the development of ICT in Malaysia.

2. The efforts to combat cybercrime

Although it was reported that the cybersecurity level in Malaysia was better than those in developed countries, Malaysians need to be even more proactive about safety measures (New Sabah Times, 2009). In 2010, phishing attacks were reported as being on the rise and considered to be one of the major threats to the country (The Star, 2010b). However, these attacks can be prevented as well as eradicated if the public is educated and the financial institutions, Bank Negara Malaysia (National Bank), the respective ministries and the law enforcement agencies collaborate to address these issues. The financial institutions may also deploy a phishing fraud-detection service that proactively monitors e-mail traffic and provides immediate notification upon the discovery of new phishing e-mails (Sani, 2004; Naples and Maher, 2002).

Hence, the obligation to combat cybercrime is not only confined to government or law enforcement but extends to the private sectors, organisations and individuals. The efforts taken by the Ministry of Science, Technology and Innovation (MOSTI) and CyberSecurity Malaysia, the Malaysian Communications and Multimedia Commissions (MCMCs), the Royal Malaysian Police (RMP) are explained below.

2.1. *Ministry of Science, Technology and Innovation (MOSTI) and CyberSecurity Malaysia*

In order to combat cybercrime activities and deal with information communication technology (ICT) related matters, the Ministry of Science, Technology and Innovation (MOSTI) has adopted a National ICT Policy framework which includes designing the National CyberSecurity Policy (NCSP). This NCSP seeks to address the risk to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. There are also eight policy thrusts under the NCSP which include reviewing and enhancing Malaysia's cyberlaws (NITC, 2012). CyberSecurity Malaysia, an agency, was appointed to manage and receive reports on Internet-related problems through its 24-h Cyber999 Help Centre. This agency has also drafted the NCSP in 2006 and given emphasis by the Science, Technology and Innovation Ministry in 2012 due to the increasing volume of cybercrime and the dangers of such crime to the security of the country (Kye Lee, 2012).

CyberSecurity Malaysia has taken various measures to ensure that Malaysia is protected from cyber attacks. Among these are collaborating with international experts and organisations in information security, which includes conducting OIC-CERT Drills organised by The Organisation of the Islamic Cooperation – Computer Emergency Response Team (Bernama, 2012d). OIC-CERT provides "a platform for member countries to explore and to develop collaborative initiatives and possible partnerships in matters pertaining to cybersecurity that shall strengthen their self reliance in cyberspace". Other measures include co-founding the Asia-Pacific Computer Emergency Response Team (APCERT), becoming a member of the Forum of Incidents Response and Security Teams (First) and a member of the Anti-Phishing Working Group (APWG). In July 2009, CyberSecurity Malaysia signed a MoU with the Malaysian Airlines System (MAS), Asia e-University, Centre for Advanced Software Engineering of Universiti Teknologi Malaysia, Management Science University and Mimos Bhd in an effort to combat cybercrime (Shafi, 2010). With such collaboration and efforts, CyberSecurity Malaysia is able to work closely with trusted and reliable international information security experts (The Star, 2010c; AsiaOne, 2011) has also suggested that the nation needs a dedicated 'cybercourt' in view of the high increase in cybercrime in the country (Patrick, 2009).

2.2. *The Malaysian Communications and Multimedia Commissions (MCMCs)*

The Malaysian Communications and Multimedia Commissions (MCMCs) are governed by the Malaysian Communications and Multimedia Commission Act 1998 and its objectives include supervising and regulating the communications and multimedia activities in Malaysia. The role of MCMC is to regulate according to the Communications and Multimedia Act 1998, Digital Signature Act 1997, Postal Services Act 1991 and Strategic Trade Act 2010. It covers telecoms, broadcasters and ISPs; postal and courier services and digital certification authorities (Iskandar, 2012). This Commission has identified twenty (20) Internet crimes which the Attorney General can prosecute. The cases cover a range of offences provided under the CMA 1998, such as abuse of religion, pornography, phishing and sedition. Besides taking the culprits to court, the Malaysian Communications and Multimedia Commission (MCMC) will also block access to phishing, fraud, illegal investment and pornography websites (Malaysia Today, 2011).

Besides that, the MCMC has also set up a bureau to receive complaints to identify and probe those responsible for providing and disseminating illegal content. The Commissions have worked hard in the past two years investigating websites and social networking pages containing offensive articles such as insulting comments on Islam and Allah (Mustaza, 2010). Nevertheless, there is still white-collar cybercrime which is not sufficiently reported due to reluctance or ignorance (Borneo Post Online, 2011).

2.3. *The Royal Malaysian Police (RMP)*

The Royal Malaysian Police through its Department of Commercial Crime Investigation (otherwise known as 'Jabatan Siasatan Jenayah Komersial') (JSJK) has established an Investigation of Cybercrime and Multimedia Unit to investigate cases. Besides that, a College of RMP and a Computer Forensic Laboratory were also established to provide training to police officers and computer forensic experts. The Inspector General of Police (IGP) Tan Sri Ismail Omar has said that cybercrime unit police will be equipped with the latest high-tech resources to combat online offences effectively. They will also come up with a new mechanism and procedures to deal with cases involving the Internet, especially on Facebook (Bernama, 2010a,b,c). Further, the Government is planning to build an anti-terrorism academy at the Langkawi International Shooting Range in order to combat terrorism and other global crimes. According to Home Ministry Deputy Secretary-General Datuk Abdul Rahim Mohd Radzi, the academy will focus on applying the latest techniques to fight terrorism, human trafficking, drug smuggling, money laundering, cybercrime, biological warfare and the use of explosives. This effort will also involve enforcement and intelligence agencies from all over the world. In this regard, Bank Negara will be playing a major role and work as coordinator between multiple agencies (Zolkepli, 2010).

2.4. *Other efforts*

CyberSecurity Malaysia has introduced new Internet guidelines known as 'Best Practice on Social Networking Sites (SNS)' in order to control the use of social networking. It has also prepared an 'Anti-Spam Framework of Best Practices and Technical Guidelines' in order to curb spamming, since there is no specific law to fight these spamming threats, although the MCMC made a proposal to curb spamming as long ago as 2004 (MCMC, 2004; Khong, 2004). Until November 2012 there is still no decision by the Government to introduce an anti-spam law in Malaysia or proposal to modify existing cyberlaw, particularly the Communications and Multimedia Act 1998 and the Computer Crimes Act 1997. According to the information available at its website Malaysia has no immediate plans to legislate. It will pursue this recourse when there is no other viable alternative (SKMM, 2012).

This is in contrast with some other countries which have already passed an anti spamming legislation. Among them are the UK Privacy and Electronic Communication (EC Directive) Regulations 2003 (SI 2003 No. 2426), the Australia Spam Act 2003 and the US Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (Shou Sien, 2004). In the Asia-Pacific region, the Australian Communication Authority (ACA) and the Korean Information Security Agency (KISA), for example, have initiated the Seoul-Melbourne Anti-Spam Agreement, a multilateral memorandum of understanding (MoU) on cooperation in countering spam with agencies from China, Hong Kong, Japan (2), Korea, Malaysia, New Zealand (2), the Philippines, Thailand and Taiwan (ACA, 2005). The ACA and KISA will work together to coordinate cooperation between the MoU members.

In addition, staffs at government agencies have also been trained and tested on their readiness to cope with cyber attacks. In between June 24 and August 2 of 2010, thirty-four organisations from nine Critical National Information Infrastructure (CNII) sectors took part in the Cyber Crisis Exercises which were also known as X-Maya. The X-Maya was carried out and involved sectors such as health, water, banking and finance, information and communication, energy, transport, defence and security, government and agriculture (Timbuong, 2010). Other than that, a higher learning institution such as University Sains Malaysia (USM), has also contributed by creating a Forensic Analysis and Discovery System (FADS) to help the investigation process. This system has been well-received by government agencies, including the Malaysian Communications and Multimedia Commission (MCMC).

In order to further strengthen the efforts to fight against the cybercriminals and cyber threats Malaysia has agreed to join the IMPACT-alliance. IMPACT (International Multilateral Partnership Against Cyber threats) and ITU (International Telecommunication Union) are two organisations that collaborate in providing services to the globe. IMPACT has also laid down five strategies namely, legal measures, international cooperation, technical and procedural matters, organisational structures and capacity building in order to achieve its objectives (IMPACT, 2012).

Nevertheless, in order to achieve more effective results, every individual should know and comply with computer ethics as well as being willing to adopt the principle of self-regulation. As for the corporations, a proper system to detect the criminals and to enforce strong security protection over the internet should be adopted. Bosses may observe their employees work ethic and ensure they comply with company policies. This is because on many occasions computer fraudsters or 'perpetrators' are employees of those organisations. They include supervisors and managerial staff, computer programmers as well as clerks (Hamin, 1999). Other potential cybercriminals could be terrorists, teenage 'geeks' and those with computer skills who either intentionally or unintentionally commit such abuses. Computer fraud committed by employees is classified as internal fraud and most of it relates to the accounting systems of the company. The offender will try to conceal his wrongful act by entering his fraudulent activity in a normal accounting system which leaves no visible trails to uncover. Nevertheless, what is important is to prepare, not only for this but more serious attacks, such as those which develop when full scale 'cyberwar' takes place. Although the solutions to such attacks are multiplying, the attacks led by sophisticated espionage are expanding and multiplying in strength and capacity (The Star, 2010d).

The above are some of the efforts taken by the government and various organisations in controlling the threats of cybercrimes. However, control of such threat still depends on the people on how well they understand the threat and can educate themselves to use computers safely and maintain the confidentiality of the data or information in their possession or passing through their online environment. Compliance with the laws and regulations will make the situation better and more protected.

3. Cyberlaw and traditional law: an analysis

In Malaysia there are nine laws that govern cyber-related activities. These laws include the Computer Crimes Act 1997 (CCA), the Digital Signature Act 1997 (DSA), the Copyright Act 1987 (CA) (also known as Copyright (Amendment) Act 1997), the Telemedicine Act 1997 (TMA), the Communications and Multimedia Act 1998 (CMA), the Communications and Multimedia Commission Act 1998 (CMCA), the Electronic Commerce Act 2006 (ECA), the Electronic Government Activities Act 2007 (EGA) and the Personal Data Protection Act 2010 (PDPA). Each law was enacted for a specific purpose and with the intention to regulate the successful implementation of the ICT environment. This also means that society is guaranteed proper protection when dealing with online matters. Those found to have abused the internet can also be charged under traditional law, namely, Banking and Financial Institutions Act 1989, Capital Markets and Services Act 2007, Sedition Act 1948Defamation Act 1957 or even under the Penal Code (Malaysia Today, 2011). It is best to analyse the application of cyberlaw and the traditional law since in certain cases the prosecution refers only to traditional law even in cyber-related cases. The main issues are to what extent cyberlaw has been applied in solving cybercrime cases in Malaysia and which law is the most preferred and effective measure? The following discussion will assess this question.

3.1. *The Computer Crimes Act 1997(CCA) vs the Penal Code*

The CCA 1997 governs limited aspects of cybercrime focussing only on hacking or unauthorised access offences (Allan & Salter, 1997). Section 3 deals with the unauthorised access offence while section 4 addresses unauthorised access with intent or aggravated hacking. This section refers to offences under section 3. The penalty for offences committed under section 3 is a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding five years or to both (CMA, 1993a) while under section 4 if a person is found guilty of an offence he shall pay a fine not exceeding one hundred and fifty thousand ringgit or face imprisonment for a term not exceeding ten years or both (CMA, 1993b). This is very similar to the UK Computer Misuse Act 1990.

Section 4 of the Act places emphasis on unauthorised access with intent to commit fraud or dishonesty or to cause injury as defined by the Penal Code (CMA, 1993c). But the time when the offence is committed does not depend on the time of when unauthorised access occurred. The CCA 1997 is silent on the punishment for repeated offences and will only be an effective deterrent if a more significant punishment is provided under the Act. Because of this the CCA has been criticised for its limited application. Nonetheless, it the law was applied in *Public Prosecutor* v *Tan Wee Suan*, *Ong Choo Ping and Ors* (unreported case, 2001) where the accused was arrested when seen using a card reader at an ATM of the Public Bank in Johor Bahru. The accused was charged under s4 (1) (a) of the CCA 1997 and being liable for punishment under s4 (3) of the same Act and s34 of the Penal Code (Penal Code, s34) but no trial ever took place as a guilty plea was entered and the punishment imposed was not recorded. However, as can be seen in the case of *Tan Wee Suan*, the guilty plea stopped further examination of the CCA 1997 and thus, its effectiveness remains unchallenged. This situation does not contribute well to the development of the Act although it was referred to again in 2012. In *PP* v *Jose Wilfredo Sosaya Carrasco* (Case Number: 62-06-01/2012) the suspect, Jose Wilfredo Sosaya Carrasco was charged under s4(1)(a) of the CCA 1997 with misusing an ATM card belonging to other person (PP v Jose Wilfredo Sosaya, 2012). As a result, he was sentenced to 42 months imprisonment for his wrongful act. By looking at the hacking cases in Malaysia, it is possible to assume that this Act will be applied extensively in the future.

In addition, the CCA 1997 also governs unauthorised modification of computer material and wrongful communication of passwords under s5 and s6 respectively. These two sections address the effect of hacking or unauthorised modification of the contents of any computer program or data. Section 5 of the CCA 1997 refers to unauthorised modification of the contents of any computer system. It does not matter whether it is not directed at any particular program or data and whether such modification is, or is intended to be permanent or merely temporary. Thus, when a person is convicted for such an offence he shall be liable to pay a fine of RM100,000.00 or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding RM150,000.00 or to imprisonment for a term not exceeding ten years or to both, if the act is done with the intention of causing injury as defined in the Penal Code. Meanwhile, section 6 prevents a person from wrongfully communicating a number, code or password to an unauthorised person. If that person is found to have committed such an offence, directly or indirectly, he shall be liable to a fine not exceeding RM25,000.00 or to imprisonment for a term not exceeding three years or to both. However, there is nothing much to discuss about the application of these two sections since so far there is no case law involving these sections.

From the study, it is found that in both sections 4 and 5 of the CCA 1997, the Penal Code is mentioned and this indicates that the Penal Code is still relevant even if the crime was committed in cyberspace. This may explain why the prosecutor prefers to charge the accused under the Penal Code even if the case involves cyber offences. In fact, in practice, the Penal Code is usually resorted to in order to prosecute computer fraudsters. The CCA 1997 is only relevant when there is an element of unauthorised access or hacking. In other words, sections 3–5 of the CCA 1997 focus on similar and related issues, that is 'unauthorised access' and 'unauthorised modification'. Thus, hacking can be done with the intention to commit fraud (ss3 and 4) and fraud can be committed by modifying the data or program in the computer system (s5). Nonetheless, the application of these provisions has never been challenged in any hacking or cybercrime cases.

Unlike Malaysia, the crime of unauthorised access to computer materials, unauthorised modifications of the contents of a computer and unauthorised access to a computer service have been discussed extensively in Singapore. For example, in the case of *Public Prosecutor* v *Muhammad Nuzaihan bin Kamal Luddin* (SLR, 2000) the defendant (respondent), a 17 year old student, pleaded guilty to three charges made against him under ss3 (1), 5(1) and 6(1)(a)

of the Computer Misuse Act 1993 (CMA). He was given 30 months probation but the prosecution appealed against the order stating that it was an inadequate sentence. The appeal was allowed. On allowing the appeal by the prosecutor, Yong Pung How CJ in his judgment stated that the district judge was wrong in giving the probation order since the inherent nature of offences under the CMA makes probation orders ineffective, as keeping the offender at home in such cases does not guarantee that the offender will not repeat his actions. The learned judge also agreed with the prosecution that;

> *…the statement of facts revealed clearly that the respondent had made a conscious decision to use his hacking skills on local servers after having gained confidence from his success at hacking into foreign sites. He not only gained unauthorised access to the local servers, but also went further and modified the programs in the server Brahms which action enabled him to access the server in future without having to hack into the system again. Thereafter, he made use of SCV's computer services for his own purposes and even had the presence of mind to obliterate all traces of his intrusions so as to avoid detection. It is pertinent that the respondent had hacked into the server Brahms only after SCV had rejected his application for cable subscription. …As a result, when offences such as these are committed, the courts may well have to apply the principles of strict liability so that the offender's state of mind is irrelevant to a finding of guilt.*

Therefore, a sentence should serve as a deterrent to stop him from repeating such offences. Although there was no tangible damage to the victim companies, the crime committed had affected their computer systems. Therefore, the probation order was quashed and the respondent was sentenced to two months imprisonment on each of the three charges.

The case of *PP* v *Muhammad Nuzaihan* was cited in *Rupchand Bhojwani Sunil* v *Public Prosecutor* (SLR, 2004) where the accused was charged under the Penal Code. In this case, the appellant (Sunil) had misused the Internet by downloading a company's website into his own website with intent to cheat the respondent (victim). He was charged under s417 of the Penal Code (Singapore) and sentenced to 12 months imprisonment by the District Court. On appeal to the High Court, the learned judge Yong Pung How CJ was of the view that '…[t]he current appeal clearly disclosed a large disparity in the nature of the offences committed. *Muhammad Nuzaihan bin Kamal Luddin* involved pure computer misuse, as opposed to the cheating offence in this appeal'. Thus, the sentence in the case of *Rupchand Bhojwani Sunil* was reduced from 12 months to six months imprisonment.

According to judge Chao Hick Tin JA in *Public Prosecutor* v *Syamsul Hilal bin Ismail* [SGHC, 2011], 'In that case (Rupchand), Yong CJ reduced the offender's sentence for cheating (punishable under s417 of the Penal Code (Cap 224, 1985 Rev Ed)) from 12 months' imprisonment to six months' imprisonment for the reason, *inter alia*, that the district judge had over-emphasised the fact of Internet misuse.'

3.2. *The CMA 1998 vs The Penal Code*

The CMA 1998 has several rules attached to it. For example, there is Communications and Multimedia (Rates) (Amendment) Rules 2010 which has been made under subsection 201(1) of the Communications and Multimedia Act 1998. In regulating Internet content, section 211(1) of the CMA 1998 provides: "No content applications service provider, or other person 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". This means, by virtue of section 211(2) of the Act, any person who contravenes the abovementioned section shall commit an offence and if convicted, shall be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or both. The Act further empowers a Content Code to be drafted to deal with offensive or indecent content.

Furthermore, s233 of the CMA 1998 explains on the consequence of improper use of network facilities or network services. If a person is proved to have improperly used a computer to communicate offensive words or threatening others, that act is considered as an improper use of network facilities or network service or applications service. The section provides for the punishment for such offence where it states that 'any person who is found guilty shall be liable to a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding one year or to both'. It was reported that in 2010, 582 investigation papers were opened and probed, 422 of which were under Section 211 and 233 of the CMA 1998 (Malaysia Today, 2011; Singh, 2012). Further, there are 33 cases being investigated under CMA 1998 until March 2012 (Iskandar, 2012). This report shows that the CMA can stand alone and there is no need to refer to the Penal Code.

From the above discussions, it can be said that the CCA and the CMA are beginning to be accepted and applied with the change of time. They can stand alone even without the Penal Code. Nevertheless, the Penal Code is still relevant and is regarded as the comprehensive Code in defining the types of crimes. Hence, the Code cannot be totally ignored.

3.3. *The CMA 1998 vs the Sedition Act 1948*

Internet pornography is not governed by any specific law in Malaysia. But distribution of pornographic materials over websites has been increased and the impact of this activity is very bad especially on children and young persons. According to section 292 of the Penal Code:

> *Whoever sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation makes, produced or has in his possession any obscene book, pamphlet, paper, drawing, painting representation or figure or any other obscene object whatsoever… shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.*

This means that those who commit this act will be charged under the Penal Code and not under Cyberlaw regulation. However, since the website or Internet is used to distribute the materials and that act is considered as distribution of obscene materials online, the question is whether the person or suspect can also be charged under the CMA 1998? This question has not been answered to date.

There are a few cases dealing with sedition. In one case, a preacher from Sarawak had allegedly insulted Islam and the Prophet Muhammad (p.b.u.h) in a video on 'YouTube'. Following this incident the IGP stated that the matter would be investigated under the Sedition Act but no detention has occurred to date (Bernama, 2010b). In another case, a man was arrested and detained when he posted on his Facebook page messages containing insults against the Sultan of Johor and his monarchy (Bernama, 2010c). The man was arrested in November 2009 and a report was sent to Attorney General's office for further action. But in these two instances there has been no clear decision as to what happened thereafter. In February 2012, the Court of Appeal also ruled that the Sedition Act was valid when dismissing Uthayakumar's application to declare that the Act was unconstitutional. He was actually a former Internal Security Act detainee who had been charged in the Kuala Lumpur Sessions Court in December 2007 with publishing a seditious letter the month before on the 'Police Watch Malaysia' website It had been addressed to then-prime minister of Britain, Gordon Brown (The Star, 2012a). Nevertheless, in July 2012, the Prime Minister of Malaysia announced that the Sedition Act will be repealed and replaced by the National Harmony Act. According to him, the decision to repeal the Act was motivated by a desire to find a mechanism that could ensure the best balance between the need to guarantee freedom of speech for every citizen and the need to handle the complexity of plurality existing in the country (The Star, 2012b). But this proposed new law will be tabled in 2013.

However, if Islamic law applies, those who insult Islam may be subjected to section 7 of the Syariah Criminal Offences (Federal Territory) Act 1997 and if proven guilty they shall on conviction be liable to a fine not exceeding three thousand ringgit or to imprisonment for a term not exceeding two years or to both.

3.4. *The CMA 1998 vs the Defamation Act 1957*

There are many cases on Internet defamation. The examples include defamation suits against bloggers Jeff Ooi and Ahirudin Attan. Both were prominent bloggers and the latter was the President of the National Press Club. They were sued simultaneously for both blog posts and readers' comments (South China Morning Post, 2007). The allegedly libellous content included Jeff Ooi's blog coverage of New Straits Times (NST) and its editors' roles in misrepresenting facts, publishing a caricature of the Prophet Muhammad and plagiarism in blog posts in 2006 (Jeff Ooi's blog). Ooi had previously been investigated by the Communications and Multimedia Commission and the police concerning comments a reader posted on his blog that were deemed offensive to the official version of Islam in Malaysia (Zuckerman, 2005).

Other than the above cases, there are several unreported cases on internet defamation including circulation of offensive remarks on Islam Hadhari on a local weblog (Singh, 2004), spreading rumours over the Internet by one veteran singer against another pop singer and the case of Raja Petra Raja Kamarudin, a blogger and an editor of *Malaysia Today* (Mageswari and Samy, 2008). In the case of Islam Hadhari, the blogger was acquitted and became one of the opposition leaders while in the second case the Magistrate's Court of Petaling Jaya decided to grant a discharge not amounting to acquittal to the veteran singer (the defendant) as its defamation charge did not constitute a complaint (Yatim, 2006). Similarly in the case of Raja Petra who was sued for defamation relating to three offending articles posted on his blog. He was charged under section 8(1) of the ISA (now repealed) and was detained in police custody for 53 days but was released on the ground of the detention being unlawful. The Federal Court has also ruled out that he is not guilty (Mageswari, 2010). The obvious reason in the above three cases is that the prosecution failed to establish the offence committed although the charge was made under the Penal Code and other traditional laws. Thus, it seems that relying on the Penal Code *per se* is not sufficient if the case involves misuse of networking facilities or internet. The suspect can just escape liability due to this mistake. What is obvious is that the CMA 1998 was not even applied although there was an element of misuse of networking facilities and services.

After these attempts failed, the prosecutor tried to charge one blogger under s233(1)(a)of the CMA. He was charged of insulting the Johor royal house by posting derogatory remarks on his blog in 2010. However, the prosecution again failed to establish prima facie case against the blogger and as a result, the blogger was acquitted by the Session Court (Singh, 2012). Contrastingly, in another case, an engineer who had posted offensive comments on the Internet against the Sultan of Perak was successfully charged under s233(1)(a) of the CMA and he was found guilty of insulting the Sultan in 2009. He has been given the maximum sentence of a RM50,000 fine and one year's jail for committing such offence (Sharma, 2012). In short, successful prosecution will result with the effective use of the CMA in cases of misuse of networking facilities.

Since blocking of websites seems to be ineffective the MCMC is trying to stretch the application and enforcement of s263 of the CMA 1998 against the Internet Service Providers (ISPs). Under this section the ISPs or the licensee shall use their best endeavour to prevent the network facilities that they own or provide or the network service that they offer 'from being used in, or in relation to, the commission of any offence under any law of Malaysia'. ISPs are expected to 'assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia including, but not limited to, the protection of the public revenue and preservation of national interests'.

3.5. *The Copyright Act 1987 (also known as Copyright (Amendment) Act 1997)*

This Act was the first Act relating to technology and copyright works. The Act was later amended and came into force in October 2011. The latest amended Act is known as the Copyright (Amendment) Act 2000. Since 1987, there are many copyright cases decided based on the Act. An example is that of *Syed Ahmad Jamal* v *Dato Bandar Kuala Lumpur* (CLJ, 2011) where the plaintiff claimed that the defendant had infringed his moral right under s25(2) of the Copyright Act 1987. The court held that section 25(2) of the Act prevents any person

from presenting a work without identifying the author or under a name other than that of the author. Removal of the unique plinth by the defendant had resulted in failure to identify the plaintiff as the author of the works. Hence, the moral right of the plaintiff to be identified as the author of the works had been infringed by the defendant. The court ordered the defendant to pay RM 750,000.00 as damages to the plaintiff's moral right.

There is also a new regulation of the Copyright Tribunal which will be enforced in April 2012. These new regulations of the Copyright Tribunal will involve expanding the jurisdiction of the tribunal on matters relating to payment of royalties to artistes (Bernama, 2012a). The Tribunal which was abolished in 2003 was revived in June 2012 (The Star Online, 2012).

3.6. *The application of other cyberlaws and traditional laws*

The above discussion shows that the CCA, the CMA and the Copyright Act 1987 or Copyright (Amendment) Act 1997 have been referred to in deciding cybercrimes cases. Apart from that in cases of cyber pornography traditional laws such as Film Censorship Act 2002, Child Act 2001 and the Penal Code will apply (Iskandar, 2012). From the above statutes, the Copyright (Amendment) Act and the Penal Code are commonly referred to when compared to others. The Copyright Act is the most popular Act within cyberlaw since there are many copyright cases decided under the Act. d (Azmi, 2004). However, this does not happen to other cyberlaw legislation such as the Telemedicine Act, DSA, ECA, EGA and PDPA. Although e-commerce practices are very much developed in Malaysia and issues on Internet privacy as well as data protection have been discussed in many writings and forums, yet the application and the effectiveness of these laws have not been tested. Only recently, since June 2012, following the Government announcement has the PDPA entered into force and it is expected that the new law will boost e-commerce industry in Malaysia (Bernama, 2012e).

It is also hoped that the PDPA will be able to resolve issues pertaining to breach of privacy. Otherwise, the claim for breach of privacy is hard to win as was illustrated by one telco subscriber who alleged that a telco company (the Celcom Axiata) had released contents of her short message system (SMS) and audio recordings of phone calls to others. The court in this case decided that the plaintiff failed to establish her allegation of breach of privacy due to lack of evidence and the case was dismissed. She was even ordered to pay RM50,000 in costs (Malaysian Insider, 2012). To make matters worse, the Ministry of Information, Communications and Culture has also affirmed that there will be no Freedom of Information Act in Malaysia (Bernama, 2012c).

4. Suggestions

Malaysia may need to refer to cybercrimes cases decided in countries like Singapore and England in order to improve the application of existing cyberlaw. The reason is due to the fact that most cases decided in Malaysia were mainly related to software contracts, admissibility of computer evidence under sections 90A, 90B and 90C of the Evidence Act 1950, infringement of copyright cases and a few cases on hacking. The reason for this lack of domestic legal development is not totally clear but, based on a study, it shows that the application of the CCA 1997 in cybercrime cases has not received a good response from the corporate or business sectors because both sectors are of the opinion that the law cannot assist them to maintain economic reputation. This is indicated by their reluctance or failure to lodge any police reports on hacking committed by their employees. In other words, corporate bodies, especially those on Public Listed Boards, simply will not expose alleged perpetrators and allow them to be sued in a court of law. For them, the company's reputation is the priority (Hamin, 2004). From an early stage there have also been questions about the clarity of CCA 1997 and its failure to accommodate the needs of corporate victims of computer crime (Betty, 1997).

The other reason is that the CCA 1997 focuses on hacking offences and not computer fraud or other cyber-related cases. The computer fraud cases are decided under the Penal Code. This is where traditional law is still relevant to cybercrime. It is suggested that the Malaysian Government might review the existing CCA 1997 so as to accommodate more cybercrime categories. The Penal Code, despite being said to be a comprehensive code, may need to be reviewed so as to accommodate the crimes of the online world. As for CMA, cases decided based on this Act should be published and referred to.

4.1. *Other relevant issues*

Apart from establishing sound laws and regulations other factors such as risk assessment should also be taken into consideration. This method is important in tackling issues on cybercrimes. In fact, the Malaysian Communications and Multimedia Commission (MCMC) has suggested that financial institutions should conduct a comprehensive risk assessment in all relevant areas of business and design suitable safeguards to control the risk and monitor their effectiveness. The risk assessment should be conducted on a regular basis and necessary adjustments made to reduce the risk (Sani, 2004).

5. Conclusion

The efforts taken by the Malaysian government and other organisations are reforming but there are still some issues that remain unresolved, especially regarding the application of cyberlaw. There is no doubt that existing cyberlaw has been promulgated with the intent to regulate cyber activities and to control cybercrime, but it seems that in some cyber-related cases the traditional law still prevails and retains greater recognition than cyberlaw in the application. Further, there is inactive cyberlaw not applied even after several years on the statute book. Questions also arise as to whether, given the delay in implementation, existing cyberlaw is in any case fit for purpose in accommodating new developments in technologies and new forms of modus operandi driven by the former. Not only that, there is the issue on risk assessment which still needs to be emphasised as a means of

implementing computer security. From the above discussion, it is submitted that for cyberlaw to be applied effectively the law needs to be tested and updated where necessary. The enforcement authorities must be able to apply cyberlaw effectively while demonstrating sound knowledge and understanding on the law of evidence as well as criminal procedural law. In short, effective implementation of cyberlaw depends very much on the fitness of the law itself and the readiness of the enforcement authorities to apply it.

Asst. Prof. Dr. Duryana binti Mohamed (*mduryana@ium.edu.my*) *Department of Legal Practice, Ahmad Ibrahim Kuliyyah of Laws, International Islamic University Malaysia.(IIUM)*.

REFERENCES

ACA. Australian regulator leads Asia-Pacific push against spam. Australian Communications Authority (ACA). Media release no. 18–27 April 2005, via ACA, http://internet.aca.gov.au/ACAINTER.65650:STANDARD:662912101:pc=PC_2975; 2005 [accessed 03.03.12].

Allan George, Salter Suzanne. Computer use and misuse. Journal of the Computer Audit Specialist Group (CASG Journal) 1997;7. via University of Portsmouth, http://www.tech.port.ac.uk/staffweb/allang/papers/pub96c.htm#5 [accessed 02.02.12].

Ahzan Azrina. Dikikis rakan siber. at, http://www.bharian.com.my; 20 July 2010.

AsiaOne. Big increase in cyber-crimes. AsiaOne 28 April 2011.

Ashford Warwick. Cyber crime costs UK organizations £2.1m a year, http://www.computerweekly.com/news/2240164639/Cyber-crime-costs-UK-organisations-21m-a-year; 2012.

Azmi Ida Madieha. Copyright cases and commentaries. Malaysia: Sweet &Maxwell Asia; 2004.

BBC News. High-tech crime costs UK Plc £2.4 billion. BBC News. via BBC, http://news.bbc.co.uk/2/hi/business/4412685.stm; 5 April 2005.

Bernama. Copyright Act to come into force in April, says Ismail Sabri. Bernama 2012a. 14 March 2012.

Bernama. Cybercriminals scam victims of RM16m in Q1. Bernama. 18 July 2012, http://www.themalaysianinsider.com/malaysia/article/cyber-criminals-scammed-victims-of-rm16m-in-q1; 2012b.

Bernama. Financial and cyber-crime most prevalent economic crime in Malaysia. Bernama. 13 April 2010 at, http://www/mysinchew.com/node/37655; 2010a.

Bernama. Government has no plans to introduce Freedom of Information Act, says minister, Bernama. New Straits Times 2012c. 13 March 2012.

Bernama. Insult on Islam: government will not keep quiet, Dr Mashitah. Bernama. 27 September 2010, http://www.bernama.com.my/bernama/v5/newsindex.php?id=530695; 2010b.

Bernama. OIC-CERT cyber drill coordination successful in addressing targeted cyber crisis. Bernama. 24 February 2012 at, http://www.cybersecurity.my/en/knowledge_bank/news/2012/main/detail/2160/index.html; 2012d.

Bernama. Held: man with Facebook insulting Sultan. Bernama. 22 December 2010 at, http://www.bernama.com.my/bernama/v5/newsindex.php?id=551839; 2010c.

Bernama. Personal Data Protection Act to be enforced in June. Bernama 2012e. 9 February 2012.

Betty Donna L. Comment: Malaysia's Computer Crimes Act 1997 gets tough on cybercrime but fails to advance the development of cyberlaws. Pacific Rim Law & Policy Journal Dec 9, 1997:351. 7 Pacific Rim Law & Policy Association.

Bologna G Jack, Shaw Paul. Avoiding cyberfraud in small businesses: what auditors and owners need to know. Canada: John Wiley & Sons, Inc; 2000. at 61.

Borneo Post Online. Many white-collar cyber-crimes go unreported. Borneo Post Online. at, http://www.theborneopost.com/?p=95412; 22 February 2011.

Carter David L. Computer crime categories. Law Enforcement Bulletin 1995;64(7):21–6. U.S Department of Justice: Federal Bureau of Investigation (FBI), http://www.fbi.gov/publications [accessed 07.03.12].

Cheng Nicholas. USM develops a better tool to fight hackers. New Straits Times 5 March 2012.

Clifford Ralph D. Cyber-crime: the investigation, prosecution and definition of a computer-related crime. Carolina Academic Press; 2001.

CLJ. Current Law Journal 2011;2:569.

CMA. See subsection (2) of s3 of the CMA 1993 provides, 'If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.' There are similarities in the wordings of s3(2) of the CCA 1997 and s3(3) of the CMA 1993, http://statutes.agc.gov.sg/aol/search/display/view; 1993a [accessed 17.03.12].

CMA. See subsection (1)(a)(b)(2) of s4 of the CCA 1997 is similar to subsection (1)(2)(4)(b) of s4 of the CMA 1993. See also *Navaseelan Balasingam* v *Public Prosecutor* [2007] 1 SLR 767, a case on illegal withdrawal from ATM machines; 1993b.

CMA. Subsections (1)(a)(b) of s3 of the CCA 1997 is similar to subsection (1)(a)(b) of s1 of the CMA 1990. The CMA 1993 also considered such access as an offence under subsection (1) of s3, but the provision under this section 3 of the CMA 1993 is more precise which includes punishment as well; 1993c.

Durbin Lindsay. Effective spam management as a vital component of your content security policy. In: Cybersecurity conference, 3rd August 2004, Kuala Lumpur; 2004.

Eu Jin Foo. Cybercrime activities on the rise. New Straits Times (Computimes) 22 November 2004.

Grabosky Peter. The global cyber-crime problem: the social-economic impact. In: Grabosky Peter, editor. Cyber-crime: the challenge in Asia. Hong Kong University Press; 2005. p. 31–41.

Hamin Zaiton. The sins of the Ss: spamming, spoofing, smurfing and scamming in cyberspace. In: National conference on intellectual property and related rights, 16–17 September 2003, Crystal Crown Hotel, Petaling Jaya; 2003.

Hamin Zaiton. The role and application of the Computer Crimes Act 1997. In: LawAsia IT Law conference, 'evolving legal issues in IT', 26–27 August 2004, Sutera Harbour Bay Resort, Kota Kinabalu Sabah; 2004.

Hamin Zaiton. Insider computer misuse: problems and perspectives. In: First Asia pacific conference on cyberlaw, 8–9 November 1999, University Multimedia (UMTM), Putrajaya; 1999.

IMPACT at http://www.impact-alliance.org/home/index.html; 2012.

Iskandar Eneng Faridah. Cybersecurity NRE executive discourse. Ministry of National Resources & Environment. at, http://www.nre.gov.my/Malay/PusatInformasi/ProgramKampusNRE/CYBER%20%20SECURITY.pdf; 2012, 4 May.

Jeff Ooi's blog. Screenshots at http://jeffooi.com/ [accessed 08.04.12].

Karim Farah Naz. Battling streets crime a priority for government. New Straits Times 28 July 2009. at 1.

Khong Dennis WK. The problem of spam law: a comment on the Malaysian Communications and Multimedia Commission's discussion paper on regulating unsolicited commercial messages. Computer Law and Security Report May–June 2004; 20(3). via ScienceDirect, http://www.science?_ob=Article

URL&_udi=B6VB3-4C82V4P-C&-User=565570&_handle=B-WA-A-A-AZ-MsSAYWW-UU [accessed 03.03.12].
Kye Lee Koi. 15 000 Cases of cyber-crimes last year. at, http://www.nst.com.my/local/general/15-200-cases-of-cyber-crimes-last-year-1.30592; 11 January 2012.
Mageswari M, Samy Florence, A. Detention order unlawful. The Star 8 November 2008:N20.
Mageswari M. Raja Petra is free after Federal Court strikes off Home Minister's appeal. at, http://thestar.com.my/news/story.asp?file=/2010/11/1/nation/20101101100313&sec=nation; 1 November 2010.
Malaysian Insider. Woman loses RM20 m 'leaked messages' suit against Celcom. Malaysian Insider. at, http://www.themalaysianinsider.com/malaysia/article/woman-loses-rm20m-leaked-messages-suit-against-celcom; 16 March 2012.
Malaysia Today. 20 Cybercrime cases under probe. Malaysia Today. at, http://www.malaysia-today.net/mtcolumns/newscommentaries/39878-20-cyber-crime-cases-under-probe; 20 April 2011.
MCMC. MCMC report on a public consultation exercise on "regulating unsolicited commercial messages", http://www.mcm.gov.my/mcmc/Admin/FactsAndFigures/Paper/PC-SPAM-04.pdf; 17 February 2004 [accessed 04.03.12].
Moores Simon. Fighting back against e-crime. at, http://www.zentelligence.blogspot.com/fighting%20Back%20Against%20Crime.pdf; 2004 [accessed 04.03.12].
Mustaza Masami. Action against online abuse. New Straits Times 6 September 2010. at 1.
Mycert. Statistics of cybercrimes in 2008 and 2009. at, http://www.mycert.org.my/en/services/statistic/mycert/2008/main/detail/566/index.html; 2008 [accessed 06.02.12].
Naples Gregory J, Maher Meredith. Cybersmearing: a legal conflict between individuals and corporations. The Journal of Information, Law and Technology (JILT) 2002;2002(2). via University of Warwick, http://www.elj.warwick.ac.uk/jilt/02-2/naples.html [accessed 02.02.12].
New Sabah Times. Cyber security level in Malaysia better than those in developed countries. New Sabah Times 14 April 2009 at http://www.cybersecurity.my/en/knowledge_bank/news/2009/main/detail/1725/index.html. See also tips on internet safety at http://www.esecurity.org.my [accessed 02.02.12].
New Straits Times. Mass web defacement: incidents on the rise and alert issued. New Straits Times (Computimes) Online, <http://www.ctimes.com.my/>; 16 August 2004.
NITC. The NITC Malaysia. at, http://www.nitc.my/index.cfm?&menuid=57; 2012 [accessed 20.03.12].
Patrick Steven. Cybercrimes on the rise – calls for dedicated court to handle such cases. The Star 16 January 2009.
Penal Code. Penal Code is the primary legislation that consists of 115 sections. Section 34 of the Penal Code provides that, when a criminal act is done by several persons, in furtherance of the common intention of all, each of such persons is liable for that act in the same manner as if he did the act alone. Other than Penal Code there is specific legislation such as Dangerous Drugs Act 1952 and Firearms (Increased Penalties) Act 1971.
PP v Jose Wilfredo Sosaya Carrasco. Case number: 62-06-01/2012, Session Court (2), Kuantan, Pahang; 9 March 2012.
Sani Rozana. Public sector braces for more cyber threats. New Straits Times (Computimes) Online. Other reports include the use of computers to commit forgery, like phishing, and harassment through e-mail or web forums, http://www.ctimes.com.my/; 20 January 2005.
Sani Rozana. Fight against phishing: steps to curb identity thefts over cyberspace. New Straits Times (Computimes) Online, http://www.ctimes.com.my/; 21 June 2004.
SGHC. Singapore High Court (Singapore): 272; 30 December 2011.
Shafi Abdul Rahman. ICT security action. at, http://www.mimos.my/wp-content/uploads/2010/07/20090727_N_NST_TU_pg14_12236_ICT-security-action.pdf; 2010 [accessed 20.03.12].
Sharma M Sivanantha. Guilty of insulting Sultan. The Star Online. at, http://thestar.com.my/news/story.asp?file=/2012/6/2/courts/11404932&sec=courts; 2 June 2012.
Shou Sien Wong. Wireless content – the legal and regulatory issues. In: 3rd International cyber laws conference, 2–3 March 2004, Kuala Lumpur; 2004. The CAN-Spam Act came into force on 1 January 2004. It criminalises, among other things, sending multiple commercial e-mail messages with materially false or fraudulent return address.
Singh Sarban. Freed of royal insult charge. The Star Online. at, http://thestar.com.my/news/story.asp?file=/2012/6/1/courts/11395012&sec=courts; 1 June 2012 [accessed 05.06.12].
Singh Sharanjit. Web closing around 'Anwar'. New Strait Times 6 October 2004. 22. The author of such offensive remark used 'Anwar' to identify himself.
SKMM. Regulatory approach to spam. at, http://www.skmm.gov.my/FAQs/SPAM/Regulatory-Approach-to-Spam/Will-Malaysia-be-enacting-new-laws-to-make-Spam-il.aspx; 2012.
SLR. 1 Singapore Law Report: 34; 2000.
SLR. 1 Singapore Law Report: 596; 2004. See also *Navaseelan Balasingam* v *Public Prosecutor* [2007] 1 SLR 767; *Public Prosecutor* v *Law Aik Ming* [2007] 2 SLR 814; *Tan Chye Guan Charles* v *Public Prosecutor* [2009] 4 SLR 5 and *Thong Sing Hock* v *Public Prosecutor* [2009] 3 SLR 47.
South China Morning Post. Newspaper sues internet bloggers for defamation. South China Morning Post. Reprinted at, http://www.asiamedia.ucla.edu/article.asp?parentid=61629; 19 January 2007.
The Star. Cyberspace policeman staying vigilant. The Star 2010a. 9 February 2010.
The Star. Phishing attacks on the rise. The Star 2010b. 14 February 2010. In April 2010, 143 incidents involving phishing sites targeting internet banking sites in Malaysia were referred to the Cyber999 Help Centre of CyberSecurity Malaysia. See "Steer clear of phishing sites", 21st April 2010 at http://thestar.com.my/news/story.asp?file=/2010/4/21/focus/6095783&sec=focus. In 2009, there were 1191 reported crime cases involving internet banking for the first six months. See Loh Foon Fong, "Parliament: 1191 internet banking cases reported in first 6 months", 9th December 2009 at http://thestar.com.my/news/story.asp?file=/2009/12/9/nation/20091209144201&sec=nation.
The Star. Cybersecurity is in good hands. The Star. 30th April 2010 at, http://thestar.com.my/news/story.asp?file=/2010/4/30/focus/6159976&sec=focus; 2010c. The APWG has organised its fifth annual Counter-eCrime Operations Summit (CeCOS V) on 27–29 April 2011 in Kuala Lumpur. During the workshop, CyberSecurity Malaysia COO Zahri Yunos said that the centre handled 3,563 cases in the first quarter of 2011, of which 36% or 1273 cases were related to online fraud, which included phishing and identity theft. In the same period also, the phishing sites have targeted 400 sites of local banks.
The Star. Moore's outlaws, intech. The Star 2010d. 17th August 2010 at IT11. Moore's Law refers to the prediction that integrated circuits will double in transistor capacity about every two years.
The Star Online. Copyright tribunal to be revived in June. at, http://thestar.com.my/news/story.asp?file=/2012/5/16/nation/20120516171106&sec=nation; 16 May 2012.
The Star. Sedition Act a valid law, says court of appeal. 24 February 2012 at, http://thestar.com.my/news/story.asp?file=/2012/2/24/nation/20120224175444&sec=nation; 2012a.
The Star. National Harmony Act replaces Sedition Act 1948. 11 July 2012 at, http://www.nst.com.my/latest/national-harmony-act-replaces-sedition-act-1948-1.106204#; 2012b.

Timbuong Jo. Government agencies taught to handle cyberattacks, intech. The Star 17 August 2010. at IT13.
Utusan Malaysia. Jenayah perdagangan libatkan kerugian RM579 juta tahun lalu. Utusan Malaysia; 3 July 2004. 5.
Wall David S. Crime and the internet. Routledge; 2002 [chapter 1].
Yatim A Hafiz. Sharifah Aini granted discharge. New Straits Times Online 24 January 2006.
Yunos Zahri, Nasir Ahmad. Cyber threats: myths or reality? According to W.J Hoong, the National Sales Manager of Trend Micro Malaysia Sdn. Bhd, the Sasser family virus was estimated by Computer Economics to be causing damage of a whopping US$3.5 billion in 2004, http://www.niser.org.my; 2003.
Zolkepli Farik. Major role for Bank Negara in anti-terrorism academy. The Star 30 September 2010:N16.
Zuckerman Ethan. Global voices blogger Jeff Ooi questioned in Malaysia regarding weblog. Global Voices, http://www.globalvoicesonline.org/2005/02/28/global-voices-blogger-jeff-; 28 February 2005.