Cyber Crimes: Lessons from the Legal Position of Malaysia and Iran

Nazura Abdul Manap and Hossein Taji

Abstract—**Cyber space offers some new and highly sophisticated opportunities for criminal misconduct and they create potential to commit traditional crimes in a modern way. It has opened the door to criminal behaviour in ways that would never have previously been possible. The existing criminal statute of Penal Code does not to certain extent cope with the possible rapid activities of the computer criminals. Thus, Malaysian government has proactively enacted a cyber-crime related law of the Computer Crime Act 1997 in order to restrain the cyber crimes activities. To the same effect, the Islamic Penal Code of Iran has been amended to incorporate specific offences relating to cyber crimes beginning from 19 November 2008 which came into force on 29 Jun 2009 by approval of the parliament. This law has five (5) parts and fifty five (55) sections with two types of punishments ,i.e, imprisonment or penalty or both. The aim of this paper is to highlight the offences stipulated in the Act in both jurisdictions, and how far do the provisions in such criminal statut*e *contribute in putting a halt to the on line criminal activities.***

Index Term—**Cyber crime, law, Malaysia, Iran**

I. Introduction

We are now living in an enormous society. This happens through a giant neighbourhood, which is made up from networked computers users around the world via the Internet. Malaysian society is not only confined to the citizens or residents of Malaysia, but it indirectly includes people in other countries in the world. This is the encouraging factor of the emergence of cyber-crime. Cyber-crimes are crimes committed virtually through Internet online. This means that the crimes committed could extend to other countries, which is beyond the Malaysian jurisdiction.

Theft, fraud, harassment, pornography, stalking, damage to property are all familiar crimes. Under new guises all are possible using the Internet. The main reason why cyber-crimes seem so important is because it can involve the transfer of large amount of money virtually instantaneously, simply because so many records exist only or primarily on computers. However, this is again too narrow a view of the effects of cyber-crimes. Cyber-crimes are not limited to only money, but also our children and privacy are at risk. In other words, cyber-crimes are even related to most other major issues in computer news nowadays, i.e., intellectual property rights, child pornography, and privacy issues. [1]

Manuscript received February 14; revised April 24, 2012

N. A. Manap is an Associate Professor in the Faculty of Law, The National University of Malaysia (UKM), 43600 Bangi, Selangor, Malaysia.

H. Taji is a PhD candidate in the Faculty of Law, The National University of Malaysia (UKM), 43600 Bangi, Selangor, Malaysia.

II. Computer Crime Issues

Parallel to the launching of Multimedia Super Corridor (MSC) by Malaysian Prime Minister in 1996, the Malaysian government has introduced three new legislation, so-called Cyber Laws. This legislation consists of the Computer Crime Act 1997, the Digital Signature Act 1997 and the Telemedicine Act 1997. The Computer Crime Act 1997 (CCA 97) has come into force on 1st June 2000. It is our hope that with the enforcement of this Act, it will to certain extend, help in curbing the problems of criminal activities occurred in the cyberspace world. The CCA 97 has only 12 provisions which are largely focused on the crime done through or using computers. This includes cyber-crime which committed using online computers. The Computer Crime legislation in Iran is a new law, which has been approved in Iranian parliament on 19 November 2008 which came into force on 29 Jun 2009. This law has five (5) parts and fifty five (55) sections with two types of punishments, i.e, imprisonment or penalty or both. In 2003, the specific law of E Commerce has been introduced to ensure secure communication of information in electronic intermediaries. In Chapter Four of the said law, it provides offences on fraud and forgery. As the Computer Crime legislation aims to cover the type of crimes which will not be supported by the previous law, therefore, crimes such as information theft, data alteration and data destruction, program damage caused by viruses, Trojan horses, worms, and logic bombs, hacking and unauthorized access are spelled out in this law. The said law outlaws the practice of illegal copying of domestic software, but it offers no protection for foreign products. All these crimes are punishable by fine or imprisonment or both. Those who develop or introduce any kind of computer virus will obtain more severe punishment as other information age law-breakers.[2]

In discussing the above mentioned offences a word computer is important to be clarified here. The CCA 1997 was one of the little legislation worldwide to define a computer for its purpose. The meaning stated in section 2 of CCA is very wide so as to cover all technological advances. Despite of its wide coverage it is ambiguous in the sense that how far this definition covers the function of microprocessor contained in the microwave oven or refrigerator. Can one be charged under this Act if he gets into the microprocessor system without authorisation? It still remains unanswered.

III. Related Offences in the Malaysian Computer Crimes Act 1997

The Act creates three main offences, those are:-

1. Unauthorised access to computer materials or also known as hacking (Section 3 of CCA 1997);
2. Unauthorised access with intent to commit or facilitate commission of further offence or also known as cracking (Section 4 of CCA 1997);
3. Unauthorised modifications of the contents of any computers (Section 5 of CCA 1997).

A. Obtaining Unauthorized Access to Computer Materials.

Section 3(1) of the CCA 1997 provides a person is guilty of an offence if :-

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
(b) the access he intends to secure is unauthorised, and ;
(c) He knows at the time when he causes the computer to perform the function that is the case.

Therefore, if a third party gets access to the websites by hacking into the system, he is committing the offence of unauthorized access to computer materials. In order to fulfil the first requirement above a hacker must seek to perform any function to secure access to a program or data held on a computer. The phrase "to perform a function" is the term in question here. To what extent can one be regarded as causing the computer to function? As defined in section 2 of the CCA 1997, function includes logic arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer. This clearly includes an act of rebooting the computer. The words communication and telecommunication show that this subsection is not limited to a crime committed to direct access. Meaning that, the offence may be committed equally by a person who obtains direct access to a computer system itself or by more advance hacker who secures access by means of internet communication via telephone connection.

The second requirement of this section deals with unauthorised access. Whether access is unauthorised access or not is defined in section 2(5) of CCA 1997 in the following terms :-

(a) he is not himself entitled to control access of the kind in question to the program or data; and
(b) he does not have consent or exceeds any right or consent to access by him of the kind in question to the program from any person who is so entitled.

The first category is clear. It refers to a person who definitely has no right over the computer system or database, get access without permission from the owner. In order to prove one's access is unauthorised, the intention of the computer's owner has to be made clear. For example, the provider may be quite willing to allow any visitor to get access to certain categories of information but may reserve other categories for a more limited class of users for instance the registered students. For the purpose of showing the service providers intention of not disclosing certain parts of information to anyone who visits the site, they will be required to take steps to bring any use limits to a user's notice. This can be done by requiring a password or identification code upon making initial contact with the computer system. A party who does not possess such information should be aware that he is not authorised to proceed further.[3]

The second category of unauthorised access deals with a person who, in the first place, is authorised to use a password but has no power to permit other person to make use of it. This can be referred to relationship between website service provider and the students, whereby a student who is entitled to access the computer system is actually not entitled to control access and therefore cannot transfer his rights to a third party. In other words, one who possesses the user name and password to access the websites are prevented from sharing the said entry code with other unauthorized persons.[4]

As provided in section3 (3) of the CCA 1997 , a person guilty of an offence under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

B. The Ulterior Intent Offence

Section 4 of the CCA 1997 deals with what is referred to as the ulterior intent offence. A person shall be guilty of this offence if he secures unauthorised access with the intention of either commit further offence involving fraud or dishonesty or which causes injury as defined in the Penal Code or to facilitate the commission of such an offence, whether by himself or by any other person.

This section, basically must involve two types of offences. Firstly, the offence of unauthorised access, and secondly the act of committing or facilitating further offence involving fraud, dishonesty or causing injury. The later is in other words depending on the offence mentioned in section 3 of the CCA 1997. An accused could not be convicted under this provision if there is no element of unauthorised access. For example, if a person gets access into the website which has no sign or notice of user's limit either in a form of password or special code or a person lawfully possesses a password to enter to the system, in these situations he is considered as authorised user. He then, proceeds further by leaving a fraudulent message or spreading a defamatory material in the website. In such a case, even though he has committed further offence, he is not liable under section 4 of the CCA 1997 as there is a lack of element of unauthorised access.

Section 4(3) provides that a person guilty of an offence under this section shall on conviction be liable to a fine not exceeding one hundred and fifty thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

C. Unauthorized Modification of the Contents of any Computer

A person shall be guilty of an offence if he does any act which he knows will cause unauthorised modification of the contents of any computer. The meaning of authority applies in a way similar to that in relation to the section 1 offence. The modification is unauthorised, if the person causing it is not entitled to determine whether the modification should be made and he does not have the consent of any person who is so entitled. Modification is extensively defined in section 2 of the Act. A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer:-

(a) any program or data held in the computer concerned is altered or erased;
(b) any computer or data is introduced or added to its contents; or
(c) any event occurs which impairs the normal operation of any computer, and any act that contributes towards causing such a modification shall be regarded as causing it.

Therefore, if someone enters into the websites and change the data or information contains in it, he can be convicted of this offence.

Section 5(4) states that a person guilty of an offence under this section shall on conviction be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding one hundred and fifty thousand ringgit 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.

D. Wrongful Communication

A person shall be guilty of an offence if he communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorised to communicate. This offence may occur in the transaction particularly in a case whereby a user of the E-learning site gives the entry code to a person who is not duly authorised by the owner of the site.

Section 6(2) provides that a person guilty of an offence under this section shall on conviction be liable to a fine not exceeding twenty-five thousand ringgit or to imprisonment for a term not exceeding three years or to both.

E. Abetment and Attempt

Abetting the commission of or attempting to commit or doing any act preparatory to the commission of the offences in the Act is an offence as stated in section 7(1) of CCA 1997. Besides that, a person who does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence. For this particular offence the imprisonment imposes shall not exceed one-half of the maximum term provided for the offence. This section has made both attempt and preparatory as offences under this Act. In criminal law, it is obviously difficult to draw a line between the preparatory stage and attempt. Nevertheless the offence of attempt may require a test of proximity in establishing the said offence, whereas preparation to commit an offence is not considered as an offence according to section 511 of the Penal Code, but it has been made an offence under section 7(2) of the CCA 1997.

F. Presumption

A computer owner who has in his custody or controls any program, data or other information which is held in any computer or retrieved from any computer which he is not authorised to do so is deemed to have committed the section 3 offence unless proven otherwise. This section stipulates that anybody who possesses in his computer data or program which was obtained unauthorisedly, is committed unauthorised access whether he has knowledge or otherwise. This offence can be charged under section 3 of the Act. The word "unless the contrary is proved" can be interpreted as a strict liability offence. Even though, the owner of a computer which contained unauthorised materials has no knowledge of the unauthorised contents, he is still liable due to the strict liability nature of the offence.[5]

IV. Legal Position of Iran

There are eight (8) main offences in the computer crime legislation. Every each of the offences will be discussed in the following paragraphs.

A. Unauthorized Access

A computer owner who has in his custody or controls any program, data or other information which is held in any computer or retrieved from any computer which he is not authorised to do so is deemed to have committed the section 729 Islamic Penal Code of Iran (Chapter on Computer Crimes) offence unless proven otherwise. This section stipulates that anybody who possesses in his computer data or program which was obtained unauthorisedly, is committed unauthorised access whether he has knowledge or otherwise. According to this section the unauthorized person will be sentenced to 3 month to 1 year imprisonment or will be fined from 5,000,000 riyal to 20,000,000 riyal or to both.

B. Unauthorized Listening on Matters Relating to Government

This offence deals with the act of listening to a communication relating to government affairs. The person involves in this offence may be punished 6 months- 2 years imprisonment or fine 10,000,000 riyal to 40,000,000 riyal or to both.

C. Spying Activities Relating to Government

This provisions is applicable when someone accesses and obtains data kept in a computers belong to government or listening to a confidential communication between government officials without authorisation. A person guilty of this offence can be punished for 1 year to 3 year of imprisonment and penalty of 20,000,000 riyal to 60,000,000 riyal or to both.

D. Forgery

There are two types of forgery stipulated in this section. First, is the modification of digital document, second, falsification of credit or debit cards. Any person who is convicted under this section can be imprisoned for 1 year to 5 years or penalty of 20,000,000 riyal to 100,000,000 riyal or to both.

E. Theft

This offence may occur when someone steals data or information from other person's computer without authorisation. A person guilty of this offence can be imprisoned for 91 days-1 year or 5,000,000 riyal to 20,000,000 riyal or to both.

F. Fraud

An unauthorised person who is using Internet or telecommunication with an attempt to obtain any properties or documents for himself or anyone else is committing an offence under this provision. On conviction, the offender must return the money to the right owner and imprisonment of 1 year to 5 years or penalty of 20,000,000 riyal to 100,000,000 riyal or to both.

G. Obscene Materials

A person makes available obscene materials on the Internet or sell or buy the said material is committing an offence under this section. The punishment is an imprisonment for 91 days to 1 year or 5,000,000 riyal to 40,000,000 riyal or to both.

H. Defamation

This section deals with defamation via the Internet in the form of video and/or audio presentation as well as picture. On conviction the offender can be imprisoned for 91 days- 2 years or 5,000,000 riyal to 40,000,000 riyal or to both.[6]

V. Issues of Jurisdiction

A. Malaysian Position

The transborderless nature of computers in transmitting and receiving data takes no account of national boundaries. Criminal activities committed through computers on-line will normally involve people from different countries. The question arises which legal system might have jurisdiction. The CCA 1997 includes the answer of the question in section 9 of the Act. This provision explains on the application of this section, whereby any person in any nationality or citizenship committed offences at any place outside Malaysia is within the Malaysian jurisdiction provided that the computer program or data is in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at material time. Obviously this section has given a vast jurisdiction to the enforcement unit. But problem may arise in enforcing the provision to hackers who resides outside Malaysia. This will interfere with a particular country's jurisdiction.[7]

B. Iranian Position

Unlike Malaysia, there is no specific provision relating to jurisdiction of Iranian authority over a person who is not a citizen or resident of Iran. In any such event, the normal process of extradition is applied, in which only countries which have extradition agreement with Iran will normally cooperate on this matter.

VI. Conclusion

The enforcement of the CCA 1997 effected from the beginning of June 2000 should be seen as an apparatus in combating the acute problems of cyber-crimes. The problems occur in the traditional laws as discussed before, are no longer exist as the new Act has got rid of the "difficult to establish" elements, which renders the relevant provision inapplicable. The offence of unauthorised access, for example, does not require the element of moveable property or corporeal property which is not appropriate to the nature of the digital crime. These three main offences in the CCA 1997 may overcome the problems in the traditional laws. However, the provisions in the CCA 1997 create difficulties in their own way. For instance the definition on a word "computer" is not clear on whether or not it includes other computer based product. The application of provision on the ulterior intent offence is limited to an act which incorporates element of unauthorised access, it does not stand alone, furthermore, the section also cross refer the offences stipulated in that section to the meaning provided under the Penal Code. This will defeat the purpose of enacting the CCA 97, which was initially legislated to solve problem brought about by the old statute. Besides that, the offence of unauthorised modification is referring to an act of a person who modifies computer materials without authorisation, what happen if the modification was done by a person who is authorised but exceed the permission granted to her. The ridiculous part of the Act is section 8 on presumption, whereby the owner of a computer which contained unauthorised materials has no knowledge of the unauthorised contents will still liable due to the strict liability nature of the offence. This liability will easily be imposed on the cyber cafés owner, who rents out his computers to the customers which is very unfair. The provision on jurisdiction of the Act is just like a dream that never come true, since it relies substantially on the cooperation of the other countries, unless and until harmonisation is made to harmonise the legal protection for cyber transaction internationally. The enforcement of the domestic legislations would not be easy without the cooperation from all countries which link to each other via the Internet networking. To amend the problematical part of the provisions, as discussed above, is the best solution. Responsibility for criminal matters has traditionally been regarded as national matter. Cyberspace, however, is no respecter of national boundaries. Our Computer Task Force may find it hard to impose our law on hackers or perpetrators outside Malaysia. There is urgent need for international cooperation and coordination in resolving the cyber-crimes problems. In contrast, the Islamic Penal Code of Iran (Chapter on Computer Crimes) is at its infant stage. It is not yet tested extensively in the court of law. However the existence of the said provisions to certain extent gives right to the enforcement unit to take action towards the computer offender.

References

[1] D. Bainbridge, *Introduction to Computer Law*, 3rd edn, Pitman Publishing, London. 1996.

[2] Edited By Chris Reed, *Computer Law*, 3rd Edn, Blackstone Press Limited, London, 1996.

[3] D. Bainbridge, *Introduction to Computer Law* (4th Edition). Pearson Education Limited: England, 2000.

[4] D. Rowland and E. M. Donald. *Information* Technology *Law*. Cavendish, 1997.

[5] A. A. Rahim, and N. A. Manap, Jenayah Berkaitan Dengan Komputer: *Perspektif Undang-Undang Malaysia, Dewan Bahasa Dan Pustaka, Kuala Lumpur*, The Computer Crime Act 1997, 2004.

[6] Islamic Penal Code of Iran (Chapter on Computer Crimes).

[7] Z. M. Yusof, N. A. Manap, and M. Mohd, *Komputer,Etika and Sosial,* Mc Graw Hill, Kuala Lumpur, 2002.

Nazura Abdul Manap is currently attached with Faculty of Law, Universiti Kebangsaan Malaysia (The National University of Malaysia). She was born in Segamat Johor, Malaysia on 29 September 1969. Her list of qualifications is as below:
Ph.D (Law), International Islamic University Malaysia (2008), LLM (Lond), November 1996.
Faculty of Laws Queen Mary and Westfield College, LL.B (Hons) (UKM), August 1993 She has been involving in the area of information technology law and intellectual property law for almost 16 years. Her expertise is shared with the public through her publications on these areas. Amongst others are "*Jenayah Berkaitan Komputer: Perspektif Undang-undang Malaysia*" (Computer Related Crimes: A Malaysian Perspective) published by Dewan Bahasa dan Pustaka, Kuala Lumpur and a text book of "*Teknologi Maklumat dan Komunikasi: Undang-undang , Etika dan Sosial*" (Information Technology: Law, Ethic and Social) published by McGraw Hill Education, Kuala Lumpur used by the students in the Faculty of Science and Information Technology , UKM. Her devotions in these fields substantiates through her continuous commitment by organizing national seminars on cyber laws in the year 2000 followed by a seminar on Intellectual property in 2001. She also contributes in encouraging public awareness of intellectual property rights and educates officers and people related to IP through her tour around Malaysia with the cooperation of Intellectual Property Training Center under Malaysian Intellectual Property Office (Mypo). Her involvement in this area has been recognized by Regional Center of Arbitration Kuala Lumpur (RCAKL) through her appointment as penalist (arbitrator) of domain name disputes resolution in 2003.