高知工科大学
KOCHI UNIVERSITY OF TECHNOLOGY

Towards a Secure and Sustainable Critical Information Infrastructure(CII) : A Study on the Policy and Legal Frameworks in Malaysia

著者	Zulhuda Sonny
journal or publication title	Society for Social Management Systems Internet Journal
volume	6
number	1
year	2010-03
URL	http://hdl.handle.net/10173/1794

TOWARDS A SECURE AND SUSTAINABLE CRITICAL INFORMATION INFRASTRUCTURE (CII) – A STUDY ON THE POLICY AND LEGAL FRAMEWORKS IN MALAYSIA

Sonny ZULHUDA
Multimedia University

***ABSTRACT*:** The increasing reliance of critical infrastructures (such as those operating the national communications, energy, transport, and defence systems) on a computerized and networked environment imposes an enormous security task for both their operators and users. The fact that attack to critical infrastructure is not merely an ordinary criminal matter but rather an issue of national security makes it more urgent for policy-makers to come up with policies or laws addressing various issues ranging from information sharing to public-private cooperation, from technical solutions to security procedures, and from public awareness to law enforcement. Looking at the scope it covers and the role it plays, the law on critical information infrastructures is so critical not only because it is part of national security measures, but also because the law may well determine the level of national readiness for landing a global investment. This is true because major business processes are now dependent on the secure information technology tools and networks. The biggest task ahead for policy-makers is therefore to prepare the best legal framework to protect the country's critical information infrastructure and, at least, to manage and minimise the security risks that surround a networked environment. This paper hypothesizes that security risk management of the critical information infrastructure can not be effectively sustained without a comprehensive framework that consists of, among others, good policies and legal framework. In Malaysia, the legal framework on CII can be found in several pieces of legislation. This paper seeks to discuss the role of the law especially on the restriction of access to and movement in the perimeters of CII as well as the law on computer and network security.

KEYWORDS: critical information infrastructure, legal framework

1. INTRODUCTION

The increasing reliance of critical sectors on the computer networks and information system provides an enormous and unprecedented task. As one commentator described, for the first time in history, an individual armed with nothing more than technical expertise, a computer system, and a network connection could theoretically bring a nation to its knees (Condron, p. 42). The fact that an attack to critical infrastructure is not merely an ordinary criminal matter but rather an issue of national security makes it more urgent for governments worldwide to come up with the necessary policies, plans or laws addressing issues ranging from information sharing to public-private cooperation, from criminal laws to national security, and from public awareness to law enforcement.

The protection of CII has been an international

concern. It was reported by the OECD in May 2008 that many countries have national plans or strategies for protecting critical infrastructure. These strategies generally define 'critical infrastructure' as physical or intangible assets whose destruction or disruption would seriously undermine public safety, social order and the fulfilment of key government responsibilities. Such damage would generally be catastrophic and far-reaching. Sources of critical infrastructure risk could be natural (e.g. earthquakes or floods) or man-made (e.g. terrorism, sabotage).

This concern is natural given the fact that we gradually step into an electronic environment where most documents are being digitised and transactions computerised, such as what is happening with revenue collection and many other applications. Given the security challenges that face electronic environment such as this, we are left with one nagging question, 'how secure are those systems?' The answer to this question will undoubtedly have a huge implication on the life of the community and country as a whole.

2. THE NATURE OF PROTECTION OF CII

2.1 Scope and definition of CII

The term 'critical information infrastructure' (CII) has been given different definitions and scope in different countries. Countries put it in their own perspective depending on the national needs and circumstances. It was reported by German agency (*Bundesamt fur Sicherheit in der Informationstechnik*: 2004), whereas it is possible to identify some common structural elements between countries, the measures taken so far, the functions performed by the responsible organisations and the degree of protection achieved to date remain widely different. The term CII itself involves some terminologies worth deliberating. These include the term 'critical', 'infrastructure, and 'information infrastructure'.

2.1.1 'Critical'

What makes the protection of CII an important national security interest is its 'criticality' criteria. CII is about the reliance of a nation or public to those information assets. It must be the information assets which are so enormously important to the extent that the loss, lack or inefficiency of which would lead to a serious impact.

Countries vary in their perception of how serious is serious. It may involve a "major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life" as defined by the Centre for the Protection of National Infrastructure (CPNI), UK. In the US, criticality is associated with the debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Condron, p. 406). Meanwhile, according to the National Information Security Center of Japan, such criticality is consigned to the "great disruption of people's social lives and economic activities". Malaysia, on the other hand, views criticality on the "severe impact that may be caused to national economic strength, national image, national defence and security, government capabilities to function, public health and safety" (See: CNII Portal Malaysia).

The above observation shows that 'criticality' has various dimensions but all share the common nature of being the utmost public and national concern. Arguably, the differences originated from different public policy adopted by each country.

2.1.2 'Infrastructure'

The word 'infrastructure' lexically means "the basic structures and facilities necessary for a country or an

organisation to function efficiently." It is observed that the meaning and scope of the word used in the plans, strategies and laws on critical information infrastructures by various governments do not depart from its dictionary meaning in general.

In many countries CII policies cover tangible and intangible assets and production or communications networks. Australia, for example, refers to "physical facilities, supply chains, information technologies and communication networks." The United Kingdom refers to 'essential services and systems including physical and electronic.' The US refers to the 'system and assets, whether physical or virtual.' Slightly uncommon proposition is however found in Germany ('organisations and institutions') and Japan ('business entities providing highly irreplaceable services'). Meanwhile, Malaysia refers to 'assets, systems, and functions.'

2.1.3 'Critical Information Infrastructure'

The term 'critical information infrastructure' (CII) refers to infrastructure which is related to information and information assets. For example, a civil aviation sector comprises of certain infrastructure including airplanes, personnel, navigation system, information and communications systems, towers and airports, administrative as well as regulatory infrastructure – this all constitutes the critical sector of the aviation system. CII is one part of these: it is all about the information and communications system operated for and by the aviation system. In this respect, the protection of critical information infrastructure refers exclusively to the security and protection of the IT connections and IT solutions within and between the individual infrastructure sectors.

The Australian Government describes critical information infrastructure as 'a subset of critical infrastructure, comprises those communications, information and other technologies and systems used to underpin Australia's economic activities and delivery of key government services. In Malaysian Government's perspective, the National Cyber Security Policy (NCSP) was outlined to address the risks to the Critical National Information Infrastructure (CNII) which comprises of 'networked information systems of the ten critical sectors.' Therefore it is noted that CII includes the information systems (information, communications and computer networks) used by each designated critical infrastructures such as banking and finance, broadcasting and telecommunication, energy, water services, transport, health, emergency services, defence, etc.

2.2 Key elements of CII protection

In the protection of critical information infrastructure, several issues require proper attention such as the public-private cooperation, clear job distribution, and transparent national system as well as social and industrial awareness.

The inclusion of private sector is imperative. Based on the report by the Bundesamt fur Sicherheit in der Informationstechnik of Germany, approximately 90% of national critical infrastructures are actually in the hands of private sector. Those companies are also arguably best placed to assess what systems and sub-systems within their own business require special protection. Therefore, it is more strategic and effective for the purpose of control and enforcement.

There is an urgent need to avoid duplication or overlapping of functions between organisations and agencies. Therefore, clarity of functions, responsibility and procedures (such as procedures for information, cooperation and reporting) is essential.

On the other hand, there is also an important prerequisite in the form of transparency of the national system for the protection of a state's own critical infrastructures. Central in this issue is the availability of freely-accessible information.

Last, but not the least, proper awareness at all levels of industry, state and society is a must while sectoral cooperation and international cooperation are a matter of urgency as critical infrastructure protection should not stop at public frontier or national border only.

2.3 Sources of threats to CII

2.3.1 Inadvertent or negligent incidents

The interconnection that we live by today is not free from risks and threats: deliberate or otherwise, tangible or otherwise. Technical glitches or negligence to the operation and maintenance of the information assets in this aspect could theoretically bring a nation to its knees. The magnitude of the problem due to the interruption of information system in the critical infrastructure is best illustrated in several incidents to follow.

In UK, a glitch caused disruption to the traffic computerised control system that led to dysfunctional lights across central London and caused long queues on main roads ("Computer glitch causes road jams," *BBC News*, 5th April 2009). Meanwhile, a computer breakdown at Taipei's international airport caused chaos and long queues, and forced immigration officials to hand-record departing passengers' data, taking the risk that certain blacklisted individuals or criminal suspects may be let free to flee the country ("Computer glitch causes chaos at Taiwan airport," *Asia-Pacific News*, 6th January 2009).

Singapore experienced technical glitches on its electricity system in 2002 when a computer glitch had resulted in the worst blackout in over a decade in the island country. It ultimately paralysed parts of Singapore for ninety minutes and prompted an emergency valve to close, cutting off the flow of the gas to one of two Singaporean providers of the fuel, the SembCorp Gas. The lack of gas consequently tripped seven power plants. As a result, there was an 8% shortfall in the amount of electricity produced ("Computer glitch behind worst blackout in decade," *The Straits Times*, 15th August 2002.).

Similar incidents have hit Malaysia, too, affecting public facilities and critical sectors such as railway operation, stock exchange, postal system as well as government agencies. In a dramatic incident, a computer system malfunction caused Bursa Malaysia, the national stock exchange, to suspend a whole-day trading ("Bursa grinds to a halt," *The Star*, 4th July 2008). According to the President of the Malaysian Investors Association, such unprecedented interruption to the stock trading was estimated to have caused the Government RM 1 million in stamp duty from contracts done while brokers stood to loose RM 5 million in the non-trading day. Arguably, these monetary losses were not the only thing incurred: stock exchange and Malaysian economy in general may suffer from credibility losses.

2.3.2 Deliberate attack

The origin of the above incidents is more of technical and non-deliberate failures; one of many threats to information security. Others come from deliberate acts that may trigger liability under a criminal law. As one commentator puts it, the annals of cyber crime now contain examples of successful attacks against air traffic control systems, sewerage treatment facilities, and large electronic retailers, as well as the occasional mail bombing of

governmental services and defacement of governmental websites (Grabosky, p.38). These attacks can prove more fatal or catastrophic, and such threats are not esoteric but are real and being exploited on a daily basis, and the consequences of such attacks are significantly harmful.

In March 1997, a teenager hacked into a telephone company computer that serviced the Worcester Airport, Massachusetts. This caused telephone services to the control tower, the airport fire department, airport security and various other departments to be suspended for more than six hours. The attack caused a ripple effect of delayed and cancelled flights across the country, leading to serious financial losses by the airport and several airlines (Taylor, p. 25).

As illustrated above, anger and disappointment can turn into a dangerous source of attack to critical infrastructure. On other incident, it was noted by Taylor (p. 25) that a disgruntled former Chevron employee disabled the firm's alert system by hacking into the company's computers. The attack was not discovered until the system failed to notify engineers of the release of noxious chemicals into the air at a plant in Richmond, California, USA. This incident put millions of people in the western US and Canada at risk.

3. POLICY AND LEGAL FRAMEWORKS IN MALAYSIA

Many countries realise that there is a pressing need to pass legislation that protect the CII. This reinforces the fact that CII is a national concern, and its protection needs to be backed by law and enforcement including penalties and sanctions. The law is the reason for the states to allocate special funds for the provision, operation and enforcement of the protection of CII.

3.1 The national policy framework

Malaysia as a fast-developing country increasingly adopts information technology and computer network in almost all sectors of its development. It is clearly stipulated in the latest national development plan (the 9th Malaysia Plan), which emphasises that a greater adoption and usage of ICT will become strategically more important. The country will need to increasingly harness ICT to improve productivity and competitiveness as well as progress to high value added and knowledge-intensive economic activities. The Government will build upon and enhance ICT capacity for ubiquitous access, develop core competencies, narrow the digital divide and expand usage of electronic transactions as part of the overall effort to empower the populace to partake in the growing networked economy. Simultaneously, this will allow for the greater expansion of ICT-related industries and services (The Ninth Malaysia Plan, p.141).

In order to realise this, it outlines, among others, information security as the focus in this period of development. For that reason, "efforts will be intensified to improve information security in order to enhance confidentiality, integrity and availability of online information systems" (The Ninth Malaysia Plan, p.152). On top of that, the aim is to enhance the integrity of networked systems, increase trust and confidence in online mechanisms and improve quality of services, among others, through compliance with information security management standards and best practices. In particular, these aspects will be of specific importance to the agencies operating the *critical national information infrastructure* (The Ninth Malaysia Plan, p.153).

It is noteworthy that the Plan makes a specific stipulation and places a specific emphasis on the protection of critical national information

infrastructure. Nevertheless, this emphasis has not been backed up by a specific legislation or legal instruments that comprehensively address all the elements of CII. Instead, the Government of Malaysia in 2006 has set up a national policy in the form of National Cyber Security Policy (NCSP), which is closely related to the protection of national critical information infrastructure albeit emphasis given on a more restricted context of cyber security.

In the preceding sections, this paper examines certain Malaysian statutes that are relevant with the protection of CII in the country. This study discovers that certain significant remedies can be found in law relating to the protection of restricted places as well as law on internal security.

3.2 The law that restricts the access to and movements in the perimeters of CII

One way to protect the security of critical information infrastructure is to prevent, restrict or regulate the access to and the movement within the perimeter of those assets. This is one important aspect of information security, i.e. the control of access or in other words the physical aspect of information security. By controlling the access physically or restricting the movement, only those with a clear and legitimate authority would be allowed entry or access. This is crucial to ensure the confidentiality of information infrastructure while at the same time safeguarding the integrity of the assets and their availability for use and services intended.

3.2.1 Protected Areas and Protected Places Act 1959

In Malaysia, the legislation that closely deals with this matter is in the form of the Protected Areas and Protected Places Act ('PAPPA') 1959 (Act 298). This Act, having been revised in 1983, is aimed at providing for protected areas and places.

'Protected area' means any area declared to be a protected area by virtue of section 4 of the Act. According to this section, such declaration will be made by an Order of the Minister "if it appears to him to be necessary or expedient that special measures should be taken to control the movements and conduct of persons therein." 'Protected place', on the other hand, is defined as "any premises declared to be a protected place by virtue of the provisions of section 5." This section further stipulates that if in respect to any premises "it appears to the Minister to be necessary or expedient that special precautions should be taken to prevent the entry therein of unauthorised persons he may by order declare the premises to be a protected place for the purposes of this Act."

As to the effect of any Order passed under this section, it is provided that "no person shall be in those premises unless he is in possession of a pass-card or permit issued by such authority or person as may be specified in the order, or has received the permission of an authorised officer on duty at those premises to enter the same." The contravention of or failure to comply with any of the provisions in section 4 or 5 is an offence that may trigger an imprisonment for a term of two years or a fine of one thousand Ringgit or both (section 7).

3.2.2 Ground for restriction

As mentioned above, both sections 4 and 5 of the PAPPA 1959 stipulate that the ground for taking actions made under such sections is if it appears to be *necessary* and *expedient*. There is however no express term in the Act that explains situations or grounds on which it is 'necessary' or 'expedient'. It is argued that such requirements should be put in the correct legal perspective. According to the rules of interpretation of the statutory provisions

(Interpretation Acts 1948 and 1967, section 17A), a construction that would promote the purpose or object underlying the Act must be preferred to a construction that would not promote that purpose or object. This PAPPA 1959, it is observed, aims at protecting some places or premises due to their importance for public in general. The fact that the Act grants significant powers to police and armed forces suggests that this relates to a public order and national security. This is also supported by a high level of security measures provided in s. 10 that can be taken in order to prevent an entry or any attempt to enter the protected areas and places.

There are so far no reported cases involving the interpretation or explanation of the provisions of the 1959 Act. There are, however, some incidents of violation under the PAPPA 1959 reported though they are not very helpful in explaining the law. In one unreported case in Klang (a district) Magistrate Court on 11th July 2005, five people were charged for trespassing into Dock 3 of the West Port Klang, Selangor, a site declared as protected area under the PAPPA 1959. At that time, the said dock was used by the US aircraft carriers USS Nimitz to harbour for an official visit in Malaysia ("*5 dituduh ceroboh kawasan USS Nimitz* [5 were accused of trespassing USS Nimitz]," *Utusan Malaysia*, 12th July 2005). It was further reported that two of them, who were there to take pictures of the carrier out of hobby, pleaded guilty as charged. At the hearing, the prosecutor had urged that the court should consider public interest and national security. Azmil Muntapha Abas J. convicted the two and punished them with the maximum fine of RM 1,000 each ("*2 lelaki didenda RM 1,000 ceroboh rakam gambar Nimitz* [2 men fined RM 1,000 for trespassing on Nimitz]," *Utusan Malaysia*, 19th November 2005).

Malaysia can borrow some guidance from a Singaporean court that has in 1999 dealt with the matter based on their Protected Areas and Protected Places Act 1963 (which is in *pari materia* with the Malaysian provision) in the case of *Lim Ah Heng & Anor* (Singapore High Court, 1999). In this case, which substantially dealt with the issue of illegal dumping, a question arose as to whether or not the site in issue, an Air Force military training area declared as a protected place under the Singaporean Act, constitutes a 'public place' for the purpose of illegal dumping offence. This restriction against a military training site indicates that this law deals with matters of national security and public safety.

3.2.3 Restriction beyond physical movements

Meanwhile, another aspect of this Act worthy of discussion is the effect of restriction to be made under the Ministerial Order. This law does not merely regulate physical restriction per se—contrary to the first impression people get from reading this law. Instead, the restriction also covers restriction on movements and conduct of persons in a protected place.

Neither 'movement' nor 'conduct' is being defined in this Act. Therefore the meaning of conduct in this case would be general and lexical, and again, regard has to be given to the purpose of the Act itself, namely to provide for the control and restriction within the protected areas and protected places. While movement would be generally physical, conduct is not necessarily so as it could refer to a non-physical or non-tangible conducts. This would arguably include those electronic activities that are potentially detrimental to the confidentiality, integrity and availability of the information system and assets (information infrastructure) within such designated area or place. The example of this would be the unauthorised or malicious use of wireless or hand-held devices that

may interrupt with the information and communications system in the designated area or place.

This proposition can borrow some support from the Government security-related circular issued by the National Chief Secretary to the Government of Malaysia on 31st of January 2007 (No. KPKK(R)200/55 Klt. 8(2), dated 31st January 2007), restricting the use of handheld devices and any other information and communications gadgets. The circular, issued to all government agencies including the ministries, federal and state offices, statutory bodies and local governments, stipulates that key administrative areas and places where official secrets and security-implicated matters are discussed, have to be designated as ICT-restricted zones to enhance the protection of vital information. Therefore, it instructs the restriction of unauthorised gadgets from being brought into high-security government premises. The ban, it says, will prevent spying and the leaking of sensitive information or official secrets, which could jeopardize national security. It also noted that the widespread use of these devices, specifically camera phones, have serious implications on homeland security as they can be abused to gather or even transmit information in any form, including unauthorized data or digital images.

The direct consequence of this legislation is the control of access and movement into or within the designated protected areas and places. Given the nature of the Order and the power it grants to authorised officer, it is argued that this law constitutes a crucial instrument in safeguarding the nation's critical information infrastructure. This is however only true if the areas and premises that host the critical infrastructure are first declared by the Minister as 'protected areas' or 'protected places.'

3.2.4 Appraisal

There have been a number of Orders being declared by the Malaysian Government in pursuant to section 4 and 5 of the PAPPA 1959. It is found that the designation of protected areas and places under the Act focuses on certain grounds such as national defence and security, law enforcement, public safety and food, and general utilities and public infrastructure as well as smooth government functions and services. By virtue of these Orders, the authority to restrict the movement, entry or conduct in the designated protected places has been rested on the Chief Government Security Officer (CGSO) of Malaysia under the command of the Prime Minister's Office.

It is observed that all the Orders made under the 1959 Act fall into any one of the critical sectors identified by the Government under their critical information infrastructure policy. Sectors such as national defence and security, law enforcement, utilities (water, gas, energy, electricity, etc.), food and agriculture, transport, information and communications and essential government functions/services, as well as banking and finance, are reflective of the ten critical sectors laid down in the national Cyber Security Policy (NCSP).

Given the above discussion, this study believes that the Act plays a crucial role for the protection of the nation's critical information infrastructure, and therefore is also an important part of information security legal framework in Malaysia. Nevertheless, there is still room for improvement to make this legislation more effective and efficient for the critical information infrastructure protection.

3.3 The law on computer network security

The recognition of the concept of critical information infrastructures necessitates the provision

of critical computers, i.e. those computer systems which are used to operate, monitor, enforce or otherwise safeguard the CII. It is noted that in some jurisdictions, cybercrime offences treat critical computers differently so as to accord greater protection. The idea behind this is that the law should be sufficiently stringent to prevent harm to critical computers.

This area of law is better known as the domain of cybercrime or computer crime. Cybercrime is generally described 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 (Ferrera, at. al., p.300). Computers may facilitate the commission of 'old-fashioned' crimes such as fraud or counterfeiting or give rise to new mischief such as computer hacking and the deliberate erasure of programs or data. Cybercrime today has grown from petty offence to massively devastating crime (Bainbridge, p. 285). Even way back in 1996, upon the discovery of hackers who broke into the US Defence Department's computer more than 160,000 times, the United States' General Account Office reported that 'at minimum, these attacks are a multimillion-dollar nuisance to the defence. At worse, Gringras (p. 211) notes, they are a serious threat to national security.'

Cyber crime law can play a significant role in the protection of critical information infrastructure by defining the offences and their penalties or punishments. The idea lying behind this is that if the potential culprit knows that disrupting information systems attached to critical information infrastructure triggers harsh punishment, the offence can be prevented or reduced.

3.3.1 International and comparative perspectives

At international level cybercrime law is addressed by the Council of Europe's Convention of Cybercrime 2001, which 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; and (4) Offences involving the infringement of intellectual property and related rights. Pertaining to the protection of the CII, the first category of cybercrime offences above is arguably of particular relevance. In the first category of substantive offence, the Convention in articles 2-6 specifically provides for certain types of criminal offences such as illegal access, illegal interception, data interference, system interference, and misuse of devices. Beyond that, certain computer laws in different jurisdictions have gone further by providing specific provisions for 'critical computers' which is more responsive to the need to protect CII.

In US, this type of critical information infrastructure is defined as 'protected computer' under the Computer Fraud and Abuse Act 1996. It refers to the information system that is used exclusively by the government or a financial institution in which the defendant's conduct affects the government or financial institutions' operation of the computer or to the computer system involved in the interstate or foreign commerce and communication.

In Singapore, there is a specific provision for enhanced punishment for offences involving protected computers. Its Computer Misuse Act 1998 provides in s. 9 that "where access to any protected computer is obtained in the commission of an offence under section 3, 4, 5 or 7, the person convicted of such an offence shall, in lieu of the

punishment prescribed in those sections, be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding twenty years or to both."

For this purpose, s. 9(2) defines the term 'protected computer' as the computer or program or data that is used directly in connection with or necessary for, among others, the security, defence or international relations of Singapore; the provision or services directly related to communications infrastructure, banking, and financial services, public utilities, public transportation or public key infrastructure; or the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

3.3.2 Communications and Multimedia Act 1998

In Malaysia, the main statute that stipulates computer crimes have been passed including the the Communications and Multimedia Act (CMA) 1998 and the Computer Crimes Act (CCA) 1997.

CMA 1998 is central to the idea of information security protection. This law seeks to uphold the national policy objectives, namely among others, to ensure information security and network reliability and integrity (section 3). To manifest this objective, the CMA sets out certain criminal offences that seek to prevent or punish those acts that pose threats to the information security. Those penal sanctions can arguably be classified into four aspects of information security, namely:

- Network-related security, reflected in the offence of fraudulent use of network facilities, etc. in section 232 of the CMA 1998;
- Content-related security, as in the offence on improper use and offensive content in section 233 CMA;
- Communications security, i.e. on unlawful interception and disclosure of communications as found in section 234 CMA; and
- Physical security, in the form of offence on the damage to network facilities and misuse of access device and tools as provided in sections 235-236 CMA respectively.

3.3.3 Computer Crimes Act 1997

Beside the CMA 1998, the Computer Crimes Act (CCA) 1997 provides for another significant measure for protecting critical information infrastructure by penalising specifically computer-related offences, as follows:

- Unauthorised access to computer material (section 3 CCA 1997);
- Unauthorised access with intent to commit or facilitate commission of further offence (s. 4);
- Unauthorised modification of the contents of any computer (s. 5);
- Wrongful communication of means of access (s. 6); and
- Abetments and attempts of any offences above (s. 7).

3.3.4 Appraisal

Be good laws as they may, nevertheless those two legislations do not make a distinction on the offences based on the types of computers that are affected; thus it does not differentiate between a harmless hacker who defaces a web-page for fun and a cyber-terrorist who desires to cause injury through the unauthorised modification of a critical computer's content. On this point, a Malaysian cyberlaw expert Professor Abu Bakar Munir in his interview with the author (in Kuala Lumpur, 2 June

2009) supports this proposition and argues that it is very important to differentiate 'normal computer system' with 'protected computers' such as those used in medical services, governments and so on.

For this matter, Malaysian computer crime law needs to be re-looked. As the country's critical information infrastructure such as banking and financial institutions, public transport, power and utilities, and defence, becomes more dependent on computerised system, it is argued that the punishment provided under the Act does not commensurate with the harm that may be caused by malicious intrusion. To address this issue, the Act should be expanded in order to prevent bigger threat to information security especially those involving the nation's critical information infrastructure. Some comparative analysis on what other countries have would be useful for coming up with an improvement.

It is argued that this approach (of providing specific penal offences against harming the critical computers) is highly recommended in improving the Malaysian legal framework on the protection of CII. If the CCA is enhanced to include more stringent punishment for any attack on the CII, this will be a strong message for future offenders.

4. FINAL REMARKS

The premise of this paper (of threats and attacks to critical information infrastructure) is that as nations and critical infrastructure became more dependent on computer networks for their operation, new risks are created. Such risks take the form of threats to national security and public safety. For now, the potential deadly threats to the security of critical information infrastructure may still look unlikely. This situation however should not be a reason to be sceptical, lenient or complacent. It is observed that this current position is not a static situation as the vulnerability of critical information infrastructure to cyber attacks could change with the increasing use of the network technology (Lewis, p.11).

Malaysia should not be complacent especially for two main reasons. First, the security of its critical infrastructure is a vital determinant for national security, thus it should not be taken lightly, leaving the security to a chance—or worse to the hands of malicious criminals. Efforts to strengthen the security and resilience of the nation's critical infrastructure should be made a priority.

Secondly, the advances of technologies and the rise of digital citizens in Malaysia form a part of a global network that seek to globalise everything from business to governance, from friendship to professionalism, and—unfortunately—from crime to terrorism. These would soon present a huge challenge to all those who are dependant on the technology and the information assets.

The policy and legal measures that are discussed in this paper arguably constitute as part of a bigger framework to secure Malaysian critical infrastructure. The law is only one element as other components—technology, standards, public-private cooperation and the institutions—are worth considering, and require further research as well as strategic development. By way of analogy, while it is correct to regard information as 'oxygen' for the people and democracy, this paper firmly believes that the critical information infrastructures or CII is the 'respiratory system' in which such oxygen is utilised, processed and acted upon.

REFERENCES

Bainbridge, D. I. (2000). *Introduction to computer*

law (4th edn.). London: Pearson Education.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (or—Federal Office for Information Security, Germany), URL: http://www.bsi.bund.de/english/index.htm (Last date accessed: 1 June 2009).

Bundesamt fur Sicherheit in der Informationstechnik (BSI), 2004. Critical infrastructure protection: Survey of world-wide activities, *BSI Kritis*, 4/2004.

Centre for the Protection of National Infrastructure (CPNI), UK, URL: http://www.cpni.gov.uk/glossary.aspx (Last date accessed: 1 June 2009)

CNII Portal Malaysia, URL: http://cnii.cybersecurity.org.my/en/about.html (Last date accessed: 2 May 2009).

Condron, S.M. 2007. Getting it right: Protecting American critical infrastructure in cyberspace, *Harvard Journal of Law and Technology*, 20 Harv. J. Law & Tec 404.

Ferrera, et. al., 2001. *Cyberlaw: Text and cases,*, Ohio: Thomson Learning.

Grabosky, P., 2007. *Electronic crime,* New Jersey: Pearson Prentice Hall.

Gringras, C., 1997. *The laws of the Internet,* London: Butterworths.

Information Security Policy Council, "Action Plan for Information Security Measures for Critical Infrastructures," National Information Security Center, URL: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf (Last date accessed: 2 May 2009).

Lewis, J.A., 2002. *Assessing the risks of cyber terrorism, cyber war and other cyber threats,* Washington, D.C.: CSIS.

OECD, Protection of 'Critical Infrastructure' and the role of investment policies relating to national security, Report, May 2008, URL: http://www.oecd.org/dataoecd/2/41/40700392.pdf (Last date accessed: 2 May 2009).

Taylor, R.W., 2006. *Digital crime and digital terrorism*, New Jersey: Pearson Prentice Hall.

The Attorney General's Department, Australia, URL: http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection (Last date accessed: 1 June 2009).