# POLICING CYBERCRIME AND CYBERPORN: INTERNATIONAL AND MALAYSIAN EXPERIENCES[1]

**By Abu Bakar Munir & Sonny Zulhuda[2]****

[1]Major parts of this paper was first presented at the national seminar on 'Cybercrime dan Cyberporn dalam Perspektif Hukum Teknologi dan Hukum Pidana,' on 6-7 June 2007, Semarang, Indonesia.

[2]** Abu Bakar Munir (abubmunir@yahoo.com) is a professor at the Faculty of Law, University of Malaysia, Kuala Lumpur Malaysia; Sonny Zulhuda (zulhuda@yahoo.com) is a lecturer and researcher at the Cyberlaw Center, Multi-media University, Cyberjaya, Malaysia.

## 1.0. INTRODUCTION

Sixteen years after being revolutionized by the invention of the World Wide Web, the Internet now becomes a common platform of over one billion users in the world who embrace into the cyberspace to exchange information, trade communications and execute commercial transactions. In this sense, the WWW founder Sir Tim Berners-Lee might have reached his prime objective in that the idea of cyberspace becoming a two-way transactional medium had been well achieved; when writing information is as simple as reading it (*The Economist*, 10/03/2007). The benefits are already acquired by Internet users; from scientific researchers to trade merchants, from university students to corporate managers, and from government officials to mothers at home who explores new recipe. However, Sir Tim may has never imagined that today's

cyberspace would also have achieved another 'reputation' of being a notorious criminal frontier where stealing data is as easy as acquiring it rather legally. The truth is that the Internet is already very helpful for malicious minds who wish to pursue their malicious intention.

This is where cybercrime gains its limelight. It has filled up so many pages of stories in books, journals, as well as magazines and newspapers. It loaded speakers with so many words to say in conferences and forums. Similarly it has laden legal fraternity with mounting jobs from enacting laws, amending them, and putting them into the realm of enforcement.

Different words have been used by legislatures in the world for the cybercrime, which includes 'computer misuse' (e.g. UK, Singapore, Brunei), 'computer crime' (e.g. Malaysia), 'cybercrime' itself (e.g. Australia), or a rather specific 'Internet law' (e.g. in Japan). All these terms reflect to a criminalization of certain acts that involve computer or computer system, either as medium or as the target or both. Ferrera (2001) describes cybercrime as any illegal act that involves a computer, its systems, or its applications. It is any intentional act associated in any way with computers where a victim suffered or could have suffered a loss, and a perpetrator made or could have made a gain. Meanwhile the US Department of Justices refers to cybercrime as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution.

## 2.0. BENCHMARKS IN UNDERSTANDING 'CYBERCRIME'

Anyone who looks into the semantic nature of cybercrime would have to look at benchmarks. These benchmarks seek to set proper understanding of the issue and thus enable us to take appropriate actions in formulating its legal framework.

*Cybercrime is a crime.*

Philosophical debates aside, crime in its most practical and pragmatic nature is the acts from which the perpetrator assumes criminal liability and therefore deserves penal sanctions. Crime is therefore limited to the acts which are declared to be a 'crime' by the law of the state. For this reason, crime may differ from one country to another: depending on whether or not such act is considered as crime by the law in that particular state. Killing cow, for instance, for whatever reason, is a crime in Nepal, but not in Malaysia. Consuming certain types of drugs is crime in Malaysia but not in the Netherlands. In certain part of China, an unreasonable horning is set to be a criminal offense. While same-sex marriage is a crime in many countries, it is legal in some other parts of the world.

Likewise, cybercrime can differ from one place to another, depending on whether or not certain types of action have been criminalized in such country. On this point, the most obvious diversity one can find is in the area of online content regulation. While an online pornography is considered a crime in Malaysia, it can be seen a reflection of one exercising his freedom of expression in America. Conversely, spamming per se can be a straight offense in America but it is not necessarily so in Malaysia (For instance,

according to Malaysian Communications and Multimedia Act 1998, in order for the spammers to be prosecuted, it has to pass, among other things, 'annoyance' test).

*Cybercrime affects cross-board targets*

In order to understand cybercrime more properly, one also needs to highlight that it is not an exclusive type of crime. Traditionally, crimes are divided into certain distinctive categories, such as *crime against body* (includes murder, manslaughter, infliction of injuries, attack and harassment, criminal defamation, as well as attack on modesty), *crime against property* (includes theft, robbery, misappropriation, wrongful conversion, damage to property, extortion, cheating and criminal breach of trust), *crime against public tranquility* (includes causing public disturbance, acts against public norm and morality and public policy) and last but not the least, *crime against the state* (such as treason, inciting hatred against the king or authority, and conspiracy to rebel). These categorizations are useful to enable the state to identify the interests and/or party(s) that are at stake in any criminal incidents so as to the appropriate suitable punishments and/or remedies.

Cybercrime, on the other hand, is a common term that blends the above traditional categories into one umbrella. Thus one can find under this term topics belonging to crime against body such as cyber harassment, cyber stalking and online defamation; crime against property such as online fraud, phishing, identity theft, online extortion, sabotage to computer networks, or even the intrusion to computers or computer networks; crime against public tranquility such as online pornography, online child pornography, cyber-sex services, or hatred emails; and also crime against the state that includes cyber terrorism. The bottom-line here is, with the convergence of technologies represented in the cyberspace phenomenon, crime has also been converged along and take place in the cyberspace with a common name of 'cyber crime.'

*The role of computer in crime*

Given the above benchmark, so what is it that commonly binds the diverse crimes together under one umbrella? This is the third point one needs to understand: which is the significant role of computer or computer system in the pursuance of crime. An Australia-based cyber crime practitioner Lim (2002) reckons that there are three distinct roles computer can play in any criminal case. First, computer becomes a target of an offense. This occurs when the criminal act was targeted at causing unauthorized intrusion, modification, or damage to computers or computer system. This includes hacking, web defacing, distributed denial of services, spreading virus and worms (well, creating/making them may not necessarily be an offense itself!), and also creating damage to computer systems by sabotage or otherwise. Secondly, the computer acts as a storage device that facilitates albeit minimally. Here the computer may be incidental to an offense, but still significant for the enforcement purposes. For instance, drug traffickers or money launderers may store data pertaining to

their transactions or criminal partners in electronic form and stored in computer system. The third role, in which computer plays more significant role is when the computer itself is used as a medium for the crime. This includes instances of online fraud, cyber porn, online harassment, unlawful sale on the net of prescription drugs or obscene materials and unauthorized interception of online communications. In line with this benchmark, an online infringement of intellectual property rights can also add to the list of cybercrime under the third category.

## 3.0. GLOBAL PRESCRIPTION FOR A GLOBAL PROBLEM

### 3.1. UN Convention Against Transnational Organized Crime 2000

Even though criminal law is subject to the local criminalization of offences as described in the earlier paragraph, there is a growing consensus that certain types of crime are given a global recognition. This is due to two-fold factors: the cross-border implication of such crime and the fact that certain crimes are perpetrated by cross-border organized criminals. This global crime reputation is currently enjoyed by criminals involved in money-laundering, global terrorism, as well as in illegal trafficking of gun, drugs and human.

In 2000, cyber criminals have surfaced in the international crime scene albeit insufficiently elaborated. This is by virtue of the introduction of the UN Convention Against Transnational Organized Crime (the TOC Convention) in December 2000. A missed opportunity it may be, the TOC Convention unfortunately does not include any substantive cyber criminal offence in its scope. Article 3.1 mentions that it applies to the criminal offences arising out of four offences, namely, participation in an organized criminal group, money laundering, corruption and the obstruction of justice. The TOC Convention, however, provided in article 3.2 that an offence is transnational in nature if it fulfills either of the following characteristics:

1. It is committed in more than one State;
2. It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
3. It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
4. It is committed in one State but has substantial effects in another State.

This characterization of a transnational crime can help at least the set up another framework for cyber crime which can aptly fit into the above nature. Indeed, cyber crime is a global problem, and therefore requires global effort to cure or prevent it.

Meanwhile, article 29(2) of the TOC Convention expressly refers to the methods for combating the misuse of computers and telecommunications networks (Broadhurst & Grabosky, 2005).

Its Article 29(2), among other things, mentions:

"Each State Party shall, to the extent necessary, initiate, develop or improve specific training programmes for its law enforcement personnel, including prosecutors, investigating magistrates and customs personnel, and other personnel charged with the prevention, detection and control of the offences covered by this Convention. Such programmes may include secondments and exchanges of staff. Such programmes shall deal, in particular and to the extent permitted by domestic law, with the following:

(h) Methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology..."

The TOC Convention is outstanding because it provides for future mindset and framework in dealing with transnational criminal offences. Nevertheless, due to the absence of criminalization of certain offences specific to cyberspace, this Convention may have done little except in terms of international cooperation and enforcement where it has laid down quite significant platform.

### 3.2. Council of Europe's Convention of Cybercrime 2001

Barely one year later, there is a light of hope arising in the land of Europe for the future cybercrime law at international level. The member countries of the Council of Europe (COE) together with other governments from Canada, South Africa, Japan and the United States drafted and signed a first multinational treaty on cybercrime called the Council of Europe's Convention of Cybercrime 2001. This Convention sets forth broadly four distinct substantive criminal offences, which are;

1. Offences against the confidentiality, integrity and availability of computer data or systems.
2. Computer-related offences
3. Content-related offences
4. Offences involving the infringement of intellectual property and related rights.

*Offences against the confidentiality, integrity and availability of computer data or systems*

The first category, i.e. offences against the confidentiality, integrity and availability of computer data or systems, covers almost typically all cybercrime that makes computers or computer systems (including data, network, software and hardware, and greater telecommunications infrastructure) as the target of the crime. The bottom line is this category of crimes put either of three pillars to information security at stake. Those three pillars are confidentiality, integrity and availability. This often-dubbed 'CIA' principle has been long known to the information security practitioners as adopted in the globally-accepted British Standards of Information Security Practices (BS7799) and later adopted to the ISO 17799 on the similar title (Whitman & Mattord, 2003). The role of law towards these three principles can be summarized in the following table:

| | |
|---|---|
| Confidentiality | The law seeks to ensure that information is accessible only to those authorized to have access. |
| Integrity | The law is concerned with the maintenance of the accuracy and completeness of information and processing methods. |
| Availability | The law is also required to give assurance that authorized users have access to information and associated assets when required. |

In this first category of substantive offense, the Convention specifically provides for certain types of criminal offences such as illegal access, illegal interception, data interference, system interference, and misuse of devices. It is worth noting here that the above terms are very generic in nature. One should not confuse them with latest terms that sound more techie and sophisticated but actually refers to similar nature substantively. Furthermore, these new words are coined from time to time in order to reflect different methods used by perpetrators. Hence, for example, the terms hacking, cracking, cyber intrusion and online trespass are all reflecting unauthorized or illegal access; while the terms cyber-stalking, cyber espionage and cyber voyeurism may involve illegal interception; and the terms web defacing, distributed denial of services (DDOS) attack and cyber sabotage may well fit the data or system interference. It is submitted here that these generic words should be used in the text of laws instead of the variant offences. This is to avoid the laws from being too technical and becoming quickly obsolete.

*Computer-related offences*

As opposed to the first group of offences, the second category refers to the group of criminal acts that involve the computers as medium of the crime. It specifically refers to two biggest problems, i.e. computer-related fraud and computer-related forgery. These two types of cyber crime are self-explaining, and may also cover variety of methods and variants that include online fraud, phising, email and sms scams, online banking scam, carding, etc (Abu Bakar Munir & Siti Hajar Yasin, 2007). Nevertheless, this provision seems to be too limited. In fact, there are a lot more offences which are computer-related than fraud and forgery. This gap has been addressed in some local cyber crime legislations with the criminalization of 'unauthorized access to further criminal act' like the one found in the laws of UK, Singapore and Malaysia.

*Content-related offences*

As the sub-title suggests, this group of offences concern with the online content. It is noteworthy here that when it comes to content, the global community as reflected in the Convention drafters and signatories can not approve more than the boundary of children pornography.

That is why this category only touches various activities pertaining to the provision of online content that depicts children as sexual objects.

This restriction of content-related offences can be viewed with a strong demand to maintain freedom of speech in the cyberspace. The US Supreme Court in the case of American Civil Liberties v. Reno in 1996 commented, among other things, that 'there is governmental interest in protecting children from harmful materials... but that interest does not justify an unnecessarily broad suppression of speech addressed to adult. Having said that, content-related offences are very much local in nature, thus can differ significantly from one jurisdiction to another. What is an approved content in one place can be greatly opposed in another. This explains why, for example, a global online clips portal 'You-Tube' had recently received complaints from Thai government for its video clip that is regarded insult to the monarchy's King. Many Muslim countries do not tolerate online content that depicts the Prophet Muhammad. Meanwhile many European countries criminalize the content that suggests denial to the Holocaust. This is a continuous debate over a controversial idea of online content regulation, where the idea of 'offensive content' is not an easy task for globally-framed regulation (Deibert, 2006; Quimbo, 2003).

*Offences involving the infringement of intellectual property and related rights.*

This last category of the substantive offences under the Cybercrime Convention strengthens the already existing global legal frameworks under the administration of WIPO that protect the family of works eligible under the boundaries of intellectual properties. These include works protected by copyright, patent, trademarks, industrial design and database right. This area of law is worth reminding due to the increasing ease caused by digital technology to inflict the infringement of copyright, for example, in the cyberspace. Due to this challenge, many countries worldwide had introduced either a new law of amendment to existing law that expands the coverage of copyright infringement to those that occurs electronically.

### 3.3. The European Union Initiatives to Combat Cyber Crime

In January 2001, the European Commission adopted a Communication on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime." The Communication discussed the need for and possible forms of a comprehensive policy initiative in the context of the broader Information Society and Freedom, Security and Justice objectives for improving the security of information infrastructures and combating cybercrime.

With the Communication, the Commission outlined four-pillar strategies and policy programs considered fundamental in the fight against cybercrime, i.e.:

1. The adoption of adequate substantive and procedural legislative provisions to deal with both domestic and transnational criminal activities.

2. The availability of a sufficient number of well-trained and equipped law enforcement personnel.

3. The improvement of the co-operation between all the actors concerned, users and consumers, industry and law enforcement.

4. The need for ongoing industry and community-led initiatives.

Apart from policy level, the Commission has also outlined a legislative reform to address specific areas of substantive criminal law in the area of high-tech crime. Three proposals for Council Framework Decision have been presented for approximation of criminal law on child pornography on the Internet, racism and xenophobia and attacks against information systems (hacking, denial of service and viruses). Negotiations on these instruments are still going on at Council competent instances, while the European Parliament has already been consulted. A fourth proposal will come soon which will address mutual recognition of pre-trial orders to obtain evidence. The main focus of the proposal will be on general judicial co-operation in criminal matters, but the proposal will also address the specific issues associated with cyber-crime investigations.

It is worth noting here that the effort which has been seriously taken by the European Union is based on a regional platform. This is one step closer to an international benchmarking and full cooperation. Similar initiatives should also be considered by other regional communities such as APEC and ASEAN. This is again because many cybercrime enforcement have failed due to the extra-territorial nature of the offense thus requires a close cooperation and mutual assistance.

## 4.0. CYBERCRIME LEGISLATION IN SOME JURISDICTIONS

The progress that is ongoing in the Europe and international level is also taking place in many individual countries in Asia. Some of them have already legislated laws on cyber crime as early as 1993 (Hong Kong and Singapore) and 1997 (Malaysia). Some of these legislations were influenced by the UK Computer Misuse Act 1984 due to the fact that they were part of English Commonwealth countries. The summary of those laws is presented here derived from various sources.

| Country | Legislation | Categories of Cybercrime |
|---|---|---|
| China | The Criminal Law of the People's Republic of China, Chapter VI Art. 285-287. Computer Information Network and Internet Security, Protection and Management Regulations 1997 (Art.4-5). | Invasion of computer information system in selected crucial sectors; unauthorized modification of computer data; causing denial of service; creating malicious and destructive programs; use of computers for crime such as fraud, theft, breach of official secrets. |
| Hong Kong | Computer Crimes Ordinance 1993 | Extends definition of criminal damage to property' to include 'misuse of a computer' i.e. unauthorized function, altering, erasing or adding any program or data; prohibits access to computer with criminal or dishonest intent.. |
| | Control of Obscene and Indecent Articles Ordinance | Concerning the distribution of pornographic material on the Internet. |
| | Gambling Ordinance | Prohibiting gambling on the Internet other than under the auspices of the Hong Kong Jockey Club. |
| Singapore | Computer Misuse Act 1993 (amended 1998) | Prohibiting unauthorized access to computer material (s.3); access with intent to commit offence or facilitate commission (s.4); unauthorized modification (s.5); unauthorized use or interception of computer service (s.6); unauthorized obstruction of ise of computer (s.7); unauthorized disclosure of access code 9s.8); offences involving protected computers (s.9). |
| Australia | Cybercrime Act 2001 (amending the Criminal Code Act 1995) | Covering unauthorized access or unauthorized modification of restricted data; unauthorized modification of data with intent to cause impairment; aggravated offences; unauthorized impairment; unauthorized impairment of data held on disks, credit cards or other device used to store data by electronic means; ancillary offences (i.e. abetment, corporate liability etc.) (ss.477-478). |

| | | |
|---|---|---|
| Japan | Unauthorized Computer Access Law (Law No. 128 of 1999) | Covering prohibition of unauthorized computer access (art.3,8); AND the facilitating of unauthorized computer access (e.g. by leaking or stealing other's passwords or security hole attack) (art.4,9). |
| | The Penal Code (Law No. 45 of 1907) | Amendments to the Penal Code both in 1987 and 2001 include criminalization of computer fraud, illegal production of electro-magnetic records for payment (including that of credit card and bank card fraud) (ss.161-2); obstruction of business by destroying computers (s.246.2). |
| India | Information Technology Act 2000, Chapter XI. | Covering offences of causing damage to computer source code (s.65); hacking (s.66); publication of obscene electronic information (s.67); offences relating to the digital signatures and the Controller of Certifying Authorities (s.68,71,73,74); failures to assist government agency in decryption upon their request (s.69); accessing (or attempting to access) secure access to protected system (s.70); breach of confidentiality and privacy 9s.72). |
| Republic of Korea | Criminal Code (Law No. 5057 of 1995) | Falsification or alteration of public and private electromagnetic records (art.227-2, 232-2); interference with business (art.314); fraud by use of computers, etc (art.347-2). |
| | Promotion of Utilization of Information and Communications Network Act (Act No. 5986 of 1999) and | Impairing data, etc (art.28); impairing protective measures (art.29); unauthorized disclosure (srt.30). |
| | Computer Program Protection Act (Act No. 3920 of 1986) | |

| | | |
|---|---|---|
| Brunei Darussalam | Computer Misuse Order 2000 | Unauthorized access to computer material (s.3); access with intent to commit or facilitate offence (s.4); unauthorized modification (s.5); unauthorized use of interception of computer service (s.6); unauthorized obstruction of use of computer (s.7); Unauthorized disclosure of access code (s.8); offences involving protected computers (s.9). |
| Malaysia | Computer Crimes Act 1997 | Unauthorized access (s.3); unauthorized access with criminal intent (s.4); unauthorized modification (s.5); wrongful communications of means of access (s.6). |
| | Communications and Multimedia Act 1998 | Fraudulent use of network facilities/ services (s.232); improper use of network facilities/service (s.233); unauthorized Interception and disclosure of communications (s.234); damage to network facilities (s.235); prohibition of offensive content for communications and multimedia industry (s.211). |

## 5.0. CYBER CRIME AND CYBER PORN IN MALAYSIA

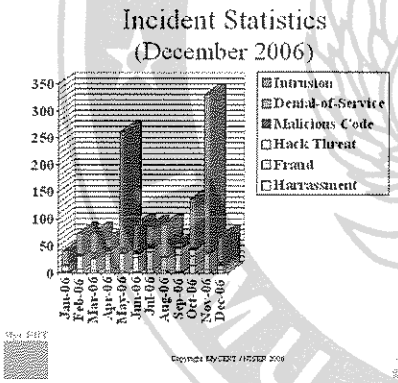
As mentioned in the preceding table, Malaysia has already passed some sets of specific cybercrime laws which mainly are embodied in the Computer Crimes Act 1997 and Communications and Multimedia Act 1998. Meanwhile, the Penal Code, even though has never been amended specifically to adjust with cyberspace medium, has occasionally been used by the law enforcement to charge criminal offences using or involving computer or the Internet as medium. Some other laws are also significant in this sense, i.e. Sedition Act and Internal Security Act. The later Act had been used by the Police in recent years to charge people who spread rumors and stories deemed causing public furor and disturbances. This includes two disturbing emails circulated widely; one was telling about bombs to explode in the town of Kuala Lumpur, and the other was spreading rumors of upcoming riot in KL caused by angry illegal immigrants (*The Star*, 19/12/2002). In these two cases there was no doubt that public tranquility and peace had been significantly disturbed thus provided the Police with grounds to take action.

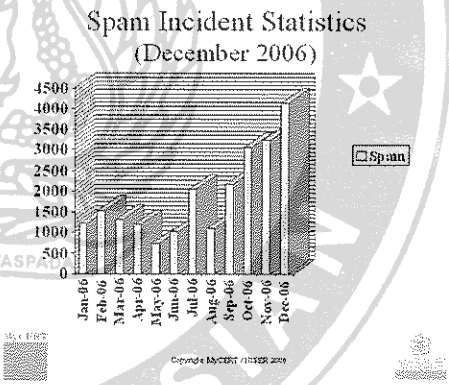
In one high-profile case involving a Malaysian singer Siti Nurhaliza in 2004-2005, the Police had also invoked section 499 of the Penal Code which deals with the offence of criminal defamation. The defamation in issue in this case was

an email that was widely circulated which suggested lots of defamatory statements against the young celebrity (*The Star*, 20/9/2007). Even though the court finally discharged the case, it was a clear indication that online defamation for now can and will be dealt with by the Malaysian Penal Code.

The above cases are among the few cybercrime-related cases that made their way to the court of law especially that involve the use of traditional laws. However, up to date, there has not been any prosecution or charge laid in the court that imposed the cybercrime-specific laws mentioned above. This is an irony because Malaysia had already had the law in place from a decade ago.

This situation is nevertheless not because there is no incident of cybercrime that may invoke liabilities under the cybercrime-specific laws. According to the report by the Malaysia's Cyber-security Centre (formerly known as National ICT Security Response Centre or NISER), the attack to Malaysian computers and Internet is a regular casualty (Abu Bakar Munir, 2002). In the latest data of year 2006 itself, there was reported a high number of 1372 incidents involving online harassment, online fraud, hack threat, malicious programs, denial of service and intrusion. Meanwhile, spamming alone in that year recorded more than 22,000 incidents (refer to Diagrams below).




| | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Harassment | 3 | 7 | 4 | 4 | 4 | 3 | 6 | 4 | 3 | 14 | 6 | 5 |
| Fraud | 9 | 23 | 22 | 32 | 31 | 26 | 34 | 21 | 31 | 19 | 30 | 9 |
| Hack Threat | 3 | 1 | 2 | 5 | 0 | 6 | 5 | 3 | 12 | 10 | 2 | 2 |
| Malicious Code | 1 | 6 | 10 | 7 | 12 | 8 | 6 | 5 | 2 | 4 | 3 | 4 |
| Denial of Service | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 0 |
| Intrusion | 26 | 36 | 35 | 15 | 215 | 47 | 34 | 57 | 8 | 89 | 288 | 47 |
| **TOTAL** | 42 | 73 | 73 | 63 | 262 | 90 | 87 | 90 | 56 | 138 | 331 | 67 |

| | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Spam | 1227 | 1538 | 1323 | 1200 | 743 | 1021 | 2059 | 1115 | 2182 | 3082 | 3245 | 4145 |

Sources: http://www.niser.org.my

Given the statistics above, one big question surfaces as to how had been these incidents addressed. The absence of prosecution against these cyber criminal offences therefore does not lie on the absence of law. This is important to note that having had law per se will not guarantee cyber crime is well taken care of. Law is yet fundamental to provide a platform for enforcers to move on, and to move from. Obviously, the implementation of law requires another set of tools. Issues such as harmonization of laws, evidentiary and investigation issues, as well as extra-territorial cooperation are equally fundamental. The later factor is very crucial because apparently many of the offenders that launch cyber attacks are either based in foreign country or having originated the attack from server outside the country. Therefore, international cooperation is vitally important.

Equally fundamental is a rather non-legal issue of capacity building of the law enforcement officials. The Malaysian Police Force had significantly geared themselves up to be more prepared in dealing with cybercrime cases by establishing a special section under the commercial crime division that deals with crimes involving computers or IT. All these remind us again to the recommendation of the European Council when it comes to the issue of implementing the cybercrime law as discussed above. Emphasizes are given to the adoption of adequate substantive and procedural legislative provisions to deal with both domestic and transnational criminal activities, and the availability of a sufficient number of well-trained and equipped law enforcement personnel. This recommendation was also followed by the initiative to improve the co-operation between all the actors concerned, users and consumers, industry and law enforcement.

Admittedly, the way to have full implementation of cyber crime laws in Malaysia is still long to achieve, depending on variety of reasons mentioned above. It is a valuable experience to share with other countries that do not yet have any cybercrime-specific law. Enacting the law is only the beginning. Equally important is to provide a strong platform for law enforcers.

## 6.0. CYBER PORNOGRAPHY AND THE INDUSTRY'S SELF REGULATORY FRAMEWORK

In Malaysia, the offence relating to pornography is dealt with in section 292 of the Penal Code which makes it an offence, among other things, to sell, lets to hire, distribute, publicly exhibits or in any many puts into circulation obscene materials for which a three-year imprisonment can be invoked with or without fine. Section 293 imposes heavier punishment for the above acts that are targeted to young persons.

There have been incidents where some local celebrities had ever been subject to sexual depiction thus causing great disturbance to the artiste. Those cases were also dealt with under the law of defamation. However, to date, there has not been any decision reported from court that prosecutes local website owners due to publication of obscene materials.

Reluctance to prosecute based on the content in the Internet is perhaps an indirect manifestation of Government's policy towards a free Internet in Malaysia. Such a national policy not to censor the Internet is clearly stated in the preamble of the Communications and Multimedia Act 1998. This is partly an attempt by the Government to support the big project of Multimedia Super Corridor, which the Government hopes to attract as much foreign investment as possible in the area of IT, communications and multimedia industries.

Therefore, the Government of Malaysia had emulated some other countries' initiatives such as Australia in providing a self-regulatory framework where rather loose guidelines are given for the industries to follow and comply with. This is reflected in the passing of the Malaysian Communications ad Multimedia Content Code ('Content Code') which is a self-regulatory set of principles.

### 6.1. The Content Code for Multimedia Industry in Malaysia

The Content Code is a model of self regulation among industry and is drafted by members representing all the key industries. Its drafting is provided by section 213 of the Communications and Multimedia Act 1998 which mentioned that a content industry forum (to be designated according to section 212) shall prepared a content code that includes model procedures for dealing with offensive or indecent content.

It specifically lists down several matters that may be addressed in the Content Code:

(a) The restriction on the provision of unsuitable content;

(b) The methods of classifying content;

(c) The procedures for handling public complaints and for reporting information about complaints to the Commission;

(d) The representation of Malaysian culture and national identity;

(e) Public information and education regarding content regulation and technologies for the end user control of content; and

(f) Other matters of concern to the community.

Although compliance is voluntary, as it is the industry's own regulation, there is no perceived problem of lack of bindingness as this Code is drafted by the industry players to bind themselves. Compliance with the Code brings a number of benefits e.g. it will be a defense against any prosecution, action or proceeding of any nature, whether in court or otherwise. As the likelihood of industry players of being sued or charged for hosting illegal or unlawful content is clear, taking note of their obligation under the Code will prove to be a wise choice (Ida Madieha, 2004).

The Code itself spell out several general principles which are reflective of the Malaysia's policy objective on national information infrastructure. Those principles are:

(a) There shall be no indecent, obscene, false, menacing or offensive content.

(b) The need to maintain a balance between the desire of viewers, listeners and users to have a wide range of content options and access to information on the one hand, and the necessity to preserve law, order and morality on the other.

(c) The need to respect cultural, ethnic and religious, gender, socio-economic status diversity in Malaysia.

(d) Particular attention is to be given to content that is created for children and in which children are portrayed.

As for the classification of offensive and prohibited materials, the Content Code first refers to the penal section of CMA 1998 (section 211) which specifically prohibits content that is indecent, obscene, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass any person. The Code further provides that it requires Code subjects to ensure that material disseminated (e.g.via the Internet) does not include anything which offends good taste or decency; is offensive to public feeling, is likely to encourage crime or lead to disorder, or is abusive or threatening in nature (The Code, Part 2, Art. 1.2).

One wonders what will be the standards by which content is measured. For this issue the Code provides that such content, when measured, will be viewed in context of the country's social, religious, political and educational attitudes and observances, as well as the need to accommodate global diversity in a borderless world (The Code, Part 2, Art. 1.3).

With regards to cyber pornography, the Code specifically mentions two distinct but related types of offensive content which are closely related to pornographic nature, i.e. indecent content and obscene content.

### 6.2. Indecent Content

Indecent Content is material which is offensive, improper and against current standards of accepted behavior. This category is divided into two further grouping, i.e. Nudity and sex & nudity. It strongly mentions that nudity and sex scenes cannot be shown under any circumstances, except if there is an approval by the Film Censorship Board.

In a country where nudity is not something which is tolerated by the public, it is not surprising that nudity comes first in the list of prohibited content (Ida Madieha, 2004). As explained in the Code, the reason why nudity is forbidden is because it offends accepted standards of decency. This proposition should also be viewed with some justifications that have been drawn in section 292 of the Penal Code; in particular in the context of works of art, the culture of a particular society, for educational purposes or in the course of science or medicine.

### 6.3. Obscene content

Obscene content has been described as content that gives rise to a feeling of disgust because of its lewd portrayal and is essentially offensive to one's prevailing notion of decency and modesty. The test of obscenity, as further provided by

the Code, is whether the content has the tendency to deprave and corrupt those whose minds are open to such communication. Among the classes of content that falls within this category are:

- Explicit sex acts/pornography
- Child pornography, and
- Sexual degradation

According to this section of the Code, any portrayal of sexual activity that a reasonable adult considers explicit and pornographic is prohibited. The restriction equally applies to the portrayal of sex crimes including rape and bestiality even if such acts were consensual or described through animation (Part 2, Art 3.1(i)).

Another major concern is child pornography. The Code goes absolutely clear that any form of child pornography is strictly prohibited (Part 2, Art 3.1(ii)). That includes the depiction of any part of the body of a minor in what might be reasonably considered a sexual context, and any written or visual and/or audio representation that reflects sexual activity with a minor no matter how implicit.

The Code goes further to prohibit the portrayal of anybody as mere sexual objects or demean them in any such manner (Part 2, Art 3.1(iii)). As Madieha (2004) reckons, these prohibitions, as strict as they may be, would have to be seen in the context of the national policy on mass communication i.e. the need to preserve the social values and ethical fabric of the society, especially that the Eastern values are far more conservative and value laden that their Western counterparts.

### 6.4. How Does the Code Work?

First of all, it is important to know the parties to whom this Code is applicable. To that question, most of the industry players in the cyberspace would be subjected to the Code. This includes the Internet Service Providers (ISP), Internet Access Service Providers (IASP), Internet content hosts, web page developers, access providers of webcast and streamed content, online content aggregators, and last but not the least, the link providers (Part 5).

The Code also mentions that it shall apply to all content made available in the content industry in the networked medium. The parties will be exempted from liability if they have neither control over the composition of such content nor any knowledge of such content (Part 5, Art. 2.1). In this respect, they can be called an innocent carrier. Nonetheless, this does not exempt them from adhering to certain measures where required. This is where the Code provides certain administrative measures to be complied with each concerned Code subject, depending on the degree of control they possess over the online content.

### 6.5. All Parties Cooperation

Stemming the outflow of 'unsuitable content' requires the cooperation of all parties. From the illustrations given on this, the Content Code requires that that all parties must do their part. No one can claim that it is not within his/her control to do so, he/she is expected to do whatever is possible within his/her control. The last example given in the

Code is illustrative of this point (Part 5, Art. 10.3):

> *Scenario 3:*
>
> *If Z (an ISP) receives a notification from the Complaints Bureau, it must notify X (Content Host) to remove the content within a period ranging from 1 to 24 hours. The period prescribed is at Z's discretion. In this instance, Z gives X 12 hours to remove the content. X may either remove the prohibited content itself or direct W (third party content providers) to remove the content.*
>
> *If the prohibited content is not removed within 13 hours, Z can suspend or terminate X's access to the Internet. If X is not Z's subscriber, Z will not be required to take any measures.*

However, in the examples given, all the parties involved are Malaysians. The main weakness of the Content Code is that it does not regulate foreign parties. The Code does not stipulate the event of foreign content hosted by Malaysian industry players, nor local content hosted in foreign lands. In this manner, the Code fails to take into account of the borderless nature of the Internet. Nor is the Code considering the fact that Net-proprietor often forum shop in the Internet and place their server in locations out of reach of local laws and regulation.

## 7.0. CONCLUSION

As seen in the preceding sections, policing cyber crime requires more than just a penal approach. While a semantic understanding of what constitutes cyber crime is very essential for every stakeholder in addressing the issue, a series of systematic approach requires serious consideration. First, it requires the harmonization of legal and regulatory frameworks at national level with those exist in international arena. Thus the initiative to take cyber crime up to a multilateral and joint convention ought to be supported. This harmonization of law should be seen comprehensively to include not only the criminalization of standard offences, but also the international cooperation in the investigation as well as enforcement of the law itself.

Secondly, given the fast-developing of the information technology, the industry ought to be given a chance and role to self-regulate within the framework of agreed laws and rules in a given country.

The experience of Malaysia may serve as a lesson on how the mechanism could be worked out, despite some weaknesses (Ida Madieha, 2004). Obviously, this co-regulatory process, i.e. between the administrative authority and the industry, would open door for an inclusive regulatory framework where the industry and technology would still be able to grow strongly. The self-regulatory framework is therefore a reflection of both order and innovation.

Finally, all these initiatives should also be supported by an initial and continuous public awareness and administrative

preparedness. Without these, our effort to police the crime and pornography in online environment would meet a stumbling block.

## REFERENCES


Abu Bakar Munir. 2002. "Cyber-Terrorism: The National and International Legal Initiatives." Paper presented at *Jagat Cyber Law Seminar II on Cyber-Terrorism in the Age of Information*, Kuala Lumpur, Malaysia.

Abu Bakar Munir & Siti Hajar Mohd. Yasin. 2007. "Would the Phishers get Hooked?" Paper presented at *BILETA 2007 Annual Conference* at Hertfordshire, UK, 16-17 April 2007. Accessed at 1/6/2007 at http://www.bileta.ac.uk/Document%20Library/1/Would%20the%20Phishers%20get%20Hooked.pdf

"Anti cybercrime legislative proposals on Council table." accessed on 1/6/2007 at http://ec.europa.eu/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm

"Convention on Cyber Crime," accessed on 1/6/2007 at http://conventions.coe.int/treaty/en/Treaties/Html/185.htm

"UN Convention Against Transnational Organized Crime 2000," accessed on 1/6/2007 at http://www.unodc.org/palermo/convmain.html

Broadhurst, R. & Grabosky, P. (ed.) 2005. *Cybercrime: the challenge in Asia*. Hong Kong: Hong Kong University Press.

"Communications and Multimedia Act 1998 (Act 588)," available at http://www.cmc.gov.my

Deibert, Ronald. "The Geopolitics of Asian Cyberspace," article in *Far Eastern Economic Review (FEER)*,6 December 2006.

Ferrera, (ed.). 2001. *Cyberlaw: text and cases*. Ohio: Thomson Learning.

Franda, M. 2001. *Governing the Internet: the emergence of an international regime*. Colorado: Lynne Rienner Publisher, Inc.

Ida Madieha Abdul Ghani Azmi. "Content regulation in Malaysia – Unleashing missiles on dangerous websites." *Journal of Information, Law and Technology (JILT)*, 2004(3), 15 Dec 2004.

Julian Ding. 1999. *E-commerce law and practice*. Malaysia: Sweet & Maxwell Asia

Lim, Y.F. 2002. *Cyberspace law: commentaries and materials*. Victoria: Oxford University Press.

Quimbo, Rudolfo Noel S. 2003. *Legal and Regulatory Issues to the Information Economy*. UNDP-APDIP.

"The Malaysian Communications and Multimedia Content Code," available at http://www.cmcf.org.my.

"Watching the web grow up," article in *The Economist*, 10/03/2007, pp. 27-28.

Whitman, M.E. & Mattord, H.J. 2003. *Principles of information security*. Massachusetts: Course Technology.

## BIODATA OF THE AUTHORS

**1. Prof. Abu Bakar Munir, LL.B, LL.M**
(abmunir@um.edu.my)

Abu Bakar Munir is a professor of law at the Faculty of Law, University of Malaya, Malaysia. Besides teaching, he has been a consultant to many governments including to the Dubai Government for the Dubai Internet City project (2000-2001), the Government of Malaysia for National Information Security Policy development (2005), and for the Government of the Republic of Indonesia for Personal Data Protection Law (2006) and the Internet Content Code (2007). He has been consulted by many private entities in Malaysia and overseas. He is also a member of the United Nations Working Group on Internet Governance and Policy; and Council member of Asia Pacific Privacy Charter Council.

Prof. Abu Bakar Munir has published several books and numerous articles on ICT law and policy including on 'Cyberlaw: issues and Challenges' (1999), 'Personal Data Protection' (2003) and 'Internet Banking Law' (2004). He has also been invited to speak at conferences in Malaysia, US, UK, Australia, Kingdom of Saudi Arabia, UAE, Greece, Indonesia, Singapore.

**2. Sonny Zulhuda, LL.B, MCL**
(zulhuda@yahoo.com)

Sonny Zulhuda, 31, completed his LL.B (Hon) (Bachelor of Laws) and MCL (Master of Comparative Laws) at the Faculty of Law, International Islamic University Malaysia. He is currently completing his Ph.D theses in the same institution in the area of 'Information Security Legal Framework for the Protection of Information Assets.' His Master dissertation was on the law of personal data protection in the European Union, the US and Malaysia.

He is an academic member at the Faculty of Management, Multimedia University, Cyberjaya, Malaysia, where he teaches law subjects including cyberlaw, multimedia law, law for engineers, media law and commercial law. He is also a member of Cyberlaw Centre at the same University. Besides teaching, he is a law consultant at Jakarta-based Center for Regulatory Research (CRR) and Kuala Lumpur-based legal consulting firm. He has been engaged in legal drafting and consultancies by some government agencies in Malaysia and Indonesia, and been invited to speak at conferences in Malaysia, Singapore, Brunei Darussalam, Indonesia, Australia, UAE and the Kingdom of Saudi Arabia.