Regulatory Framework in Cyber Crime Laws

Roos Niza Mohd Shariff
Executive Development Centre, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia
Tel: 604 – 9285110 Fax: 604 – 9285767
E-mail: roosniza@uum.edu.my

ABSTRACT

The technology age has assimilated each and every one of us in one way or another. With the growth and widespread use of technology information (IT), we have witnessed and shared the fruition of its many new applications, e-commerce and business opportunities. There has also been a corresponding upsurge of a new generation of crimes known as cyber crimes. Cyber crimes or computer crimes are harmful acts committed from or against a computer or network or against information on computers or network. This paper attempts to describe the growing danger and rise of cyber crimes throughout the nations since cyber crimes are transnational nature of cyberspace. The highlight will be on the types of cyber crimes and the current laws available to combat these crimes. By understanding the crimes and the laws governing them, we would be able to appreciate some of the common threats that are often neglected or taken for granted. This paper will end with some recommendations to curb the issues raised.

Keywords: *cyber crimes, cyber laws, e-commerce, computer crimes.*

1.0 INTRODUCTION

The late 1990s and early 2000 witnessed a strong growth of information technology (IT) investment. Technological awareness has been shaping the development and strategies of human resource and major economies in the world. Greater accessibility to computers and communication technology are leading to higher frequency of usage and hence, higher dependency on computers to perform work for many people and organisations. Personal use of computers in chats, sending messages, and business use of computers for online transactions (computerised banking transactions, business transactions and payment of bills at home) show great reliance by people and businesses on digital communication technology.

However, the trend of greater dependency on IT is attracting problems of crimes relating to illegal use, unauthorised access and intrusion of personal and business data, plus intentional sabotage. This paper explores and interprets cyber crimes, the respective laws and the impact of these laws towards cyber crimes. The major focus being the identification of major laws relating to cyber crimes. For these reasons, cases of cyber crimes are explained with the aim to illustrate the impacts of cyber crimes to businesses operations and individuals' livelihood.

2.0 CYBER CRIME

What is cyber crime?

Cyber crimes are crimes that are relating to computers, IT and the Internet technology. In some cases, computer science system is the target of the criminal act, and in other cases, the computer science systems is used as the tool for such crimes. Cyber crimes create many personal problems such as frustration, stress and fear, and business problems such as fatal loss of corporate data and confidentiality. This has led most countries to spend money and time to address this criminal behaviour.

Cyber crimes involve conventional criminal activities committed in a different nature, such as theft, fraud, forgery, defamation and mischief, all of which are conventional criminal activities, using either computer as a tool or a target or both. This definition centers on computers as the mechanism in which cyber crimes are based upon. It means that cyber crimes would include the use of computers as a tool for unlawful acts.

Types of cyber crimes

They are two basic types of cyber crimes; one is where computers are used as the tools for cyber crimes and the other is where the computer is the target for unlawful acts. Examples of computers as tools in cyber crimes are financial crimes (cheating, credit card frauds and money laundering), cyber pornography (pornographic websites and pornographic magazines), online gambling (websites that offer types of gambling via computers and internet), Intellectual Property crimes (software piracy, copyright infringement, trademarks violations and theft of computer source code), forgery (counterfeiting currency notes, postage and revenue stamps using sophisticated computers, printers and scanners), cyber defamation (occurs when defamation takes place with the help of computers, such as through the use of e-mails and web publications).

Instances where the computer is the target for unlawful acts (computers as the criminal targets) are unauthorised access to computer systems (hacking), theft of electronic information, e-mail bombing (sending a large number of emails to the victim, rendering crashing of the victim's email), Salami attacks (insignificant alterations within a computer system, for financial gains and the triviality of the alteration is not noticed by others), virus attacks and denial of service tools - these are tools of attacks to make a particular service unavailable to someone who is authorized to use it.

3.0 REGULATORY FRAMEWORK

Legislations covering cyber crime laws, be it in the form of punishment to the offender or protection to the victim, were enacted to cover each and every types of cyber crimes via the scope of its sections, which are meant to be read exhaustively. Thus, discussion on regulatory framework on cyber crime laws take a few dimensions, namely, the laws governing cyber crimes, the existing and current laws available and legal dilemma in digital revolution in regards to the implementation of these laws.

The laws governing cyber crimes

- **Cyber crime laws in Malaysia**

Similar to other nations, Malaysia has been making attempts to address several cyber and Internet issues relating to illegal cyber activities and protection of property for businesses and individuals. Numerous legislations have been enacted in 1997 to 1998. They are: -

1. Multimedia and Communications Act 1998
2. Multimedia Commission Act 1998
3. Digital Signature Act 1997
4. Computer Crimes Act 1997
5. Telemedicine Act 1997
6. Copyright (Amendment) Act 1997

In Malaysia, the main Act use for combating cyber crimes is the Computer Crimes Act 1997. However, the offences are only described in sections 3, 4, 5, 6, 7 and 8 in Part II of the Act. **Section 3** of the Act criminalizes any intentional access to a computer without authorization. The penalty is a fine up to RM50,000 or imprisonment for the term up to 5 years or both. This covers hacking or any other types of unauthorized access to computer, whether or not security measures were infringed or damage was actually done.

Section 4 goes further by covering unauthorized access with intention to commit a further offence in the form of another crime. Example, gaining unauthorized access to computer with the intention to commits acts of fraud or dishonesty. It is immaterial whether the future offence is to be committed at the same time as the unauthorized access or in the future. However, the Act is silence in terms of whether the future crime has actually been committed or not. This is considered more serious, thus, punishable by a fine up to RM150,000 or a prison term up to 10 years or both.

Section 5 regulates the criminalization of unauthorized modifications. Section 17 of the UK Computer Misuse Act 1990 defined modification as an alteration of any program or data or the addition of any program or data to the contents of a computer (Yaman Akdeniz, 1996). This includes viruses, worms, Trojan horses, logic and time bombs. Violation of this provision is punishable by a fine of RM100,000. Section 5 of the Malaysian Computer Crimes Act 1997 is similar to Section 3 of the United Kingdom Computer Misuse Act 1990. **Section 6** highlights communication as a means of access to a computer to an unauthorized person. The penalty is RM25,000 or 7 years imprisonment or both.

Anyone abets the commission of an offence under the Computer Crimes Act 1997, or does any preparatory to or in furtherance of an offence is guilty under **section 7**. This covers abetting or attempting to commit an offence under the Act. **Section 8** may prove to be the most useful provision both in the prevention of computer crimes and in instilling investor confidence. This section creates a statutory presumption that anyone who has unauthorized custody or control over information held in a computer has obtained unauthorized access to that information. This provision is directed at preventing software piracy and the theft of trade secrets.

Notably, the Computer Crimes Act 1997 does not cover many areas of computer-related activities, whereas, the criminal laws of Malaysia, in particular the Penal Code, do not specifically provide for any computer-related crimes. Therefore, the legal standing of these cyber crime protections must be determined in the context of the existing laws. The main constraint is, the existing laws were not drafted with computer technology in mind and in most cases, is not sufficiently broad enough to encompass the various types of computer-related activities. Consequently, as mentioned by Khaw Lake Tee, et.al., (1996), no matter how odious or nefarious such activities may be in the perception of the policy-makers and the public, they may not constitute unlawful or prohibited behaviour.

- **Cyber crime laws in India**

India is chosen as the country to illustrate cyber laws because India has, among other nations, the best IT skills and software development capabilities. In fact, majority of the highly skilled IT professionals in the Silicon Valley are Indians.

*The law of e-contract: M*ost sections of the contract laws relating to e-commerce in the Information Technology Act 2000 are incorporated from the Indian Contracts Act 1872 and Sale of Goods Act 1930.

Power to search and arrest: Section 80 of the IT Act 2000 grants to a police officer, or any other authorized government officer, the power to enter any public place and search and arrest without warrant any person who is reasonably suspected of having committed or of committing or of being about to commit any offence under the IT Act 2000.

The law of consumer protection: The Information Technology Act 2000 has been silent on rights and protection of the cyber consumers, and the rights and

protection of consumers are only refrered to the traditional Consumer Protection Act 1986 of India (Vivek Sood, 2000).

The existing and current laws available

The current laws available and some existing laws are not enforceable against such crimes. Effectiveness of the regulations can be most difficult to achieve as the issue is about borderless crimes, difficulty to identify stakeholders, lower technological competency of some nations, lack of cooperation, and differences in emphasis and interpretation of such illegal activities. Plus, many of us may not have heard of international conventions and bodies relating to counter illegal cyber activities. This points to the situation that awareness is still remain low in many nations regarding the potential threats and disruptions that can be brought about by those illegal cyber activities.

A good example is regarding the denial of service tools, where the denial-of-service attacks had brought down websites like Amazon, CNN, Yahoo and eBay. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks are a very perturbing problem for law enforcement agencies mainly because they are difficult to trace. Furthermore, these attacks are targeted at sensitive systems and networks. Even when the perpetrators can be traced, international extradition laws may not be effective in bringing them under the authority of the law.

Legal dilemma in digital revolution

A major legal dilemma in dealing with this borderless cyber crime is that individual countries are spending different effort and emphasis to respond. The concerted effort to formulate laws relating to cyber crimes would appear to be an encouraging scenario, but the negative aspect is that the effort lacks general consensus and collaboration to agree to standards and to share efforts to address the cyber issue. A reason to this discrepancy might be that computers and computer networks are at present almost wholly local and national in scope.

The illegal cyber activities, through the Internet technology thus pose many challenges to authorities on how to formulate strategies to regulate them, and at the same time, to ensure security against these illegal cyber activities and terrorism.

Moreover, cyber crimes are illegal and/or non-acceptable activities relating to computers, telecommunication and electronic technology. They can be considered as a new scope to many people. Hence, there are many limitations to conduct regulatory framework accepted by all countries.

The nature of cyber crimes per se is a limitation. Computers, telecommunication and electronic technology are developing at a very fast pace over the last decade and it can be difficult to monitor the types of crimes and their potential impacts. Hence, it is difficult to discuss all types of laws and crimes relating to cyber activities.

Most efforts to formulate laws to deter cyber crimes remain national in nature and this means that individual governments are having their own interpretations, priorities and laws for regulating the crimes. Thus, there are no sufficient standards and shared efforts to address the issues.

4.0 SELECTED CASES

Case 1 – Credit card fraud

In April 2001, the Hyderabad police arrested two persons and charged them under various sections of the IPC and the IT Act (India) for stealing and misusing credit card numbers belonging to others. This case showed the issue of unauthorized access. This is relevant to the Malaysian Cyber Crime Act 1997, Section 3(1) of the Unauthorised Access. Section 3(2) also applies for the intent of the employees who used the credit card details to make financial gains. Punishment under The Malaysian Act would be a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or both (Department of Justice Press Release, May 21, 2002).

Case 2 – Illegal access and criminal extortion

In May 2002, two Kazakhstan citizens were extradited to the United States on charges of breaking into a Bloomberg (provider of financial database services) computer system to extort money from Bloomberg. They sent e-mails to Michael Bloomberg, the company's founder, demanding that he paid them US$200,000 in exchange of details on how they were able to infiltrate Bloomberg's computer system.

This is a traditional extortion case that had occurred via the internet. The unathorised access is intentional, with monetary motive, directing at a website hosted in a foreign nation (the United States). The two Kazakhstans had committed the crime of 'computer sabotage' and 'illegal use of computer systems belonging to other people' (Department of Justice Press Release, May 21, 2002).

Case 3 – Cyber pornography

The Delhi Police Cyber Crime Cell registered a case under section 67 of the IT Act India 2000. A 16-year-old student of the Air Force Balbharati School in New Delhi created a website at the URL www.amazing-gents.8m.net. On this site, lucid, explicit, sexual details were given about various girls and teachers of the school. Pornography in the Internet is the case here. The student was later charged under section 67 of the Indian IT Act 2000 (Department of Justice Press Release, May 21, 2002).

Case 4 – Erasure of corporate data
In February 2002, a former computer network administrator was sentenced to 41 months in prison for causing over $10 million in damages when he deleted all the production programs of a New Jersey-based high-tech measurement and control instruments manufacturer.
(Department of Justice Press Release, Feb 26, 2002).

5.0 THE EFFECTIVENESS OF CYBER CRIME LAWS

The study into the laws relating to cyber crimes so far has faced difficulties in ascertaining the effectiveness of such laws. Major problems arise from following areas.

- Definitions – different definitions or interpretations by different authorities
- Emphasis – different emphasis of applications of such laws
- Effects of cyber crimes – different nations have different priority on the effects and hence punishment to such crimes
- Jurisdiction – the authority to trace, indict and penalise mostly is related to individual nation
- Crimes – crimes committed can come from any source from any physical locations and thus it can be difficult to apply laws of a particular nation to punish
- The means of crime – means and tools to carry out cyber crimes are various and are changing fast, and hence the laws can find it difficult to keep pace in terms of definitions and penalty

6.0 PROBLEMS IN REGULATING THE LAWS RELATING TO CYBER CRIMES

The Asian School of Cyber Laws has suggested many issues relating to the effectiveness of cyber laws. Following highlights two viewpoints of the School.

Difficulty in enforcement of laws universally
When the computer system and data exist in a foreign country, the enforcement of cyber laws by one nation may infringe national sovereignty of another. This matter is complex as different nations would have different interpretations and responses to cyber crimes. For cyber laws to be effective, international judicial cooperation will be necessary but this involves international politics. It also requires establishment of quick devices that allow the investigators of different countries to interact in a legal way. This can be extremely difficult and time consuming.

Problems in the cross-border investigation
It can be difficult to establish a new type of jurisdiction for cyber crimes by just basing on the principle of the conventional territorial (physical location) definition. Thus, the principle of territoriality is not the only principle to be applied to cyber crimes investigation. It means that establishment of jurisdiction should also follow along the principle of nationality of the victim or of the alleged criminal. This is the system which is common in dealing with complex international crimes, but ordinary cyber crimes may not subject to such investigation.

There are other problems in regulating the laws relating to cyber crimes. They are:

- ***Concealment of cyber cases by victims***

Although no one really knows how pervasive cyber crime is, the number of IT-related security incidents is increasing dramatically. Many attacks go undetected, as many as 60% according to some security experts in the Internet. Out of the attacks that are exposed, only 15% are reported to the law enforcement agencies. Most companies that have been electronically attacked were more concern with the loss of public trust and image, plus the fear of encouraging copycat hackers. Therefore the existing laws may not be effective to regulate such diversity and complexity, yet unreported cyber crimes.

- ***Differences in cultures and customs in the global place***

Laws can be difficult to apply effectively for all nations. For example, internet copyrights laws in the United States will not be noticed or enforced seriously in nations where there are little concern nor respect for such copyrights.

- ***Problems of detection, enforcement and evidence***

The major hurdle in bringing the cyber criminals before the court lies in the problems of detection, enforcement and evidence. For example, the chaotic case of intrusion of Parliament websites by the Brazilian hacker (known as "Topeira"), where none of the hackers have been brought before any court of justice.

- ***Side effects of cyber laws***

The target of cyber laws is to regulate cyber activities and to protect rights and properties of individuals and businesses. However, there are some side effects to these laws. As reported in eWeek (2004), cyber laws discouraged, inhibited or limited many aspects of technology development, innovations, applications and businesses. In the United States, there are multiple types of laws relating to cyber activities. Many of these are limiting the freedom of use and innovation. For example, the federal Digital Millennium Copyright Act and state laws known as Super DMCAs (laws that were intended solely to protect intellectual property and copyright) have negative effects on innovation, product interoperability and consumer usage.

7.0 RECOMMENDATIONS

Even though cyber laws have been created and implemented but computers and networks can never be completely protected against crimes. According to eWeek (2004), one of the biggest threats is from regular users such as employees. Although firewalls provide good perimeter control to prevent crime from the outside, procedures and protection measures are needed to protect against internal cyber crimes by employees. Passwords, identification numbers, and tighter control of employees and managers help in preventing internet related crime. No matter how extensive or how sophisticated the electronic surveillance or other form of surveillance against attack by intruders, there is always an element of surprise and non-expectation from the unexpected.

A legal framework, a serious view by the courts and ethics are insufficient even if we have the best of cyber cops. This effort must be topped up by proper security measures. Cyber crime is an international problem requiring a formal system for international cooperation. Extradition and mutual assistance treaties must be put into place fairly quickly which must necessarily take into account the harmonization of laws in different countries and establishing common legal definitions for criminal acts as well as for accidental or negligent misuse of computer systems. All of these changes and improvements must take place with due respect for human rights and fundamental freedoms (http://www.mlj.com/articles/beldue2.htm).

In many nations such as in Malaysia, series of legislation regarding computer-related crimes are provided. The problems arise mainly in terms of enforcement. Therefore, improving the effectiveness of **enforcement** of the laws is the main idea.

Some of the Acts cannot cope with the advancement of computer misuse activities. As such, more effort should be focused in monitoring the changing types and nature of such crimes and their potential harmful effects on individuals and businesses. The existing legislations should be updated and/or amended to reflect the new and changing dimensions of the crimes. For instance, using new technologies to prevent the crime created by technologies, such as encrypted tunneling where an encrypted tunnel allows secure communications across the Internet.

More severe and deterrent sentences should be imposed to the offenders. The relevant legislations must also have the extraterritorial effect to widen the coverage and punishment.

Furthermore, there should be more conventions and joint efforts among nations to encourage awareness and concerted efforts to manage the cyber crimes.

One other way of curbing the issues is to examine the current statutes to determine their sufficiency to combat these crimes. Where loopholes exist, best practices should be applied.

8.0 CONCLUSIONS

Crimes conducted through computers, networks and telecommunication systems are growing in number. Although this may not be prominent or made known in some developing nations, this remains a major concern for individuals and business. Cyber crimes and terrorism are causing financial damages and distress (personal and business levels) throughout the world. National and international authorities are seeking ways to address this issue, to raise awareness among stakeholders, to formulate laws to regulate and to punish the criminals. However, problems relating to cyber crimes are wide ranging and they can be most difficult to define, to contain and be responded to. Furthermore, there are insufficient collaboration and standards among the nations in formulating laws to monitor, deter and punish such crimes. This resulted in a rather slow development in the legal systems which create difficulty in detering IT crimes through the legal systems.

Even though existing laws relating to cyber crimes are various, there can be conflicts among these laws. For example in Malaysia, the implementation of cyber laws such as Multimedia and Communications Act 1998, Multimedia Commission Act 1998, Computer Crimes Act 1997, and Copyright Act 1997 (Amended) are seen as encouraging efforts to address the cyber issues. However, there can be confusion and overlapping among these laws in terms of roles of personnel, scope of authority and definitions of terms. Also, these Acts are relatively new and there can be problems in implementing them – such as some Acts may not have been tested, amended or enforced. The relevant authorities given power to enforce them could lack experience in defining, enforcing and managing them. Only time, continual serious investment and experience shall improve the usability and practicality of these laws.

REFERENCES

Asian School of Cyber Laws. (2004). *Cyber Crime Laws Hurt More Than They Help*. eWeek, http://www.eweek.com/article2/0,1759,1588190,00.asp

Asian Schools of Cyber Laws. (2004). *Tools and Techniques*. Cyber Crimes – Technical Issues. http://www.asianlaws.org/cyberlaw/library/cc/what_cc.htm

Beldue Singh & Annette John. *Internet Crimes*. http://www.mlj.com/articles/beldue2.htm

Communications and Multimedia Act 1998. International Law Book Services, Kuala Lumpur.

Computer Crimes Act 1997. International Law Book Services, Kuala Lumpur.

Department of Justice Press Release. (May 21, 2002). http://www.usdoj.gov

Department of Justice Press Release. (Feb 26, 2002). http://www.usdoj.gov.

Khaw Lake Tee, et.al. (1996). *Laws and Policies Affecting the Development of Information Technology.* Final Report, National Information Technology Council.

Nurhayati Ismail & Hafiza A. Razak (2002). *The Enforcement of Computer Crime Act In Malaysia.* Persidangan Kebangsaan Undang-undang Korporat 2002. Isu & Cabaran Di Era Globalisasi. 12-13 Julai 2002. Pusat Konvensyen, UUM.

_____(2002). *Polis Mula Siasat Kes Ceroboh Laman Web Parlimen.* Januari 30, 2002.
http://www.utusan.com.my/archive, 30th.

Ralph K., Stair M. and Reynolds G.W. (2003). *Principles Of Information System.* Thomson Learning, pp. 620 – 622, p 637.

Vivek Sood. (2000). *Online Learning Centre Cyber Law Simplified.* Online article. Available at: http://www.tatamcgrawhill.com/digital_solutions/viveksood/chap1.htm

UK Computer Misuse Act 1990.

Ulrich Sieber. Available at: http://www.wjin.net/Pubs/2690.htm.

Yaman Akdeniz. (1996).*Section 3 of the Computer Misuse Act 1990: An Antidote for Computer Virus.* Available at: www.webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html