Washington International Law Journal

Volume 7 | Number 2

3-1-1998

Malaysia's "Computer Crimes Act 1997" Gets Tough on Cybercrime But Fails to Advance the Development of Cyberlaws

Donna L. Beatty

MALAYSIA'S "COMPUTER CRIMES ACT 1997" GETS TOUGH ON CYBERCRIME BUT FAILS TO ADVANCE THE DEVELOPMENT OF CYBERLAWS

Donna L. Beatty

Abstract: Malaysia is in the process of developing the Multimedia Super Corridor ("MSC"), a high-tech zone sometimes called "the Silicon Valley of the East." As a way of attracting investors to the MSC, Malaysia is adopting business-friendly policies and comprehensive "cyberlaws" designed to assure MSC participants that they and their technology will be protected. One of Malaysia's many goals is to be a leader in the development of cyberlaws. However, the Computer Crimes Act 1997 is too flawed to place Malaysia in that role. The Computer Crimes Act is designed to prevent computer crimes such as hacking, virus planting and the cracking of passwords. Although the Act contains some progressive provisions that appear in recommendations adopted by organizations such as the Organization for Economic Cooperation and Development, some provisions lack clarity and can be interpreted in ways which make them overly broad and unenforceable. Other provisions seem to ignore the needs of corporate victims of computer crimes, thus failing to meet the goal of assuring potential MSC investors that their technology will be protected. By modifying some of the statutory language to clarify the meaning and by adopting provisions which offer more progressive solutions to the problem of computer crime, the Computer Crimes Act 1997 could contribute to Malaysia's standing as a leader in the development of cyberlaws.

I. INTRODUCTION

Malaysia is in the midst of a remarkable transformation due to Vision 2020, a plan championed by Prime Minister Datuk Seri Dr Mahathir bin Mohamad.[1] The objective of Vision 2020 is Malaysia's emergence as an economically-developed, industrialized nation by the year 2020[2] with an economy rivaling those of Asian leaders such as Hong Kong, Japan and Singapore.[3] The centerpiece of this ambitious undertaking is the Multimedia Super Corridor ("MSC"), a 750 square kilometer high-tech zone extending from Kuala Lumpur's new city center to the new Kuala Lumpur International Airport.[4] The key to the success of

---

[1] *See, e.g.*, Helen Johnstone, *Entering the Twilight Zone*, ASIAN BUS., Feb. 1997, at 48, *available in* LEXIS, Asiapc Library, Allasi File.

[2] Lori Valigra, *Multimedia Peninsula*, GLOBAL TELEPHONY, June 1997, *available in* LEXIS, News Library, Iactl File.

[3] Johnstone, *supra* note 1.

[4] Valigra, *supra* note 2.

the MSC and Vision 2020 is the participation of knowledge industries,[5] many of which Malaysia hopes will establish research and development facilities in the MSC.[6] Malaysia is relying on both a high-tech "hard infrastructure" and an advanced, business and investor-friendly "soft infrastructure"[7] to attract the corporations that will make the MSC a success.[8] The hard infrastructure of the MSC includes high-tech, high-speed telecommunications media which will link all businesses, government offices, and homes in the area to each other and to an international gateway with direct links to many nations of the world.[9] The soft infrastructure of the MSC includes business- and investor-friendly laws and policies that ease employment restrictions for foreign knowledge workers,[10] as well as forward-thinking "cyberlaws"[11] designed to reassure potential investors that the government takes the protection of technology and the problem of high-tech "cybercrimes" seriously.[12]

This Comment identifies and analyzes the problem areas and unmet opportunities in the Computer Crimes Act 1997, one of the four cyberlaws recently adopted by the Malaysian parliament.[13] Part II of this Comment establishes the importance of curtailing computer crimes by briefly examining their global proliferation and financial impact. Part III discusses the history of the Computer Crimes Act 1997 and evaluates the contributions its provisions make toward furthering Malaysia's goals of deterring cybercrime, reassuring potential MSC investors, and positioning

---

[5] "Knowledge industries" are those industries which require leading-edge technology and a high level of human input and creativity. Johnstone, *supra* note 1.

[6] *Id.*

[7] *New Cyberlaws Show Malaysian Commitment to MSC*, ASIA PULSE, July 10, 1997, *available in* LEXIS, Asiapc Library, Apulse File.

[8] *DAP Wants Public Discussions on Proposed Cyberlaws*, NEW STRAITS TIMES (Malaysia), Mar. 4, 1997, at 8, *available in* LEXIS, Asiapc Library, Nstrtt File.

[9] The telecommunications equipment which will serve the MSC includes a fiber optic backbone with asynchronous transfer mode switching and integrated services digital network offerings. Valigra, *supra* note 2.

[10] *Id.*

[11] "Cyberlaws are laws and policies designed to promote commerce and new applications in the era of digital information and multmedia." *Cyberlaw Int'l Enforcement Needs Common Approach*, ASIA PULSE, Aug. 6, 1997, *available in* LEXIS, Asiapc Library, Apulse File.

[12] *Malaysian Government—Speech by the PM of Malaysia, The Honourable Dato Seri Dr Mahathir Bin Mohamad*, M2 Presswire, May 27, 1997. *available in* LEXIS, World Library, M2pw File.

[13] The four cyberlaws passed thus far by the Malaysian government are the Digital Signature Act, Computer Crime Act, Telemedicine Act and Copyright (Amendment) Act. The Mulitmedia Convergence Bill and the Electronic Government Bill are expected to be tabled in the upcoming Parliament sitting. Cheah Chor Sooi, *Special Legislations Needed for MSC*, NEW STRAITS TIMES (Malaysia), Sept. 30, 1997, at 38, *available in* LEXIS, Asiapc Library, Nstrtt File.

Malaysia as a leader in the development of cyberlaws.[14] This analysis is supported by comparing the provisions of the Computer Crimes Act 1997 with recommendations made by international organizations and similar laws passed in other countries. Part IV recommends several modifications to Malaysia's approach to meeting the goals of the Computer Crimes Act 1997. In addition to recommending that Malaysia impose an affirmative duty on businesses locating within the MSC to implement a minimum level of system security, this section proposes statutory language refinements and the adoption of additional provisions. Finally, Part V concludes that by clarifying some of the language of the Computer Crimes Act 1997 and incorporating more modern approaches to addressing the computer crime problem, Malaysia will be well on its way to establishing itself as a leader in the development of cyberlaws.

II. AN OVERVIEW OF THE GLOBAL COMPUTER CRIME PROBLEM

It has been said that no country has yet formulated a set of laws that effectively deals with high-tech criminals.[15] However, it is important that even less than completely effective computer crime laws are passed because authorities are often unable to secure the convictions of cybercriminals under traditional laws.[16] Today's computer crimes are perpetrated not only by mischievous hackers,[17] but high-tech gangs that deal in "fraud, theft, character assassination, breaches of government security, [and] terrorism . . ."[18] Estimates of annual world-wide losses from computer crimes are as high as $22 billion.[19] As noted in the *United Nations Manual on the Prevention and Control of Computer Related Crime*, the global proliferation of computer

---

[14] *See infra* text accompanying notes 56-59.

[15] Cheah Chor Sooi, *supra* note 13 (quoting Dennis Unkovic, a partner in the Pittsburgh-based firm Meyer, Unkovic and Scott, and an expert in corporate and international legal matters).

[16] *See, e.g.*, Robert Sciglimpaglia Jr., *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199, 202 (1991) (discussing the fact that Australian Federal Police were unable to begin an investigation into known hacking activities until legislation covering computer crimes became effective in 1989).

[17] Ferina Manecksha & Nazzatul Shahreen. *Outlook: Ensuring Effectiveness of Proposed Cyberlaws*, COMPUTIMES, Oct. 13, 1997, at 30, *available in* LEXIS, Asiapc Library, Nstrtt File.

[18] *Crime and the P.C.*, INDIANAPOLIS STAR, May 14, 1997, at A08.

[19] Law enforcement agencies' estimates of world wide losses from various computer crimes range from $5 billion to $22 billion, with a reported total of $2.5 billion in 1996. *Computer Crime Rising Against Financial Institutions*, FIN. SERVICE ONLINE, May 1997, *available in* LEXIS, News Library, Fgray File.

crime has prompted governments and international organizations to call for the adoption of laws which specifically address this threat.[20]

Defining the term "computer crime" is a challenge in itself. A computer can be the subject of a crime, the site of a crime, or the instrument of a crime.[21] As the scope of the term "computer crimes" is quite broad, this Comment will emphasize only the primary activities criminalized in Malaysia's Computer Crimes Act 1997: unauthorized computer access and virus implantation.

A. Unauthorized Access of a Computer

Unauthorized access, popularly known as "computer hacking" or "cracking,"[22] is now occurring at an alarming rate. It is estimated that one computer on the Internet is broken into every twenty seconds,[23] although only three to fifteen percent of these intrusions are detected.[24] In 1995 the United States Department of Defense's computers were targeted for illegal access an estimated 250,000 times, with a success rate of approximately sixty-five percent.[25] One estimate put the cost to businesses of unauthorized access at $3 billion.[26] Even more alarming is the fact that the number of these incidents is doubling every year.[27]

Hacking is often just the beginning step in the criminal activity. Sabotage and revenge, as well as theft of information, financial identities, money and phone services are among the pursuits of criminal hackers.[28] A

---

[20] *See generally* UNITED NATIONS CENTRE FOR SOC. DEV. AND HUMANITARIAN AFF., INT'L REV. OF CRIM. POL'Y, ¶¶ 4, 116-26, U.N. Doc. ST/ESA/SER.M/43-44, U.N. Sales No. E.94.IV.5 (1994) [hereinafter UN MANUAL].

[21] Marc S. Friedman & Kenneth R. Buys, *"Infojacking": Crimes on the Information Superhighway*, COMPUTER LAWYER, Oct. 1996, at 1.

[22] *Leading Edge: The Importance of Being a Hacker*, FT Asia Intelligence Wire, Sept. 1, 1997, *available in* LEXIS, Asiapc Library, Aiw File.

[23] Marianne Curphey, *Computer Crimes Costs Business Pounds 200m Each Year*, TIMES (London), Apr. 1, 1997, *available in* LEXIS, Allwld Library, Ttimes File.

[24] These estimates were made by the United States Federal Bureau of Investigation. Jackie Cox, *Stealing Information is the Name of the Game; Information Systems Security*, AM. PAPERMAKER, Jan. 1996, at 44, *available in* LEXIS, News Library, Ampapr File.

[25] *Networks: Internet Hackers on the Rise*, LAN MAG., Jan. 1, 1997, *available in* LEXIS, Asiapc Library, Aiw File.

[26] Beverly Head, *Australia: Hackers From Hell*, AUSTRALIAN FIN. REV., Feb. 13, 1995, *available in* LEXIS, News Library, Txtnws File.

[27] *Networks: Internet Hackers on the Rise*, *supra* note 25.

[28] *See, e.g.*, Marcy Gordon, *Thieves Commit Financial Fraud With a Mouse Click*, CHATANOOGA TIMES, Sept. 17, 1997, at D10; *infra* notes 29-32. One notorious cybercriminal, Vladimir Levin, managed to steal $10 million from Citibank before he was apprehended. Levin frequently accessed Citibank's

profitable computer crime is "phreaking"—the term hackers have given to accessing phone systems in order to get long distance services at someone else's expense.[29] One leading British company saw its phone bill increase by $305,250 over a period of four months due to this criminal activity.[30] Theft of information by organized crime is an increasing problem.[31] One way organized crime profits from the theft of information is by using information about corporate mergers and acquisition plans to make profitable stock trades.[32]

Although unauthorized access by hackers creates numerous problems, losses are far more commonly attributable to disgruntled employees, ex-employees, or contract workers who retaliate for real or imagined wrongs by destroying data or committing fraud.[33] One estimate pegs the percentage of computer crime losses caused by insiders at eighty-two percent.[34]

B. *Computer Viruses*

Computer viruses are programs whose execution by an unknowing user can result in effects ranging from annoying computer behavior to the destruction of all resident data.[35] As of July 1997, there were 8,000 known viruses, 200 of which were classified as "frequently encountered."[36] Approximately four or five new viruses appear daily, though many are non-destructive and many are variants of existing viruses.[37]

---

system in New York from his personal computer in St. Petersberg, Russia, in order to transfer funds from various accounts into accounts he had established in banks world-wide. Philip Jacobson, *Crime in the Cyber Age*, SUNDAY TELEGRAPH (London), Oct. 19, 1997, at 28, *available in* LEXIS, World Library, Telegr File.

[29] Amruta Slee, *Australia: Highway Robbery—Computer Hacking*, THE AGE (Melbourne), Mar. 4, 1995, *available in* LEXIS, News Library, Txtprm File.

[30] Robert Uhlig, *It's Costing Nothing to Talk: Phone Hackers are Breaking Into Company Switchboards With Increasing Regularity*, DAILY TELEGRAPH (London), Oct. 15, 1996, at 3, *available in* LEXIS, World Library, Telegr File. This amount is in 1998 U.S. dollars, converted from 1996 British pounds. Kurt Swanson, *Foreign Exchange Rates: British Pound-United States Dollar* (visited May 11, 1998) <http://www.dna.lth.se/cgi-bin/kurt/rates?GBP+USD>.

[31] *Computer Crime Rising Against Financial Institutions*, *supra* note 19.

[32] *Id.*

[33] *Id.*

[34] *Id.* (quoting William Marlow, a senior vice president of Science Applications International).

[35] *What is a Computer Virus?*, THE HINDU, July 24, 1997, at 22, *available in* LEXIS, Asiapc Library, Hindu file.

[36] *Id.*

[37] Adarsh Madhavan, *Keep Your Mouse o[f][the Trojan Horse; Internet Users in Oman Warned Against E-mail Virus*, MONEYCLIPS, May 17, 1997, *available in* LEXIS, World Library, Txtlne File.

Computer viruses can be transmitted from one system to another through "infected" diskettes, infected software downloaded from the Internet, and infected files attached to email messages.[38] Even computer users who do not share diskettes, download software, or receive email are not safe. For example, an entire batch of low-priced Compaq personal computers manufactured and sold in Japan was infected with a virus while still in production.[39]

The global nature of this problem was demonstrated by various surveys taken of businesses world-wide. A recent survey of Australian companies found that nearly all have experienced virus problems at one time.[40] The National Computer Security Association ("NCSA"), a United States-based organization, released a survey revealing that ninety-eight percent of 300 multinational companies questioned had been affected by computer viruses.[41] In April 1996, the NCSA projected that North American businesses would lose between $5 billion and $6 billion in 1996 due to disinfection and downtime costs resulting from computer virus contamination.[42]

III. ANALYSIS OF THE COMPUTER CRIMES ACT 1997

A. A Brief History of the Act

Malaysia's Computer Crimes Act 1997 was drafted by a committee from Malaysia's Attorney General's Chambers[43] at the direction of the Ministry of Energy and Telecommunications[44] and was modeled after the

---

[38] Maria O'Daniel, *Viruses,Worms and Trojan Horses*, NEW STRAITS TIMES (Malaysia), Aug. 7, 1997, at 50, *available in* LEXIS, Asiapc Library, Nstrtt File; *Industry Research Indicates That Even the Most Savvy Computer Users are not Properly Protected Against Computer Virus Threats*, Canada NewsWire, June 19, 1997, *available in* LEXIS, World Library, Cnw File.

[39] *Compaq's Low-priced PCs Found Infected with Virus*, JAPAN COMPUTER INDUSTRY SCAN, Oct. 6, 1997, *available in* LEXIS, News Library, Iacce File.

[40] *Viruses Still Big Blight*, CANBERRA TIMES, Aug. 4, 1997, at A13, *available in* LEXIS, Asiapc Library, Canber File.

[41] *McAfee Responds with VirusScan Version 2.2C*, M2 Presswire, Apr. 23, 1996, *available in* LEXIS, World Library, M2pw File.

[42] *Id.*

[43] The role and responsibilities of the Attorney General are stated in Article 145 of the Federal Constitution. The Attorney General is the Public Prosecutor and acts as the legal advisor to the Government. Additionally, the Drafting Division is responsible for drafting all Federal laws that are to be tabled in Parliament. Razia Begum Mukhtar Ahmad, *Jabatan Peguam Negara Homepage* (visited May 8, 1998) <http://spl.pnm.my/~peguam>.

[44] Email from the law firm of Raja Darryl & Loh, Microsoft's counsel in Malaysia, to Donna L. Beatty, Writer, *Pacific Rim & Policy Journal*, (Dec. 9, 1997) (on file with the author).

United Kingdom's Computer Misuse Act.[45] Prior to being introduced in the Dewan Rakyat, Malaysia's House of Representatives,[46] in late March 1997, the bill was shrouded in secrecy.[47] The opposition party protested this secrecy[48] and called for public discussions prior to its introduction in the Dewan Rakyat before the parliamentary debates.[49] After its introduction, opposition party members voiced concern over some penalties they believed were unreasonable.[50] Despite these controversies, the Act was adopted in June 1997.[51]

The Computer Crimes Act 1997 is divided into three parts.[52] Part I contains preliminary matters such as its short title and relevant definitions.[53]

---

[45] Email from Dr Khaw Lake Tee, Associate Professor and Deputy Dean of Universiti Malaya's Law Faculty, to Donna L. Beatty, Writer, *Pacific Rim Law & Policy Journal* (Nov. 10, 1997) (on file with author).

[46] The Parliament is bicameral, being divided into the Dewan Negra (Senate) and the Dewan Rakyat (House of Representatives). Bills almost always originate (are introduced) in the Dewan Rakyat. *Malaysia 1994 File* (visited Oct. 22, 1997) <http://asnic.utexas.edu/asnic/countries/malaysia/Malayconstitution.html>. A Minister will present the Bill by tabling it, which is called the First Reading. The following day, the Minister may conduct the Second Reading which he does by presenting the policy of the Bill. Once another member expresses support for the Bill, the policy is debated. If the Bill is accepted by the Dewan Rakyat at this level, it will continue to the Third Reading during which the particulars of the Bill are debated and amended as necessary. Once the Bill is agreed upon, it goes to the Dewan Negra. The Dewan Negra has no power to revoke the Bill, but if the Bill is not monetary it nature, the Dewan Negra may delay its enforcement for one year. *See The Functions of Parliament File* (visited Oct. 22, 1997) <http://www.parliament.gov.my/bifung.si.htm>.

[47] *See* Rozana Sani, *Cyberlaws Amendment to Help Local IT Growth*, NEW STRAITS TIMES (Malaysia), Apr. 3, 1997, at 4, *available in* LEXIS, Asiapc Library, Nstrtt File. For an example of secrecy information see, *Malaysia: Cyber Laws Passed to Support High-Tech Dreams*, InterPress Service, Apr. 2, 1997, *available in* LEXIS, World Library, Iapress File; Carolyn Hong, *No real Mystery Over Cyberlaws*, NEW STRAITS TIMES (Malaysia), Mar. 9, 1997, at 13, *available in* LEXIS, Asiapc Library, Nstrtt File; *DAP Wants Public Discussions on Proposed Cyberlaws*, *supra* note 8; *Get Feedback on Cyber Bills, Urges Kit Siang*, NEW STRAITS TIMES (Malaysia), Jan. 17, 1997, at 4, *available in* LEXIS, Asiapc Library, Nstrtt File.

[48] The bill was presented to the Prime Minister's Cabinet before the end of Jan. 1997, however as late as mid-March, only a "trickle" of information had been made public. Hong, *supra* note 47.

[49] *DAP Wants Public Discussions on Proposed Cyberlaws*, *supra* note 8; *Get Feedback on Cyber Bills, Urges Kit Siang*, *supra* note 47.

[50] *Kit Siang: Reduce Proposed Punishments For Hackers*, NEW STRAITS TIMES (Malaysia), Apr. 26, 1997, at 5, *available in* LEXIS, Asiapc Library, Nstrtt File.

[51] Cheah Chor Sooi, *supra* note 13.

[52] Computer Crimes Act 1997. *See Computer Crimes Bill 1997* (visited May 12, 1998) <http://zek.upm.edu.my/comcrime.html>.

[53] *Id.* As an attempt to define the term "computer" at the Committee stage of the Bill was unsuccessful, the judiciary is must give the term its "ordinary meaning." *See* Martin Wasik, *The Computer Misuse Act 1990*, 1990 CRIM.L.R. 767, 768 n.7 (Nov. 1990). The similarities between the Malaysian and United Kingdom Acts are particularly apparent in Part I of The Computer Crimes Act 1997 with one key exception: the Computer Crimes Act, unlike its United Kingdom counterpart, defines the terms computer, data and program. The Computer Crimes Act 1997 §2. *Compare with* The Computer Misuse Act 1990 § 17, *available in* LEXIS, Intlaw Library, Englaw File [hereinafter Computer Misuse Act].

Part II of the Act enumerates the offenses relating to misuse of computers and specifies penalties for each offense.[54] Part III deals with ancillary provisions such as jurisdictional and investigational issues.[55]

B. *The Goals of the Act*

The criminalization of activities such as hacking and the spreading of computer viruses is intended to serve several related purposes. One obvious purpose is to prevent and punish computer crime.[56] However, the Act, in combination with the other cyberlaws recently proposed and/or adopted by the Malaysian Parliament, is also designed to establish Malaysia as a leader in the devlopment of cyberlaws.[57] Additionally, the Act was designed and adopted to ensure the success of the Multimedia Super Corridor by sending a clear message to MSC investors that their interests and technology will be protected.[58]

A logical premise for evaluating the merits of Malaysia's Computer Crimes Act is an examination of the Act's contribution toward the realization of these three particular goals. First, the Act's potential efficacy in the deterrence of computer crime can be evaluated by comparing its provisions to similar provisions adopted by other nations and which have already been tested in courts of law. Additionally, the Act's provisions can be evaluated in light of current theories on the causes of computer crime and how best to

---

[54] The Computer Crimes Act 1997 §§ 3-8.

[55] *Id.* §§ 9-12.

[56] *Malaysian Government—Speech by the PM of Malaysia, The Honourable Dato Seri Dr Mahathir Bin Mohamad, supra* note 12.

[57] *Malaysia Mahathir "We Want To Be a Leader in Cyberlaw Development,"* FT Asia Intelligence Wire, June 1, 1997, *available in* LEXIS, News Library, Aiwsel File. The Prime Minister's precise meaning of "leader in cyberlaw development" is difficult to discern, however he did propose that other ASEAN countries adopt the cyberlaws that Malaysia has enacted. *Malaysia Proposes Common Laws For ASEAN Covering Media Technology,* Agence Fr. Presse, May 18, 1997, *available in* LEXIS, News Library, Afp File.

[58] The New Straits Times stated "[t]he cyberlaws formulated by the Government are to attract and encourage corporations to use the Multimedia Super Corridor and turn Malaysia into the region's information technology hub." *DAP Wants Public Discussions on Proposed Cyberlaws, supra* note 8. According to Dennis Unkovic, "Certainty is what every local and foreign compan[y] wants. For the MSC to be successful, the fear that companies have regarding the protection of technology must be removed." Ferina Manecksha, *Business News: Involving All Sectors in Cyberlaw Creation*, NEW STRAITS TIMES (Malaysia), Sept. 22, 1997, *available in* LEXIS, Asiapc Library, Nstrtt File. According to Ken Wasch, Software Publishers Association President, Malaysia's cyberlaws are "just the kind of legislation needed to lure operations of foreign IT companies into the country." Sharifah Kasim, *Attracting Software Vendors to Invest in Malaysia*, NEW STRAITS TIMES (Malaysia). May 1, 1997, *available in* LEXIS, Asiapc Library, Nstrtt File.

address it. Second, to determine if the Act furthers Malaysia's goal of being a leader in the development of cyberlaws, its provisions should be examined for internal consistency, clarity, and portability to other nations. Also, by comparing its provisions to the recommendations of various international organizations charged with addressing cybercrimes,[59] and with similar laws adopted by other nations, the relative merits of the Act can be ascertained. Finally, whether the Act will provide reassurance to potential MSC investors can be evaluated in light of concerns businesses have expressed about computer crime, their concerns about computer crime laws in other countries, and the Act's ability to address these concerns.

Although the passage of the Act is an important step toward the achievement of Malaysia's goals, the Act, as it stands, fails to take progressive steps to deter computer crime, fails to establish Malaysia as a leader in the development of cyberlaws, and in fact may fail to convince MSC investors that their interests will be protected.

C. Criminalization of Unauthorized Access

Section 3 of the Act criminalizes any intentional access to a computer without authorization.[60] The penalty for violation of this provision is a fine of up to RM50,000 (approximately $13,000),[61] a prison term of up to five years, or both.[62] This provision is a bold and decisive statement of Malaysia's intolerance of hacking and will undoubtedly reassure potential investors. This provision goes beyond the recommendations of the Organization for Economic Cooperation and Development ("OECD")[63] and the Council of Europe.[64] Both of these

---

[59] The two organizations which have made recommendations examined in this Comment are the Organization for Economic Cooperation and Development and the Select Committee of Experts on Computer-Related Crime. *See infra* notes 63-64.

[60] The Computer Crimes Act 1997 § 3.

[61] As of May 8, 1998, the Federal Reserve Bank of New York reported the Ringgit exchange rate was US $.261780 per ringgit. Therefore, a fine of 50,000 ringgit would be approximately U.S. $13,089.00. Kurt Swanson, *Foreign Exchange Rates: Malaysian Ringgit-United States Dollar* (visited May 11, 1998) <http://www.dna.lth.se/cgi-bin/kurt/rates?MYR+USD>.

[62] The Computer Crimes Act 1997 § 3.

[63] The Organization for Economic Cooperation and Development (OECD) is an international body composed of twenty-nine countries which coordinate the policies of member nations. Its principal goals are to promote the economic growth of its member nations and improve the social and economic well beings of their populations. *About OECD*, (visited May 11, 1998) <http://www.oecd.org.about/.whats.htm>.

[64] In 1986, the OECD recommended that member states adopt laws which would consider five activities to be offenses: inputting or altering data or programs with intent to illegally transfer funds or other items of value; inputting or altering data with intent to commit a forgery; inputting or altering data

organizations have included the criminalization of unauthorized access on their mandatory lists of offenses, but only if security measures, such as password protections, are infringed in order to gain access to the computer.[65] Although the United States Congress has not criminalized mere unauthorized access of a computer which does not contain data related to national security,[66] most states within the US have made simple, unauthorized access a crime whether or not security measures were circumvented.[67]

Criminalization of simple, unauthorized access is wise, whether or not security measures were infringed and whether or not damage was actually done. All too often, hackers access one computer in order to gain access to another computer, sometimes many times over.[68] One reason hackers take this indirect approach is to take advantage of one computer's recognition of another computer as "a trusted computer."[69] This technique saves the hacker the trouble of cracking the passwords to the second system. Other times this strategy is used by hackers to cover their tracks and make it more difficult for their identities to be determined.[70]

---

or programs with intent to disrupt the functioning of a computer; the infringement of the exclusive right of the owner of a protected computer program with the intent of commercial exploitation; and the access of a computer system by infringement of security measures or for other dishonest or harmful means. This list was formulated to serve as a basis for harmonization of computer crime laws among the members of OECD. UN MANUAL, *supra* note 20, at ¶ 118. From 1985 to 1989 the Select Committee of Experts on Computer-Related Crime of the Council of Europe and the European Committee on Crime problems examined the computer crime problem and prepared Recommendation No. R(89)9 which they adopted in Sept. of 1989. *Id.* at ¶ 119. Several offenses listed in Recommendation No. R(89)9 were considered non-optional including: computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage and unauthorized access by infringing security measures. The Recommendation also contains an optional list which includes unauthorized use of a computer when there is significant risk of loss or intent to cause loss. *Id.* at ¶ 122. Unlike the OECD, the Council of Europe Convention is a contractual commitment made by the ratifying states. *Id* at ¶ 135.

[65] The Computer Crimes Act 1997 § 3.

[66] 18 U.S.C. § 1030(a) (1997).

[67] *See, e.g.*, CAL. PENAL CODE § 5029(c)(7) (Deering 1996), CONN. GEN. STAT. § 53a-251 (1997), HAW. REV. STAT. §§ 708-892 (1997), IOWA CODE § 716A.2 (1996), OHIO REV. CODE ANN. § 2913.04 (Anderson 1997).

[68] *See, e.g.*, Carolyn Hong, *Keeping Hackers at Bay With Help of New Organisation*, NEW STRAITS TIMES (Malaysia), Mar. 23 1998, at 13, *available in* LEXIS, Asiapc Library, Nstrtt File.

[69] A "trusted" computer is one which is able to connect with another computer which recognizes its Internet Protocol address number. Lisa Mitchell, *Australia: Criminal Hacker Activity Rising, Industry Watchdog Body Warns*, THE AGE (Melbourne), Jan. 31, 1995 *available in* LEXIS News Library, Txtprm File. Every computer that is connected to the internet has an assigned address that enables other computers to "find" it. These addresses currently consist of a four groups of numbers from 0 to 255 separated by periods. ITS HELP DESK, UNIVERSITY OF IOWA, *Terminology and Conventions*, (visited May 8, 1998) <http://wolf.weeg.uiowa.edu/helpdesk/FAQhtmls/conventions.html.>

[70] *See, e.g.*, Hong *supra* note 68.

Unauthorized access with intention to commit a further offense in the form of another crime is considered to be more serious under the Act, with penalties commensurate with that status.[71] Unauthorized access with intent to commit acts of fraud or dishonesty is punishable by a fine of up to RM150,000,[72] a prison term of up to ten years, or both.[73] The OECD and the Council of Europe address this offense in their recommendations of activities which should constitute criminal offenses and, like Malaysia, do not restrict criminalization to occurrences when the accessed computer was "secured."[74]

D. Criminalization of Actions Causing Unauthorized Modifications

Section 5 of the Act is another bold and definitive statement against the activities of those who would harm the interests of MSC investors. Under Section 5 it is a crime to do any act which the actor knows will cause the unauthorized modification of a program or data, even if the actor does not target a specific computer, specific data, or a specific program.[75] Violation of this provision is punishable by a fine of RM100,000.[76] Because viruses always cause some modification of programs or data, this provision criminalizes knowingly putting a computer virus into circulation.[77]

The recommendations of the OECD and the Council of Europe include provisions regarding the modification of a program or data in specific circumstances.[78] The simple act of modifying a program or data does not appear in the OECD recommendations, though it is included in the Council of Europe's list of optional provisions.[79] But Malaysia's inclusion of program or data modification in its Act is not the only way in which the Malaysian Act surpasses the minimum recommendations of the OECD and Council of Europe. While the OECD's and Council of Europe's "minimum list" language recommends criminalizing modification of data or programs which damage a computer system or impair its functioning,[80] the language in the

---

[71] The Computer Crimes Act 1997 § 4.

[72] RM150,000 is equivalent to $39,267.00. *See supra* note 61.

[73] The Computer Crimes Act 1997 § 4.

[74] *See* UN Manual, *supra* note 20, at ¶¶ 118, 121-22.

[75] The Computer Crimes Act 1997 § 5.

[76] RM100,000 is equivalent to $26,178.00. *See supra* note 61.

[77] A virus is a computer program that propagates itself by attaching to programs which will be shared among computer systems. UN MANUAL, *supra* note 20, at ¶ 69.

[78] *See* UN MANUAL, *supra* note 20, at ¶¶ 118, 121-22.

[79] *Id.* at ¶¶ 121-22.

[80] *Id.* at ¶¶ 118, 121.

Malaysian provision will allow prosecution for the release of a virus, even if the virus is non-destructive.[81]

The wording of Section 5 of Malaysia's Computer Crimes Act is quite similar to Section 3 of the United Kingdom's Computer Misuse Act 1990 which also criminalizes acts that cause an unauthorized modification to the contents of any computer whether or not the intent to make modifications was directed at any particular computer, data or program.[82] This provision in the United Kingdom's Act was successfully used to convict the notorious virus writer, Christopher Pile.[83] In November 1995 Pile, known as "The Black Baron," pleaded guilty to charges of violating Section 3 of the Computer Misuse Act stemming from writing two viruses which eventually spread throughout the world.[84] Upon conviction, Pile was sentenced to eighteen months in prison.[85] Malaysia's adoption of a statute which is textually similar to one used to obtain the conviction of at least one high-tech criminal should reassure MSC investors that the Malaysian law is effective and the government is serious about protecting investors' interests.

E. Criminalization of the Unauthorized Communication of Access Codes

Section 6 of the Act criminalizes the communication of a means of access to a computer to an unauthorized person and provides for a RM25,000[86] fine, a prison term of up to seven years, or both.[87] Although this is a progressive measure that the OECD and Council of Europe did not include in their recommendations,[88] it fails to specify whether or not even the unintentional communication of the password is criminalized.[89] If Malaysia's

---

[81] Among the European nations, the spreading of a virus is currently a criminal offense in Britain, Italy, the Netherlands and Switzerland, while Finland was considering similar legislation as of early 1997. *Finland Considering Law Against Spreading Computer Viruses*, Agence Fr. Presse, Feb. 6, 1997, *available in* 1997 WL 2054584. The United States has criminalized the knowing transmission of a program which results in damage to computers containing national security information. 18 U.S.C. § 1030(a)(5)(A).

[82] Computer Misuse Act 1990 § 3.

[83] Geoffry Gibbs, *Black Baron's Computer Virus Plague*, GUARDIAN (London), Nov. 16, 1995, at 2, *available in* LEXIS, News Library, Guardn File; Robert Uhlig, *"Black Baron" Jailed Over Computer Virus That Caused Chaos,"* DAILY TELEGRAPH (London), Nov. 16, 1995, *available in* LEXIS, World Library, Telegr File.

[84] *Id.*

[85] *Id.*

[86] RM25,000 is equivalent to $6544.50. *See supra* note 61.

[87] *See* The Computer Crimes Act 1997 § 6.

[88] *See* UN MANUAL, *supra* note 64, at ¶¶ 118-22.

[89] *Id.*

intent was to create strict criminal liability regarding this offense, that intent should be clearly stated. However, the imposition of strict criminal liability on employees and others by criminalizing mistakes is of questionable value.[90] The fact that this provision of the Computer Crimes Act lacks clarity and can be interpreted in a way which may be of questionable value undermines Malaysia's ability to be a leader in the development of cyberlaws.

Strict criminal liability is frequently criticized by legal scholars as inadequate for retributive, deterrent and rehabilitative purposes.[91] In addition, trial judges may have difficulty imprisoning a defendant who has not intentionally committed a crime.[92] Prosecutors and legislators, however, are not as disapproving of strict criminal liability which, by definition, removes the burden of proving the defendant had a culpable mental state.[93] The imposition of strict criminal liability is both an efficient and nearly guaranteed way to convict defendants.[94]

The Malaysian Parliament may have intended to make unauthorized communication of an access method a strict criminal liability offense, but without guidance in the statutory language, the applicability or nonapplicability of a mens rea requirement is seemingly left to the discretion of the Malaysian judiciary.[95]

F. Abetting or Furthering an Offense Under the Act

Under Section 7 of the Computer Crimes Act, anyone who abets the commission of an offense under the Act, or does any act preparatory to or in furtherance of an offense, is guilty of the substantive offense.[96] Abetting, or attempting to commit, an activity criminalized by the Act is punishable by the same penalty as the substantive violation.[97] Actions taken in preparation or

---

[90] *See, e.g.*, Anthony A. Cuomo, *Mens Rea and Status Criminality*, 40 S. CAL. L. REV. 463, 516-22 (1967).

[91] *Id.*

[92] Laurie L. Levenson, *Good Faith Defenses: Reshaping Strict Liability Crimes*, 78 CORNELL L. REV. 401, 404 (1993).

[93] *Id.* at 403-04.

[94] *Id.* at 404.

[95] For an example of the confusion resulting from the absence of statutory language requiring culpability, *see* Morissette v. United States, 342 U.S. 246, 72 S.Ct. 24 (1952). Morissette was convicted of converting government property in violation of a federal statute which on its face did not require a showing of intent. The Supreme Court overturned the conviction holding a statute which does not require a showing of intent should rarely impose strict criminal liability. Morissette, 342 U.S. at 275.

[96] *See* The Computer Crimes Act 1997 § 7.

[97] *Id.*

furtherance of an activity criminalized by the Act is punishable by one half the maximum prison term of the substatntive offense, the full fine, or both.[98] Neither the OECD nor the Council of Europe address these offenses in their recommendations.[99]

Due to its apparent inconsistency with Section 6, Section 7 may be better suited to attracting businesses to the MSC than it is to putting Malaysia in a position of leadership in the development of cyberlaws. Given that the Act specifically criminalizes the unauthorized communication of passwords or computer access codes in Section 6,[100] it is difficult to construe the scope of Section 7's anti-abetting provision.

Malaysia's statutory interpretation cannons may allow its judges to deal with the apparent inconsistency of Sections 6 and 7 without difficulty. However, Malaysia cannot expect to be considered a leader in this area of the law when it adopts seemingly conflicting provisions that judges of other nations might not be able to reconcile. A basic principle of statutory interpretation used by judges in the United States is the presumption that since "the legislature does not intend to contradict itself or to include meaningless provisions, every part of a statute should be given effect if possible."[101] It appears that in order to give meaning to the provision which prohibits the unauthorized communication of passwords, the term "any act in furtherance" in the anti-abetting provision must be interpreted narrowly.

Requiring such a narrow interpretation would not be cause for concern except for the fact that Malaysia seeks a leadership role in the development of cyberlaws.[102] However, in those countries which have statutory interpretation cannons similar to those of the United States, following Malaysia's lead in this case could result in some rather constrained interpretations. If password trafficking is not considered to be in furtherance of an offense under the Act, questions arise as to the law's applicability to someone who purposefully inserts a "trap door" into an operating system program which allows anyone with a predetermined access code to log into the affected system. Malaysian courts will likely be able to interpret these provisions favorably. However, the courts of other nations may find the interpretation of such provisions to be problematic.

---

[98] *Id.*

[99] *See* UN Manual, *supra* note 21, at ¶¶ 118-21.

[100] *See* The Computer Crimes Act 1997 § 6.

[101] Alan R. Romero, *Interpretive Directions in Statutes*, 31 HARV. J. ON LEGIS., 211, 232-33 (1993).

[102] *See supra* note 57, and accompanying text.

G. Unauthorized Custody or Control of a Program or Data

Section 8 may prove to be the most useful provision both in the prevention of computer crimes and in instilling investor confidence. Section 8 creates a statutory presumption that anyone who has unauthorized custody or control over information held in a computer has obtained unauthorized access to that information.[103] This provision is directed at preventing software piracy and the theft of trade secrets, a crucial factor in assuring the success of the MSC.[104] As one article put it, Section 8 of the Computer Crimes Act will give "added ammunition to the current campaign to wipe out software piracy" which previously had to shoulder the burden of proving that the "errant party actually committed the act of piracy."[105] The creation of a statutory presumption of unauthorized access is an approach which neither the OECD nor the Council of Europe included in their recommendations.[106]

One criticism of Section 8 is that it may make criminals out of those who own systems which are used by hackers to deposit information retrieved from other, less accessible, systems.[107] Under Section 8 of the Computer Crimes Act, the critics contend, an unknowing owner of the deposit site would be presumed to have obtained unauthorized access to that program.[108] However, Representatives from the Attorney General's Chambers have asserted that mere possession of unauthorized data is not enough to prosecute someone under this provision.[109] The representatives explained that custody and control, as well as possession, is required.[110] Given that the legal definition of possession usually contains elements of control and intent to

---

[103] *See* The Computer Crimes Act 1997 § 8.

[104] According to Dennis Unkovic, a partner in a Pittsburgh based law firm and participant in a panel discussion on the MSC, assurances that trade secrets and other technology will be protected is crucial to Malaysia's ability to attract foreign companies to the MSC. *See* Cheah Chor Sooi, *supra* note 13. *See also* Ferina Manecksha, *supra* note 58. According to Energy, Telecommunications and Posts Minister Datuk Leo Moggie, "software piracy in Malaysia is not as serious as in other countries, yet the country must strive to curb the problem in order to protect the country's software industry, particularly in view of the MSC development." Sharifah Kasim, *Delay in Cyberlaw Implementation*, NEW STRAITS TIMES (Malaysia), Dec. 2, 1996, at 1, *available in* LEXIS, Asiapc Library, Nstrtt File.

[105] *Bill Deals Blow to Hackers, Software Piracy*, NEW STRAITS TIMES (Malaysia), Apr. 6, 1997, at 31, *available in* LEXIS, Asiapc Library, Nstrtt File.

[106] *See* UN MANUAL, *supra* note 20, at ¶¶ 118-22.

[107] *Cyberlaw-Makers Must Look Into Hackers' Minds: Nair*, FT Asia Intelligence Wire, Apr. 25, 1997, at B41, *available in* LEXIS, Asiapc Library, Aiw File.

[108] *Id.*

[109] *Id.*

[110] *Id.*

exercise that control,[111] this explanation is redundant and the criticism is likely unfounded.

The added ammunition this provision provides against software piracy by criminalizing the knowing possession of illicitly obtained software will undoubtedly reassure MSC investors that software piracy is taken seriously by the Malaysian government.

H. Jurisdictional Issues

Section 9 extends Malaysia's jurisdiction to those who commit an offense under the Act if the computer, program or data accessed or modified was in Malaysia or capable of being connected to, sent to, or used by or with a computer in Malaysia at the material time.[112] This provision is problematic because any computer in Malaysia which has a floppy drive or any type of internet connection can be accessed by, or receive a program or data from, any other computer which has similar capabilities. In other words, this provision applies Malaysian law to any hacker or virus writer who accesses or infects any computer, whether or not a Malaysian computer is ever involved in, or affected by, the activity. It is impossible to say whether this broad assertion of jurisdiction was intentional. Media analyses and government statements indicate this provision was intended to allow Malaysia to extradite those who access a computer located in Malaysia without authorization and those who made unauthorized modifications to the contents of a Malaysian computer from outside the country.[113]

With the adoption of this provision Malaysia appears to be joining the United States in circumventing the principle of territoriality,[114] a principle which is generally accepted as an axiom in international criminal jurisdiction doctrine.[115] The principle of territoriality is based on mutual respect for the sovereignty of States and is related to the principle of non-intervention in the

---

[111] *See, e.g.*, BLACK'S LAW DICTIONARY 1163 (6th ed. 1990).

[112] *See* The Computer Crimes Act 1997 § 9.

[113] *See, e.g.*, Risen Jayaseelan, *Policing Cyberspace*, NEW STRAITS TIMES (Malaysia), Aug. 16, 1997, *available in* LEXIS, Asiapc Library, Nstrtt File; *Extradition of Foreigners for Computer Crimes*, FT Asia Intelligence Wire, June 4, 1997, *available in* LEXIS, Asiapc Library, Aiw File.

[114] The United States asserts extraterritorial criminal jurisdiction when the interests of corporate actors are at stake or when criminal activity might have negative consequences within the United States. Mark P. Gibney, *The Extraterritorial Application of U.S. Law: The Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles*, 19 B.C. INT'L & COMP. L. REV. 297, 304-05 (1996).

[115] *See, e.g.*, UN MANUAL *supra* note 20, at ¶¶ 249-60.

exclusive domain of other States.[116] There are only a few accepted bases for applying the principle of extraterritoriality: the nationality of the accused, the nationality of the victim, the protection of national security interests of a State, and the rarely invoked basis of protection of universal values.[117] Although there are no rules of international law that impose limitations on the establishment of extraterritorial criminal jurisdiction, a State should be expected to take due account of the principles of cooperation and reasonableness in exercising such jurisdiction.[118] Neither the OECD nor the Council of Europe propose extension of jurisdiction in this manner.[119]

Practically speaking, it does not matter if the language of the provision authorizes law enforcement to assert jurisdiction over a foreign hacker or virus writer whose activities have never affected a Malaysian computer. Malaysian law enforcement officials will simply be unable to pursue such a prosecution without international cooperation.[120] In fact, according to Malaysian experts, Malaysian officials will have a difficult time pursuing a foreign offender who does affect Malaysian computers.[121] Regardless of the practical application of this provision, however, Malaysia has adopted a provision which may foster resentment in the international community and damage its credibility with its unrealistic assertion of jurisdiction. Malaysia cannot claim leadership in the development of cyberlaws when provisions as unrealistic or as awkwardly drafted as this one are in effect.

I. Search & Seizure and Hinderance of an Investigation

The ancillary provisions, Sections 10 and 11, which give the Malaysian police broad authority to investigate computer crimes, may be cause for concern among potential MSC investors. Through Section 10 of the Act, Malaysia has given any officer above the rank of inspector the power to seize evidence of a computer crime, in some cases without a warrant.[122] Additionally, Section 11 makes it a crime to "hinder or delay any police officer in affecting entrance to any premises . . . or in the

---

[116] *Id.* at ¶ 249.
[117] *Id.* at ¶ 255.
[118] *Id.* at ¶ 259.
[119] *Id.* at ¶¶ 118-22.
[120] *See generally, Cyberlaw Int'l Enforcement Needs Common Approach, supra* note 11; UN MANUAL, *supra* note 20, at ¶¶ 245-88.
[121] *See generally, Cyberlaw Int'l Enforcement Needs Common Approach, supra* note 11.
[122] *See* The Computer Crimes Act 1997 § 10(2).

execution of any duty imposed . . . by this Act."[123] Section 10 undoubtedly applies to the victims of computer crimes as well as the perpetrators because evidence of a computer crime can often be found on a victim's computer. Because failure to report a computer crime could hinder or a delay a police officer who is investigating a string of computer crimes, Section 11 could be interpreted to mandate that victims report computer crimes. This possible interpretation once again raises the issue of clarity and the obvious risk of misapplication of the law posed by the statutory language.[124]

These provisions seem to conflict with the goal of reassuring MSC investors that their businesses and technology will be protected. It is well documented that businesses frequently fail to report being struck by a computer crime,[125] with one survey showing only seventeen percent of respondents who had suffered computer intrusions reported them to law enforcement.[126] The reasons for failing to report include fear of diminished confidence in the corporation among clients and investors,[127] fear of negative publicity in general,[128] and concerns that police seizure of documents, accounts and computers will disrupt business activities.[129]

In light of this reluctance, the Scottish Law Commission, on whose report the United Kingdom's Computer Misuse Act 1990 was in part based,[130] recommended that a mandatory reporting provision be considered.[131] The British Parliament, however, elected not to follow that recommendation.[132] Similarly, the *United Nation's Manual on the Prevention and Control of Computer-Related Crime* recommends promoting victim cooperation in reporting computer crime, but does not go so far as to recommend mandating it.[133]

---

[123] *See Id.* § 11.

[124] *See supra* notes 96-110 and accompanying text for another example of ambiguous statutory language.

[125] *See, e.g.*, Liz Duff and Simon Gardiner, *Computer Crime in the Global Village: Strategies for Control and Regulation—in Defence of the Hacker*, 24 INT'L J. SOC. L. 211, 215 (1996).

[126] Adrian Croft, *Security Group Sounds Alarm About Computer Crime*, Reuters N. Am. Wire, Mar. 6, 1997, *available in* LEXIS, World Library, Reuna File.

[127] Cox, *supra* note 24.

[128] *Id.*

[129] Jacqui MacDonald, *Australia: Immunity Being Considered for Whistleblowers*, THE AGE (MELBOURNE), Sept. 15, 1994., *available in* LEXIS, News Library, Txtprm File.

[130] Wasik, *supra* note 53, at 767.

[131] *See* Steve Shackelford, *Computer-Related Crime: An International Problem in Need of an International Solution*, 27 TEXAS INT'L L.J. 479, 500-01 (1992).

[132] *Id.*

[133] UN MANUAL, *supra* note 20, at ¶ 294(q).

Although mandating the reporting of suspected computer crime activities would greatly assist law enforcement, it seems unrealistic to expect businesses to obey such a law. In fact, regional Computer Emergency Response Teams ("CERTs") have been established in many countries, including Malaysia,[134] in order to give businesses a resource for information about computer crimes and a place to report them in complete confidentiality.[135]

The questionable precision and clarity of the statutory language of the Computer Crimes Act is evident in this provision.[136] Given Malaysia's MSC investor-friendly attitude, it is unlikely that failure to report a computer crime was intended to be a violation of Section 11 of the Act. However, only judicial interpretation can lay to rest this possibility. Again, the drafters have taken a gamble, calling into question Malaysia's leadership role in cyberlaw development as well as its ability to instill investor confidence.

IV. RECOMMENDATIONS FOR STRENGTHENING THE ACT

The Computer Crimes Act can be strengthened by clarifying the existing provisions and by making substantive enhancements to the Act. The existing provisions can be clarified by making alterations in the statutory language which are minimal in scope, but significant in their effects. The Act can be enhanced by supplementing the traditional approaches to computer crime with modern approaches designed to address its causes and minimize the attraction it holds for its perpetrators.

A. Recommended Clarifications to the Statutory Language

In order to establish itself as a leader in the development of cyberlaws, Malaysia's Computer Crimes Act 1997 must provide clear notice of exactly what is being criminalized as well as the territorial scope Malaysia is asserting under the Act. The following clarifications are appropriate: (1) criminalizing only the intentional communication of passwords or access

---

[134] Hong, *supra* note 68.

[135] *See, e.g.*, James Riley, *Australia: Disaster Looms For Hackers' Foe*, SYDNEY MORNING HERALD, July 2, 1996, *available in* LEXIS News Library, Txtnws File. According to Agent Day of AUSCERT, Australia's CERT agency, "[a] business would never report a 'hack' unless confidentiality was assured." *Id.*

[136] A lack of clarity in the statutory language seems to be a problem common to the provisions which were not modeled after the United Kingdom's Computer Misuse Act. *See, e.g., supra* notes 96-110 and accompanying text for another example of this problem.

codes to unauthorized individuals; (2) narrowing the territorial scope of the Act; and (3) criminalizing the knowing failure to report a computer crime.

1. Revealing Access Codes to an Unauthorized Individual

If the Malaysian government did not intend to make the unauthorized communication of an access code a criminal strict liability offense, the statutory language should be modified to preclude this interpretation. This could be accomplished by adopting the following language:

> (1) A person shall be guilty of an offense if he intentionally communicates, directly or indirectly, a number, code, password or other means of access to a computer to any person who he knows, or has reason to believe, is not duly authorized to receive such information.

An alternative to this approach is statutory language which allows the defense of a lack of mens rea.[137] In order to allow such a defense, the alternative provision could be worded as follows:

> (1) A person shall be guilty of an offense 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 authorized to communicate, unless he can establish that he had no intention to communicate that information to an unauthorized person.

This wording would maintain the advantage of relieving the prosecution of the burden of proving intent without creating criminal strict liability.[138]

2. The Territorial Scope of the Act

The assertion of jurisdiction over any individual who violates a provision of the Computer Crimes Act unjustifiably abandons the principle of territoriality and diminishes Malaysia's credibility.[139] Rather than asserting

---

[137] *See* Levenson, *supra* note 92, at 405.
[138] *Id.*
[139] *See supra* notes 114-121, and accompanying text.

jurisdiction over anyone who performs a prohibited act on any computer that is capable of being connected to a computer in Malaysia, it would be more reasonable to assert jurisdiction over individuals who have committed an offense which has a nexus with Malaysia. This could be an offense which affected a computer in Malaysia, was committed by a person who was located in Malaysia at the time, or was committed using a computer located in Malaysia regardless of the location of the computer(s) ultimately targeted or the location from which the offense was initiated.

The United Kingdom's Computer Misuse Act also contains complex and somewhat unclear assertions of jurisdiction,[140] but by extracting some of its statutory language, a clear and concise provision can be attained. One possible way this provision could be worded is:

> (1) It is immaterial for the purposes of any offense under this Act if any act or other event which is an element of the offense occurred in Malaysia, provided there was a link with Malaysia in the circumstances of the act or event.

This wording would enhance the likelihood that other nations will want to incorporate Malaysia's Computer Crimes Act into their own penal codes, thereby enhancing Malaysia's leadership role in the development of cyberlaws.

3. Hinderance of Police Officer's Investigation

If Malaysia intends Section 11 to serve as a mandate that victims report a suspected computer crime, this requirement should be made clear in explicit terms. One possible means of accomplishing this would be to add a new subsection, (1)(c), as follows :

> (1) A person shall be guilty of an offense if he. . .
>
> (c) knowingly fails to report his reasonable suspicion that an offense under this Act has been committed.

[140] Computer Misuse Act (1990) ch. 18, § 2.

However, if the government wants to preclude this Section from being interpreted as mandating the reporting of computer crimes, the new subsection (1)(c) should be worded:

> (c) This section shall not be interpreted to require that a victim of an offense under this Act report the matter to any law enforcement agency or personnel.

B. Recommended Enhancements: Modern Problems, Modern Solutions

Malaysia will not fulfill its goal of being a leader in the development of cyberlaws by relying on the approaches taken in the relatively early days of technology law development. For instance, Malaysia's reliance on the statutory language of the U.K.'s Computer Misuse Act has confined Malaysia to the solutions adopted in that era.[141] If Malaysia would incorporate the following progressive measures into its Computer Crimes Act, it would achieve its goal of becoming a leader in the development of cyberlaws.

1. Adopting Penalties That Fit the Crime

While some critics of the Computer Crimes Act were aghast at the harsh penalties imposed on traditional hackers,[142] others praised its penalty provisions as reasonable in light of the costly damage hackers can inflict.[143] Fines and incarceration are arguably appropriate punishment options, but there are perhaps more meaningful penalties that can be statutorily prescribed as options. One such penalty is the confiscation of the technology used to perpetrate the crime. Confiscating the technology used by the perpetrator is a penalty allowed under the California Penal Code[144] and has the support of at least one expert in the field of technology law.[145]

Another meaningful penalty is the proscription of the criminal's employment in the computer field or any activities with computers for a specified length of time. Proscribing employment or activities that involve

---

[141] *See supra* note 45 and accompanying text.

[142] *Kit Siang: Reduce Proposed Penalties for Hackers*, *supra* note 50.

[143] Zulkifi Othman, *Pikom: Cyber Laws Will Provide Clarity*, BUS. TIMES (Malaysia), Mar. 28, 1997, at 2, *available in* LEXIS, World Library, Txtlne File.

[144] CAL PENAL CODE § 502.01(a)(1) (Deering 1996).

[145] Professor Andrea Johnson, Director of the Center for Telecommunications and Cal Western School of Law in San Diego, suggests this penalty may be an effective deterrent to those who might be tempted to engage in this type of criminal activity. Manecksha & Shahreen, *supra* note 17.

computers may at first blush seem solely retributive, but such a measure may arguably serve to break an addictive pattern that a computer hackers may have developed.[146]

2. *Expand the Scope of the Abetting Provision*

Section 7(1) of the Computer Crimes Act, which makes it an offense to abet the commission of any offense under the Act, would be a formidable weapon in the battle against computer crime if it specifically included supplying cracking software, virus code and the like. Virus how-to guides and code generators are available on underground world-wide Web sites and bulletin boards.[147] System passwords can easily be broken using software programs such as "CRACK"—a program freely available on the Internet.[148] Credit Master, a program available to savvy Internet users, displays valid credit card numbers using algorithms based on numbers used by VISA, MasterCard, American Express, and Discover.[149] Prosecution of those who disseminate, or knowingly allow to be disseminated, software and information which is used in the commission of a crime may effectively reduce its availability.

The idea of holding those who publish criminal how-to guides responsible for the harm they ultimately cause may be an idea whose time has come. One example of a similar basis for liability is a civil case in the United

---

[146] *See generally* MARGARET A. SHOTTON, COMPUTER ADDICTION? A STUDY OF COMPUTER DEPENDENCY (1989). Computer dependency occurs in a small proportion of computer users. *Id* at 235. Frequently recurring characteristics were apparent within a sample of students who described themselves as being computer dependent: a particular personality type, usually described as introverted; excessive amounts of time spent using and thinking about computers; computing undertaken for its intrinsic merit; programming often without a definite, useful end-product; programs unstructured, poorly written and ill-documented; enjoyment of debugging and refining programs; need for power and control over the computer; computer interaction used as an escape from other relationships; lack of desire or time to take part in previous activities; and detrimental effects on academic work. *Id.* at 14, 17.

One such hacker is Kevin Mitnick, characterized as "Cyberspace's Most Wanted Fugitive." John Sweeney, *To Catch A Hacker*, GUARDIAN (London), Sept. 4, 1994, *available in* LEXIS, News Library, Guardn File. When Mitnick was finally arrested after a lengthy FBI investigation, his lawyer portrayed him as a "computerholic." *Id.*

[147] Chris Barton, *New Zealand: Viruses Pose Growing Threat*, NEW ZEALAND HERALD, Apr. 22, 1997, *available in* LEXIS, World Library, Txtlne file.

[148] Peter McLaughlin & Gerard Davis, *Here's How to Handle Corporate Computer Fraud—The Software Feature You Didn't Order*, LEGAL INTELLIGENCER, Aug. 4, 1997, *available in* LEXIS, Legnew Library, Lglint File.

[149] Hiroshi Hirai, *Hackers Take Advantage of Software Displaying Valid Credit Card Numbers—Internet Becomes Major Vehicle For Code-Busters*, DAILY YOMIURI, Nov. 5, 1996, at 8, *available in* LEXIS, Asiapc Library, Yomiur File.

States where a Federal Court of Appeals decided that certain criminally-oriented publications are not protected by the free speech provisions of the First Amendment of the United States Constitution. By so deciding, the court allowed a wrongful death civil suit to proceed to trial.[150] This suit was filed against a publisher for publishing a book which described in detail how to commit murder.[151] While this is far more serious than an economic crime, there is no reason for any society to tolerate the aiding and abetting of costly computer crimes through published information.

3. *Mandate System Security Measures*

Whether by statute or as a condition of granting permission to locate in the MSC, Malaysia should consider mandating organizations to implement common-sense system security measures. There are two reasons these system security measures are critical. First, hackers often gain entry to one or more systems, particularly ones without adequate security, as an initial step in their criminal activity. Among the most prominent reasons hackers access multiple systems are: to prevent being traced,[152] to easily gain access to another system which allows unverified logons from the first computer,[153] and to deposit illicit, and relatively difficult to get, materials on an easily accessed system.[154] Second, businesses located in the MSC will likely keep confidential data about customers which should be protected from unauthorized disclosure.

Corporations are surprisingly lax about installing adequate computer security.[155] Yet one information security specialist contends that most banks already own ninety percent of what they need to prevent computer attacks.[156] The reason so many systems are left unsecured may be that people just do not think their systems will be invaded.[157] The prevalence of this careless attitude

---

[150] Rice v. Paladin Enterprises, Inc., 128 F.3d 233 (4th Cir., 1997) *cert. denied,* 1998 U.S. LEXIS 2548 (U.S. Apr. 20, 1998) (allowing the publisher of a "how-to guide" for hitmen to be subject to a civil suit for wrongful death because speech that constitutes criminal aiding and abetting does not enjoy the protection of the First Amendment).

[151] *Id.*

[152] Hong, *supra* note 68.

[153] Mitchell, *supra* note 69.

[154] "Huge amounts of pirate or bootleg software can be (and are) copied (i.e., "cached") onto unwitting host machines. Within a matter of hours or even minutes, users around the world instantly make hundreds—or even thousands—of illicit copies." Friedman & Buys *supra* note 21.

[155] McLaughlin & Davis, *supra* note 148.

[156] *Computer Crime Rising Against Financial Institutions, supra* note 19.

[157] *Networks: Internet Hackers on the Rise, supra* note 25.

is one reason the authors of the *United Nations Manual on the Prevention and Control of Computer-Related Crime* urges nations to encourage senior executives and management to commit their organizations to security and crime prevention.[158]

The minimum security measures that all organizations should put into place are not burdensome due to the availability of technology for computer security.[159] Basic security measures include: the use of passwords, controlling the information to which users have access, and the use of audit trails.[160] An additional advisable measure recommended by security professionals is the installation of a firewall which restricts access by screening all network communications such as email, file transfers, and remote logins before they are allowed access to the internal network.[161] Some firewall programs are even available without charge on the Internet.[162]

Although some organizations may incorrectly perceive these measures as overly burdensome, the benefits of more secure systems will outweigh any minimal burdens and provide much needed protection to businesses located within the MSC.

V. CONCLUSION

Malaysia is undertaking two ambitious and admirable projects: the development of the Multimedia Super Corridor and the promulgation of cyberlaws which will both promote and protect its growth. The Computer Crimes Act 1997 is a testament to the danger posed by those who use high technology as a tool and a target of crime. It is also a testament to the seriousness with which the Malaysian government is taking this threat. Malaysia's desire to be a leader in the development of cyberlaws is not surprising given the ambitious nature of the MSC and the determination of its leaders in fulfilling Vision 2020. But if a cyberlaw leadership role is in Malaysia's future, the Computer Crimes Act 1997 needs fine-tuning.

While the proposed modifications to those provisions which lack clarity and precision are fairly minor, they would result in provisions which more clearly define the boundary between criminal and non-criminal activities. Moreover, the inclusion of certain additional penalty options, such

---

[158] UN MANUAL, *supra* note 20, at ¶ 294.
[159] Sciglimpaglia, *supra* note 16, at 243.
[160] *See* McLaughlin & Davis, *supra* note 148.
[161] Cox, *supra* note 24.
[162] Head, *supra* note 26.

as the confiscation of technology used in the commission of the crime, would maximize the deterrent effects of the law as well as address some of the possible causes of the miscreant behavior and would thereby strengthen the Act. By holding those who indirectly participate in computer crime activity by posting, or otherwise distributing, software which enabled others to violate the provisions of the Act, Malaysia would break new ground in the deterrence and curtailment of computer crime and deservedly earn a position as a leader in the development of cyberlaws.