

**ETHICS OF INFORMATION COMMUNICATION
TECHNOLOGY (ICT)**

Paper prepared by Tengku Mohd T. Sembok,
Universiti Kebangsaan Malaysia
for the Regional Meeting on
Ethics of Science and Technology
5-7 November 2003, Bangkok

UNESCO
Regional Unit for Social & Human Sciences in Asia and the Pacific
(RUSHSAP)

ETHICS OF INFORMATION COMMUNICATION TECHNOLOGY (ICT)

1. INTRODUCTION

Globalization and digital convergence in the emerging knowledge society has raised complex ethical, legal and societal issues. We are faced with complex and difficult questions regarding the freedom of expression, access to information, the right to privacy, intellectual property rights, and cultural diversity. ICT is an instrumental need of all humans for the gathering of information and knowledge, and as such, should be guaranteed as a basic right to all human beings. All over the world, rights that are already legally recognised are daily being violated, whether in the name of economic advancement, political stability, religious causes, the campaign against terrorism, or for personal greed and interests. Violations of these rights have created new problems in human social systems, such as the digital divide, cybercrime, digital security and privacy concerns, all of which have affected people's lives either directly or indirectly.

It is important that the countries of the Asia-Pacific region come up with an assessment of the situation, followed by guidelines for action to combat the incidence of malicious attacks on the confidentiality, integrity and availability of electronic data and systems, computer-related crimes, such as forgery and fraud, content related offenses, such as those related to child pornography, and violations of intellectual property rights (IPRs). Further, threats to critical infrastructure and national interests arising from the use of the internet for criminal and terrorist activities are of growing concern after the September 11 incident. The harm incurred to businesses, governments and individuals in those countries in which the internet is used widely, is gaining in scope and importance, while in other countries, cybercrime threatens the application of information and communication technology for government services, health care, trade, and banking. As users start losing confidence in transactions and business, the opportunity costs may become substantial.

The challenges to the region, reportedly, lie mainly in the general lack of awareness of information security issues, the rapidly evolving complexity of systems, the increasing capacity and reach of information and communication technology, the anonymity afforded by these technologies, and the transnational nature of communication networks. Few countries in the region have appropriate legal and regulatory frameworks to meet these challenges. Even where awareness is growing and where legislation may be adequate, capacity to use information security technologies and related procedures, as well as to protect against, detect and

respond effectively, to cybercrime, is low. As a result, reports of cybercrime may represent only a small fraction of their incidence, creating a need for more accurate estimates of the prevalence of cybercrime. (Duggal, <http://www.cyberlaws.net/cyberindia/articles.htm>).

There are a few countries of the region which, as a result of governmental investment, policy development and human resources development programmes, have built significant capacity, experience and know-how which can be shared with other countries. Cybercrime is a global problem that threatens all countries and economies. As a crime that is committed across national borders, it requires cooperative, pro-active approaches in support of the less developed countries of the region.

The objective of this paper is to compile:

- i. Information concerning ethical issues in the Asia-Pacific regarding:
 - i. Digital Divide
 - ii. Poverty
 - iii. Piracy
 - iv. Cybercrime
 - v. Human Rights
 - vi. Gender Equality
- ii. Information on the initiatives and programmes undertaken at the local, national, regional, and international levels concerning the above matters; and
- iii. Recommendations to overcome the challenges and issues raised.

Based on the findings, recommendations for action will be highlighted as programmes towards combating the negative aspects of the use of ICT, and towards achieving the positive results of embracing ICT culture in everyday life.

1.1 Overview

Information technology is impacting all walks of life all over the world. ICT developments have made possible a transition in information storage, processing, and dissemination, from paper to virtual and from atoms to bits, which are now setting new standards of speed, efficiency, and accuracy in human activities. Computerized databases are extensively used to store all sorts of confidential data of political, social, economic or personal nature to support human activities and bringing various benefits to the society.

However, the rapid development of ICT globally also has led to the growth of new forms of national and transnational crimes. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness, policy formation, and enactment of necessary legislation in all countries for the prevention of computer related crime. Globally, internet and

computer-based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activities, and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. The new boundaries, which are manifested in the monitor screens, firewalls, passwords, intruder detection, and virus busters, have created new personalities, groups, organizations, and other new forms of social, economic, and political groupings in the cyber world of bits. Traditional border-based law making and law enforcing authorities find this new environment of cyber boundaries very challenging.

Cyber systems across the globe have many different rules governing the behaviour of users. Users are completely free to join or leave any system whose rules they find comfortable or uncomfortable. This flexibility may at times lead to improper user conduct. Also, in the absence of any suitable legal framework, it may be difficult for System Administrators to check on frauds, vandalism or other abuses, which may cause the lives of many online users to be miserable. This situation is alarming because any element of distrust for the internet may lead to people avoiding doing transactions online, thereby directly affecting the growth of e-commerce. The use or misuse of the internet as a medium of communication may in some situations lead to direct damage to real physical society. Non-imposition of taxes on online transactions may have its destructive effect on physical businesses, and also government revenues. Terrorists may also make use of the web to create conspiracies and violence. Wide and free sharing of ideologies, beliefs, convictions, and opinions between different cultures might cause physical and emotional stress and confusion that might lead to physical violence.

1.2 What is Ethics

In the last decade, dozens of ethics centres and programmes devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. These centres are designed to examine the implications of moral principles and practices in all spheres of human activity on our lives.

Ethics can be viewed from two angles, normative and prescriptive. First, ethics refers to well-based standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, and specific virtues. Ethics, for example, refers to those standards that impose the reasonable obligations to refrain from rape, stealing, murder, assault, slander, and fraud. Ethical standards also include those that enjoin virtues of honesty, compassion, and loyalty. And, ethical standards include standards relating to rights, such as the right to life, the right to freedom from injury, the right to choose, the right to privacy, and right to freedom of speech and expression. Such standards are adequate standards of ethics because they are supported by consistent and well-founded reasons.

Secondly, ethics refers to the study and development of personal ethical standards, as well as community ethics, in terms of behaviour, feelings, laws, and social habits and norms which can deviate from more universal ethical standards. So it is necessary to constantly examine one's standards to ensure that they are reasonable and well-founded. Ethics also means, then, the continuous effort of studying of our own moral beliefs and conduct, and striving to ensure that we, and our community and the institutions we help to shape, live up to standards that are reasonable and solidly-based for the progress of human beings.

Definition

“Ethics are moral standards that help guide behaviour, actions, and choices. Ethics are grounded in the notion of responsibility (as free moral agents, individuals, organizations, and societies are responsible for the actions that they take) and accountability (individuals, organizations, and society should be held accountable to others for the consequences of their actions). In most societies, a system of laws codifies the most significant ethical standards and provides a mechanism for holding people, organizations, and even governments accountable.” (Laudon, et al, 1996)

1.3 ICT Ethics

ICT ethics are not exceptional from the above-mentioned view of ethics. In a world where information and communication technology has come to define how people live and work, and has critically affected culture and values, it is important for us to review ethical issues, as well as social responsibility, in the Asia-Pacific region. This is a difficult task because of the diversity in creed, class, caste, dialect, language, culture and race throughout the region. Moreover, the issue of ICT ethics takes on added significance as the region struggles with the dynamics of globalization and the current political environment after the September 11 incident.

ICT Ethical Issues

Analysing and evaluating the impact of a new technology, such as ICT, can be very difficult. ICT does not only involve technological aspects, but also epistemology since the main component of ICT is information which represents data, information, and knowledge. ICT assists and extends the ability of mankind to capture, store, process, understand, use, create, and disseminate information at a speed and scale which had never been thought possible before. Some of the impact and changes of ICT are obvious, but many are subtle. Benefits and costs need to be studied closely for a nation to progress and improve the quality of life for its citizens. Issues that have arisen from the adoption of ICT, such as the application of automated teller machines (ATM), can be summarized as follows (Baase, 1997):

- Unemployment

The automation of work has caused creative destruction by eliminating some vocations and creating new ones. How does this affect the employment or unemployment of the work force of a nation?

- Crime

Stolen and counterfeit ATM cards are used to steal millions of dollars each year throughout the region. The anonymity of the machines makes some crimes easier and creates many new types of crimes.

- Loss of privacy

Transactions are transmitted and recorded in databases at banks, hospitals, shopping complexes, and various organizations, in the public or private sector. The contents of electronic communications and databases can provide important and private information to unauthorised individuals and organizations if they are not securely guarded.

- Errors

Information input into the databases is prone to human and device error. Computer programmes that process the information may contain thousands of errors. These errors can create wrong and misleading information about individuals and organizations. Information and programme errors might result in financial loss, or even the loss of lives.

- Intellectual property

Millions of dollars of software is illegally copied each year all over the world. This phenomenon has a great impact on the software industry in the region. Local and foreign software industries need consumers support all over the world to maintain the progress of technology. Most importantly, for the sake of growth in indigenous ICT innovation and invention, local software industries in Asia-Pacific need local support in protecting their intellectual property rights and investment.

- Freedom of speech and press

How do the constitutional rights of individuals in terms of the freedoms of speech and press apply to electronic media? How seriously do the problems of pornography, harassment, libel, and censorship on the net affect individuals and society? What government initiatives have been used in handling this crisis?

- Digital Divide

How does ICT affect local community life? The increasing use of computers has increased the separation of rich and poor, creating a digital divide between the information “haves” and “have-nots.” What subsidies and programmes have been provided by governments of the region to address the issue?

- Professional Ethics

How well trained and ethical are our ICT professionals in dispensing their duties? Faulty and useless systems that cause disasters and hardships to users might be built by incompetent ICT professionals. In dispensing their duties ICT professionals must demonstrate their best practices and standards as set by professional bodies for quality assurance.

1.4 UNESCO's Info-Ethics Programme

The development of digital technologies and their application in worldwide information networks are opening vast new opportunities for efficient access to and use of information by all societies. All nations can fully benefit from these opportunities on the condition that they meet the challenges posed by these information and communication technologies. Thus, UNESCO's Info-Ethics Programme was established for the principal objective of reaffirming the importance of universal access to information in the public domain, and to define ways that this can be achieved and maintained in the Global Information Infrastructure. It seeks to address the areas of ethical, legal and societal challenges of cyberspace, as well as privacy and security concerns in cyberspace. It aims to encourage international cooperation in the following aspects: (http://www.unesco.org/webworld/public_domain/legal.html)

- Promotion of the principles of equality, justice and mutual respect in the emerging Information Society;
- Identification of major ethical issues in the production, access, dissemination, preservation and use of information in the electronic environment; and
- Provision of assistance to Member States in the formulation of strategies and policies on these issues.

2. REGIONAL ISSUES

2.1 *Cybercrime*

There are no scientifically conducted detailed studies exclusively on the issue of cybercrime and information security in the Asia-Pacific region. However, some broad figures are available in the public domain, which can serve as indicators of the broad situation in the region today. Surveys conducted by Computer Security Institute (CSI, 2003) confirm that the threat from computer crime and information security breaches continues unabated and that its financial toll is mounting. However, the financial losses reported have plummeted. Fifty-six percent of respondents reported unauthorized use, compared to 60 percent last year (and compared to an average of 59 percent over the previous seven years of the survey). The total annual losses reported in the 2003 survey were \$201,797,340, a figure that is down 56 percent from the high-water mark of \$455 million reported last year. The overall number of significant incidents remained roughly the same as last year, despite the drop in financial losses. Followings are some of main findings reported in the survey:

- As in prior years, theft of proprietary information caused the greatest financial loss (\$70,195,900 was lost, with the average reported loss being approximately \$2.7 million).
- In a shift from previous years, the second most expensive computer crime among survey respondents was denial of service, with a cost of \$65,643,300.
- Losses reported for financial fraud were drastically lower, at \$10,186,400. This compares to nearly \$116 million reported last year.
- As in previous years, virus incidents (82 percent) and insider abuse of network access (80 percent) were the most cited forms of attack or abuse.
- Respondents again weighed in strongly opposed to the idea of hiring reformed hackers (68 percent were against).
- The percentage of those who reported suffering incidents in the prior year who said they reported those incidents to law enforcement remained low (30 percent).

The statistics gathered on few countries in the region, as listed below, gives us some indication as to the seriousness of cybercrime in the region.

2.1.1 **Cybercrime in Malaysia**

Cases related to ICT are often reported in local vernacular papers concerning various issues ranging from cybercrime to equal access to the internet. The following are some examples of common news items concerning cybercrime that appeared in Malaysian newspapers:

- Hackers have struck at government websites again, this time targeting the Social Security Organization (Socso) by posting an image of a covered skull on its site at: <http://www.perkeso.gov.my> (26th June 2001).
- Sixty government websites have been hacked between February 1, 1999 and April 3 this year, with a total of 89 actual hacking incidents taking place.
- Dec 29, 2001: A hacker intrusion on the Malaysian Parliament's website has reportedly generated criticism from some officials who claim the government has taken a slapdash approach to internet security.
- 22nd August 2000: A hacker is believed to have tried to dupe internet users into giving away their private financial information by posing as an online executive at Maybank Bhd.

In the first six months of 2003, Malaysian NISER recorded 394 incidences of cybercrime as shown in Table 2.1 below. 48.47 percent of the reported incidences were hack threats followed by virus attacks at 28.68 percent.

Table 2.1. Incident Statistics in Malaysia JAN-JUN 2003

	<i>Jan</i>	<i>Feb</i>	<i>Mar</i>	<i>Apr</i>	<i>May</i>	<i>Jun</i>	<i>Total</i>	<i>%</i>
Hack Threat	20	4	42	40	41	44	191	48.47
Virus	16	6	3	24	51	13	113	28.68
Spam	3	5	6	7	6	8	35	8.88
Intrusion	4	2	0	5	11	3	25	6.34
Harassment	5	2	1	3	1	3	15	3.80
Forgery	1	1	1	2	2	3	10	2.53
Denial of Service	0	0	0	1	1	1	3	0.76
Mail bomb	0	0	0	0	1	0	1	0.25
Destruction	0	0	0	0	0	0	0	0
TOTALS	49	20	53	83	114	75	394	100

Source: NISER (<http://www.niser.org.my>).

2.1.2 Cybercrime in Japan

The following are some examples of cases reported in Japan:

- Crime related to internet dating services in Japan more than doubled in the first six months of 2002.
- 800 sex crimes have been reported for the first half of 2002 as compared to 888 for the whole of 2001.
- The total number of crimes involving the internet was almost 60 percent higher in the first half of 2001 than in the first half of 2000.
- A worker for NEC Toshiba Space System Co. illegally accessed Mitsubishi Electric Corporation's antenna designs for a high-speed internet satellite in December 2001 (*Ananova*, <http://www.ananova.com/news/story/>).

- The National Police Agency said that there were about 51,000 attempts by hackers to break into police computer systems throughout the country during the three-month period from July to September 2002 (The Japan Times, <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20021108a3.htm>).

Crimes reported in 2000-2001 (Tatsuzaki, 2002):

- The combined figure for the purchase of sex from underage children and child pornography has doubled.
- Internet fraud has increased by 94 percent.
- Crime involving internet auctions has increased by 140 percent.

2.1.3 Cybercrime in South Korea

The following are a couple examples of cases reported in South Korea (Computer Crime Research Centre, <http://www.crimeresearch.org/eng/news/2002/10/Mess1602.htm>):

- In South Korea, cyber offences, including slandering and financial fraud online, shot up 126 percent (33,289 cases) in 2001 from a year before.
- The number of cases jumped 43 percent in 2000, with computer-savvy teenagers topping the list of offenders.

2.1.4 Cybercrime in Hong Kong

The table below is of cybercrimes reported in Hong Kong from 1995-2000 (Broadhurst, 2002) showing an increase from a total number of 14 in 1995 to 368 in 2000, an increase in 26 times in 5 years.

Table 2.2. Cybercrime in Hong Kong 1995-2000

<i>Cases</i>	<i>1995</i>	<i>1996</i>	<i>1997</i>	<i>1998</i>	<i>1999</i>	<i>2000</i>
Hacking/Cracking*	4	4	7	13	238	275
Damage Online	2	4	3	3	4	15
Deception	0	0	2	1	18	29
E-Theft & Other	8	13	8	17	57	49
TOTALS	14	21	20	34	317	368

Source: TCD HKP September 2002.

2.2 Pornography

Pornography, which is a moral crime in most societies, has started to attract millions of internet surfers from all over the world, including from the Asia-Pacific region. Table 2.3 below shows some statistics to highlight the seriousness of this problem.

Table 2.3. Increasing Pornography in Asia-Pacific

<i>Country</i>	<i>Number of Internet Users Flocking to Pornographic Sites During March 2002</i>	<i>Increase In % Over March 2001</i>
South Korea	10.7 million	72%
Taiwan, China	2.5 million	30-40%
Hong Kong, China	715,700	–
Singapore	373,100	–

Source: http://www.unescap.org/escap_work/ict/cybercrime.

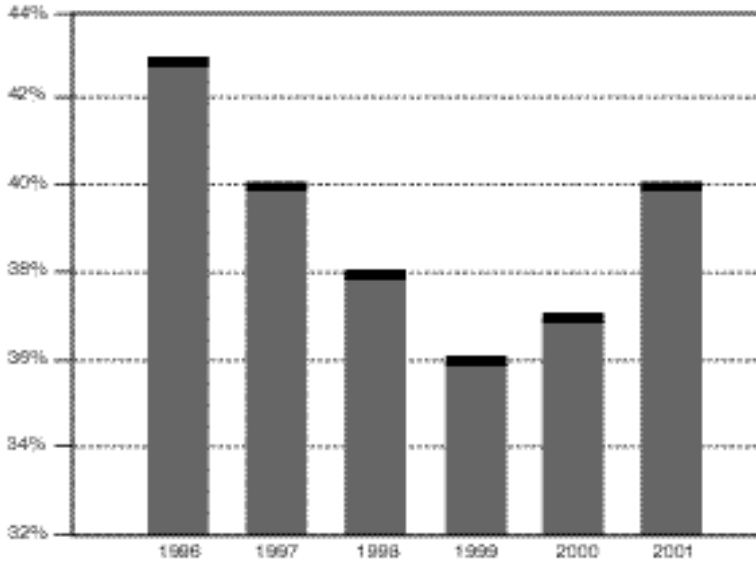
Internet brings great benefits, but also great risks to children. Among the worst forms of cybercrime is the global trade in child pornography. International criminal investigations have revealed several global networks exchanging child pornography. Several operations had been carried out to investigate the seriousness of the matter, among them are (Bryneson, 2002):

- Operation Wonderland, 1998: identified 100 suspects in 12 countries, more than 1 million images of child pornography discovered;
- Operation Avalanche, 2001: identified 250,000 subscribers, grossed more than \$5 million, and 100 arrests in the US alone.
- Operation Landmark, 2001: identified 11,000 users, 400 distributors, 130 search and arrest warrants issued in 19 countries.

2.3 Piracy

In early 2002, International Planning and Research Corporation (IPR) completed an analysis of software piracy for the year 2001 as part of an ongoing study for the Business Software Alliance (BSA) and its member companies. The purpose of the study is to review the available data and utilize a systematic methodology to determine worldwide business software piracy rates and the associated dollar losses. Software piracy is measured in this study as the amount of business application software installed in 2001 without a license (BSA Global Software, 2001).

The results from the annual BSA Global Piracy Study for 2001 indicate that software piracy continued to pose challenges for the software industry. For the first time in the study's history, the world piracy rate increased in two consecutive years, 2000 and 2001. The 2001 piracy rate of 40 percent is a marked increase from 37 percent in 2000. Both years were up from the low set in 1999 at 36 percent.



Source: BSA Global Piracy Study for 2001.

Figure 2.1. World Piracy Rate

Since the study began in 1994, there had been a steady decrease in the rate of software piracy. Unfortunately, this downward trend in piracy rates has not been evident in the past two years. In 2000, the level of piracy for developed countries increased, rather than continue the downward trend as expected. In 2001, the effects of a worldwide economic slowdown that hit technology spending particularly hard probably caused the increase in the piracy rate. The results of the study indicate that software piracy rose in response to the pressure of the curtailed spending of the economic downturn. This was the first period of a general global economic slowdown since the study began in 1994. The results suggested that the progress made against piracy in the 1990s was conditional. Compliance with software licensing is at risk of being considered an economic luxury that can be abandoned in difficult times.

2.3.1 Piracy in Asia-Pacific Region

Several large countries in Asia experienced increases in their piracy rates. Malaysia and India experienced rate increases of 70 percent for both countries in the above BSA Global Piracy Study for 2001. The Philippines' rate increased to 63 percent. Most other countries showed small changes in their piracy rates. Indonesia had an 88 percent piracy rate, down from 89 in 2000. Japan held steady with a 37 percent piracy rate. Australia had a 27 percent piracy rate, down from 33 in 2000. New Zealand, with a 26 percent piracy rate, continued as the country with the lowest piracy rate in the Asia-Pacific region. Vietnam, with a piracy rate at

94 percent, continued as the country with the highest piracy rate in the region. China, at 92 percent, followed as the country with the second highest piracy rate. As the chart in Figure 2.1 shows, the regions with the highest dollar losses in 2001 were Asia-Pacific, Western Europe, and North America.

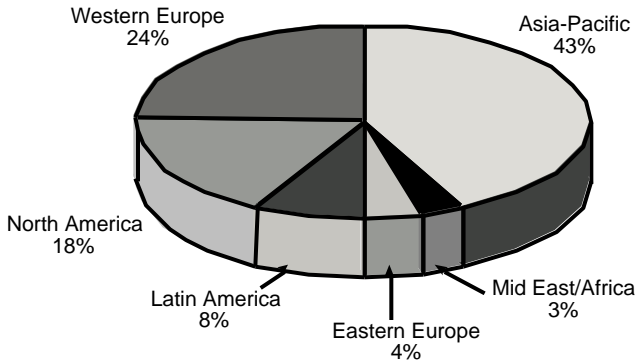


Figure 2.2. Dollar Losses by Region to Piracy in 2001

2.3.2 Piracy in other regions (2001)

Middle East

The three largest economies in the Middle East, Turkey, Israel, and Saudi Arabia, each saw a decrease in the piracy rate, with Turkey dropping the most, from 63 percent in 2000 to 58 percent in 2001. Israel, with a 40 percent piracy rate, was the country with the lowest piracy rate in the region. Lebanon, Qatar, and Bahrain had the three highest piracy rates in the region, at 79, 78, and 77 percent respectively.

Africa

Africa saw a small increase in the piracy rate, from 52 percent in 2000 to 53 percent in 2001. South Africa, the largest economy in the region, had the lowest piracy rate, at 38 percent. Kenya with 77 percent and Nigeria with 71 percent were the two countries in the region with the highest piracy rate.

As Figure 2.1 shows, the regions with the highest dollar losses in 2001 were Asia-Pacific, Western Europe, and North America. These regions have the largest economies and correspondingly, the largest PC and software markets. In Western Europe and North America, the relatively low piracy rates still translate into large dollar losses. The Asia-Pacific region, where the piracy rate is substantially higher than North America or Western Europe, made up 43 percent of the world losses due to piracy. In the US, the piracy rate declined to 25 percent in 2001, down

from 31 percent in 1994. This is the lowest rate of any country, but still represents a dollar loss of \$1.8 billion. Japan's 37 percent piracy rate resulted in the second largest dollar losses in 2001 at \$1.7 billion. China, which historically has had some of the highest piracy rates in the world and is still among the highest with 92 percent, has the third largest losses with just under \$1.7 billion. In Western Europe, Germany and France had the highest dollar losses with \$681 million and \$527 million, respectively. Italy was third with \$468 million in dollar losses.

2.4 Other Cases

Examples of regional cases that have been reported in the last few years in countries in the Asia-Pacific region are summarised in Table 2.3 below.

Table 2.3. Examples of regional cases reported

<i>Country</i>	<i>Cases</i>	<i>Year</i>
Singapore	Commercial Affairs Department (CAD) of the Singapore Police Force has received 32 complaints from consumers that their credit cards had been used to make fraudulent online purchases from local and foreign websites. Online transactions only make up 5 percent of total credit card transactions, but make up 50 percent of all credit card fraud, according to an Asian Wall Street Journal report.	2001
Japan	Police arrested five teenage girls, members of a virtual motorcycle gang formed via the internet, on suspicion of assaulting a member in June who tried to leave the group. The group called "Mad Wing Angels" was established in January by 30 girls across Japan who got acquainted with each other through the "i-mode" mobile phone internet access service of NTT DoCoMo Inc. Members include girls who do not have a motorcycle and the group has never held a gathering of all its members. However, some gang members plan to burn up the road in the future wearing the same gear. The members also set internal rules – such as "an eye for an eye" – and pledged to fight all-out battles with opponents. According to investigations, the girls were angered by the 16-year-old member's request to leave the group in order to study abroad and called her to a park in Tokyo's Minato Ward on the night of June 1. They allegedly beat her in the face and abdomen and pressed lit cigarettes onto both of her arms, inflicting injuries requiring three weeks of treatment.	August 2001

Table 2.3. (continued)

Country	Cases	Year
Thailand	A Ukrainian man, Maksym Vysochansky was arrested by Crime Suppression Division (CSD) police and US Secret Service agents. He was on the US Secret Service's most-wanted list as he is said to have pirated software and then sold copies on several channels on the World Wide Web. Head of the US Secret Service in Thailand said his operations had caused over \$1 billion in damage to the US software industry. A US court charged Vysochansky with criminal copyright infringement, trafficking in counterfeit goods, money laundering, conspiring to launder money, and possession of unauthorized access devices.	2003
	A man has been found guilty of posting defamatory messages on the internet in Thailand's first ruling on cyber-defamation. Thanet Songkran was given a two-year suspended sentence for posting a note on a web bulletin board, which listed the phone number of a young woman and a message alleging she was a student prostitute, <i>The Nation</i> newspaper said.	2002
	Thai university students arrested for hacking have been ordered to pay for their crime by serving at the very website they defaced. The hackers planted a bogus news flash on a government ministry's site, detailing plans to set up a new club to promote prostitution and pornography. The message was removed after a few hours and the intrusion traced to a local university. As punishment, these undergraduates were ordered to work on the ministry's website for a certain period.	2002
Korea	Korea's <i>Chosun Ilbo</i> newspaper reported that a 15-year-old student was the country's "Hacker Queen" after winning a contest organized by an internet security provider. Analysts noted that Choi Hae-ran's hacking skills were good enough to break into almost any company's homepage easily. Choi says that she learned about hacking by simply browsing various websites. She is now listed in an online Hall of Fame for Korean hackers, and her dream is to become "a hacker that catches hackers."	2001
Taiwan	The CIH virus (aka Chernobyl) infected 600,000 PCs worldwide in 1999, and on its trigger date of April 26 it wiped out entire hard drives on many machines. The damage was estimated at over \$100 million. It was concentrated in a few countries, especially South Korea, where about 250,000 computers were hit. The virus was written by an engineering student in Taiwan, Chen Ing Hau, supposedly as a challenge to anti-virus makers. Tracked down while serving in the army, Chen apologised and claimed that he never meant to cause any damage. In the end, no charges were filed because no Taiwanese citizen filed a complaint. Surprisingly, several software firms recruited Chen when he left the army, and he took a job with one called Wahoo. He appears to have escaped	1999

Table 2.3. *(continued)*

<i>Country</i>	<i>Cases</i>	<i>Year</i>
	punishment for his actions, although he should probably avoid visiting Korea.	
China	Prosecutors in China announced the country's first criminal case against a hacker in May 2001, signalling a tougher line on internet crime. Lu Chun, a 21-year-old sophomore in Beijing, allegedly used downloaded hacker Trojans to steal a company's internet account and password. He then gave out the information to schoolmates and friends, and sold it through the internet, resulting in over 1,000 people using the company's internet account fraudulently.	2001
Filipina	23-year-old Onel de Guzman was a student at AMA Computer College in Manila before he admitted to possibly releasing (but not to writing) the "Love Letter" virus in September 2000. "Love Letter" brought down hundreds of corporate networks and infected millions of PCs, becoming the most costly virus in history, with damages estimated at US\$8.7 billion. Guzman apparently dropped out of school after professors rejected his thesis proposal on methods for stealing computer passwords. Investigators concluded that he belonged to a hacker society, and other members also contributed to the "Love Letter" virus. However, prosecutors decided he didn't commit any crime under Philippine law. The Philippine Congress later enacted a law specifically covering computer crimes such as virus writing.	2000

3. EXISTING STRUCTURES AT REGIONAL/SUB-REGIONAL OR NATIONAL LEVEL

3.1 Introduction

Asia-Pacific is characterized by numerous diverse trends socially and politically. There are a number of poor countries in Asia-Pacific, as well as developing countries which aspire to join the rank of a few like Japan, Taiwan, and Singapore. Penetration of the internet is varied among the countries. The future holds tremendous promise for the Asia-Pacific region, but countries will have to respond quickly in order to combat the cybercrime that poses a serious threat to the region. A survey conducted by Computer Security Institute confirmed that threats from computer crime and information security breaches continue unabated in the region and that financial toll is mounting. The region needs coordinated and strict measures in the form of cyberlaws to combat these increasing crimes.

Cyberlaws in Asia-Pacific are beginning to take shape in response to incidents that have affected the region. Many countries have enacted cyberlaws: Australia, India, Japan, Malaysia, Philippines, Korea, Taiwan, Philippines, Singapore, and Pakistan. Numerous international and regional endeavours have been made which have laid the foundation for further evaluation of regulatory mechanisms for cybercrime.

Cyberlaw is a new phenomenon having emerged long after the invention of internet. Initially, the internet grew in a completely unplanned and unregulated manner. As such, it was open to all sorts of new criminal activity. Even the inventors of the internet could not foresee the scope and consequences of cyberspace. The growth rate of cyberspace has been enormous, roughly doubling every 100 days. Cyberspace is becoming the new preferred environment of the world, especially among the younger generation. With the phenomenal growth of cyberspace, new issues relating to various legal aspects began to emerge. In response, cyberlaws were created. There is no one definition of the term "cyberlaw." Anything concerned with, related to, or emanating from, any legal aspects or issues concerning any activity of netizens and others, in cyberspace, comes within the ambit of Cyberlaw (Duggal, 2002).

Addressing cybercrime starts with prevention, i.e. enhancement of information security and ensuring that the private sector and other users take a pro-active approach to information security. Thus, some frameworks based on combating cybercrime are discussed below.

3.2 Regional and International Cooperation Frameworks for Combating Cybercrime

There exist several cooperation frameworks for combating cybercrime at the regional and international levels. Among these cooperation frameworks are:

a) G8 24-Hour Network for High-Tech Crime

Justice and Interior Ministers from the G8 nations, Canada, France, Germany, Italy, Japan, Russia, UK and USA, met in Washington, DC, on 10 December 1997 under the chairmanship of the United States (Broadhurst, 2002) (G8, 2002). A common decision was reached to combat high-tech crime, recognizing the unprecedented ways the new computer and communications technologies were vulnerable. A 24-hours surveillance principle and a ten-point action plan to combat high-tech crime was put forward as follows:

Principles to Combat High-Tech Crime

- i. There must be no safe havens for those who abuse information technologies.
- ii. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
- iii. Law enforcement personnel must be trained and equipped to address high-tech crimes.
- iv. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
- v. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- vi. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- vii. Trans-border electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.
- viii. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
- ix. Information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
- x. Work in this area should be coordinated with the work of other relevant international forums to ensure against duplication of efforts.

Ten-Point Action Plan to combat High-Tech Crime

- i. Use our established networks of knowledgeable personnel to ensure a timely, effective response to trans-national high-tech cases and designate a point-of-contact who is available on a 24-hour basis.
- ii. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other states.
- iii. Review our legal systems to ensure they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
- iv. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
- v. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; trans-border searches; and computer searches of data where the location of that data is unknown.
- vi. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
- vii. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.
- viii. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax or e-mail, with written confirmation to follow where required.
- ix. Encourage internationally recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.
- x. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions. (<http://www.g8summit.gov.uk/brief0398/prebham.shtml>)

b) The Forum of Incident Response and Security Teams (FIRST)

FIRST was formed to address the continuous stream of security related incidents affecting millions of computer systems and networks throughout the world. FIRST was founded in 1990 in California, USA, to bring together a variety of computer security incident response teams from government, the commercial sector, and academic organizations to discuss how to improve the implementation or

institutionalization of ICT ethics. Thus, FIRST aims to foster cooperation and coordination in incident prevention, to promote prompt rapid reaction to incidents, and to promote information sharing among members and the community at large (FIRST, <http://www.first.org/about/first-description.html>).

The goals of FIRST are:

- To foster cooperation among information technology constituents in the effective prevention, detection, and recovery from computer security incidents;
- To provide a means for the communication of alert and advisory information on potential threats and emerging incident situations;
- To facilitate the actions and activities of the FIRST members including research, and operational activities; and
- To facilitate the sharing of security-related information, tools, and techniques.

FIRST provides a forum for facilitating trusted interactions among incident response and security teams. Assistance for interactions is available on either a team-to-team basis (through introduction to teams) or by using FIRST infrastructure to share information among all members in a secure way. The increased ability to communicate with peer entity teams allows for faster resolution of computer security incidents, regardless of their source, destination, or transit path. FIRST also hosts an annual Computer Security Incident Handling conference. This conference focuses on the issues of incident response and security teams, and brings together incident response and security professionals from around the world who share their experiences and expertise. The presentations are international in scope and include the latest in incident response and prevention, vulnerability analysis, and computer security.

c) Asia-Pacific Networking Group

The Asia-Pacific Networking Group (APNG) is the oldest Asia-Pacific Internet organization dedicated to the advancement of networking infrastructure in the region, and to the research and development of all associated enabling technologies. Its mission is to promote the internet and the coordination of network interconnectivity in the Asia-Pacific region. From APNG emerged the Asia-Pacific Policy and Legal Forum (APPLe), in 1996, focusing on internet governance, legal and policy issues. In 1998, APNG helped form the Asia-Pacific Security and Incident Response Coordination Working Group (APSIRC), which focuses on the design of network security. APNG set up APSIRC in order to catalyze the formation of national Computer Emergency and Response Teams (or commonly known as CERTs) and increase awareness among internet practitioners and network managers of its ethical procedures to combat cybercrime.

d) Computer Emergency Response Team and Coordination Centre (CERTCC-KR)

The Korea Computer Emergency Response Team and Coordination Centre (CERTCC-KR) is the first incident response organization in Asia, except for Australia. CERTCC was originally established in the United States to solve problems regarding computer incidents such as internet hacking.

As the Korea Information Security Agency's (KISA) incident response team, CERTCC-KR supports counter-measuring activities involving networks in Korea. It also plays a key role in the creation of unified cooperative systems among network operating institutions. CERTCC-KR joined the Forum of Incident Response and Security Teams (FIRST, the international institution comprising of national representative CERTs in North America, Europe and Asia-Pacific) in 1998 as an official member in order to actively countermove against global incidents requiring international cooperation. And CERTCC-KR also participated in the Asia and Pacific Networking Group (APNG) to create an aggressive security-work group named the Asia-Pacific Security Incident Response Coordination (APSIRC).

Moreover, CERTCC-KR acts as the secretariat of CONSortium of CERTs (CONCERT) established in 1996 to jointly counteract domestic incidents in order to boost information security technologies of domestic institutions, respond to incidents, and share information for the prevention of incidents.

The main objective of CERTCC-KR is to protect the information on the domestic network infrastructure in an ethical manner. Its goals are as follows:

- Prevent incidents in information networks;
- Cooperate to receive incident reports and correspond to incidents;
- Analyse the damaged system and support technologies;
- Restore damages, and analyse and trace the attackers;
- Hold public education seminars related to incident prevention;
- Publish and distribute various types of technological documents to prevent hackings and viruses; and
- Develop technologies to prevent incidents.

e) Asia-Pacific Computer Emergency Response Task Force (APCERTF)

Asia-Pacific Computer Emergency Response Task Force (APCERTF) was proposed by AusCERT and formed with the following memberships (Yamaguchi, 2002):

- Australian Computer Emergency Response Team (AusCERT)
- Bach Khoa Internetwork Security Centre (BKIS)
- CERNET Computer Emergency Response Team (CCERT)

- Computer Emergency Response Team Coordination Centre-Korea (CERTCC-KR)
- China Computer Emergency Response Team Coordination Centre (CNCERT)
- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT/CC)
- Indonesia Computer Emergency Response Team (IDCERT)
- Information Security Centre – Korea Advanced Institute of Science and Technology (ISC/KAIST/KCERT)
- Information-technology Promotion Agency/IT Security Centre (IPA/ISEC)
- Japan Computer Emergency Response Team/Coordination Centre (JPCERT/CC)
- Malaysian Computer Emergency Response Team (MYCERT)
- Singapore Computer Emergency Response Team (SingCERT)
- Taiwan Computer Emergency Response Team/Coordination Centre (TWCERT)
- Taiwan Computer Incident Response Coordination Centre (TW-CIRC)
- Thai Computer Emergency Response Team (ThaiCERT).

The mission of APCERTF is to maintain a trusted contact network of computer security experts in the Asia-Pacific region in order to:

- Enhance regional and international cooperation on information security;
- Develop measures to deal with large-scale or regional network security incidents;
- Facilitate information sharing and technology exchange;
- Promote collaborative research and development; and
- Address legal issues related to information security and emergency response across regional boundaries.

f) The Yokohama Global Commitment 2001

The “Yokohama Global Commitment 2001,” was held in Yokohama, Japan on 17-20 December 2001. Representatives from governments, intergovernmental organizations, non-governmental organizations, the private sector, and members of civil society from around the world, focused on strengthening the commitment to protect children against commercial sexual exploitation and sexual abuse, in the physical realm or cyberspace. This was a follow up of the First World Congress against Commercial Sexual Exploitation of Children held in Stockholm, Sweden in 1996. The Yokohama Global Commitment reaffirmed the protection and promotion of the interests and rights of the child to be protected from all forms of sexual exploitation. It calls for more effective implementation of the Convention on the Rights of the Child by States party to the convention in order to create an

environment where children are able to enjoy their rights. It also calls for the development of international and regional standards to protect children from sexual exploitation through new instruments, including the following: Supplementing the United Nations Convention against Trans-national Organized Crime, and the Convention on Cybercrime (<http://www.unicef.org/events/yokohama/outcome.html>).

g) Asia-Pacific Cyberlaw Forum (APCF)

The Asia-Pacific Cyberlaw Forum (APCF) is committed to the cause of developing strong, logical and vibrant cyberlaws in the different countries of Asia-Pacific. It is of the opinion that Asia-Pacific as a region seems to be far behind in the field of enacting cyberlaws for regulating activities of netizens in cyber space. Barring a handful of countries in Asia-Pacific, most of the countries in this region have low Internet penetration and consequently, have not felt the need to legislate cyberlaws. However, given the way internet is rapidly growing, it will only be a matter of time before all the countries in Asia-Pacific need to enact and adopt cyberlaws. The Asia-Pacific Cyberlaw Forum (APCF) aims to become the focal point for giving appropriate input to all governments of Asia-Pacific in the field of drafting, enacting and adopting cyberlaws.

APCF is committed to the fact that Asia-Pacific nations should not reinvent the wheel. Asia-Pacific nations should learn from the previous wisdom and practical experiences of other nations in the world who have enacted and implemented cyberlaws. APCF aims to become a rallying point for research, brainstorming, information and all kinds of matters concerning cyberlaw in Asia and the Pacific. APCF will coordinate cyberlaw Asia, being Asia's premier membership-based cyberlaw body, in raising awareness about different facets of cyberlaw. (<http://www.cyberlaws.net/asiapac.htm>).

Other initiatives for combating cybercrime are summarised in Table 3.1 below.

Table 3.1. Example of Initiatives in Combating Cybercrime

<p>APEC LOS CABOS DECLARATION, 26-27 OCT 2002</p>	<ul style="list-style-type: none"> • Identify national cybercrime units and international high-technology assistance points of contact and create such capabilities by October 2003. • Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Terms) by October 2003. • Calls for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime.
---	---

Table 3.1. (continued)

APEC e-SECURITY TASK GROUP	<ul style="list-style-type: none"> • CERT Capacity Building • UNGA 55/63 Report to Ministers/Shanghai Declaration • IT security training material • Compendium of IT Security Standards • IT security skills recognition • Encryption policies • Electronic authentication
APEC Cybersecurity strategy	<p>Action Items</p> <p>Legal developments</p> <ul style="list-style-type: none"> • Adopt comprehensive substantive, procedural and mutual assistance laws and policies • APEC to facilitate development of laws and policies • Report status to TEL Ministers <p>Information sharing and cooperation</p> <ul style="list-style-type: none"> • Assist in development of information sharing institutions • Assist in development of 24/7 units <p>Security and technical guidelines</p> <ul style="list-style-type: none"> • Identify standards and best practice • Encryption and authentication legal and policy issues • Security business case for corporations <p>Public awareness</p> <ul style="list-style-type: none"> • Material development, such as OECD Guidelines • Website to provide cyber ethics and cyber-responsibility material <p>Training and education</p> <ul style="list-style-type: none"> • Identify and organize training opportunities • Promote training of technology security professionals and distribution of materials • Website of training opportunities wireless security • Examine issues (Steve Orłowski, 2002).
ASEAN COMMUNIQUE: Joint Communique of the Third Asean Municipal Meeting on Transnational Crime, October 2001	<ul style="list-style-type: none"> • Recognize the growing need for the region to deal with many more forms of transnational crime, including cybercrime. • Expressed concern with the newly emerging trends of transnational crime, such as cybercrime.
E-ASEAN CYBER SECURITY PLEDGE	<ul style="list-style-type: none"> • The E-Asean Task Force Group of Nations signed the E-Asean cyber Security Pledge in September 2002 as a reiteration of the commitment of its members against the terrorism. • This pledge was adopted and signed in the aftermath of the scenario that emerged after the 11th September attacks.

3.4 ICT Policies of Selected Countries in the Asia-Pacific

Findings from a few countries in the region are presented below, based on the availability of information concerning ICT policies and frameworks that have been initiated, in order to provide insight on the efforts committed so far. Most of the information is taken from Asia-Pacific Conference on Cybercrime and Information Security held in Seoul, Republic of Korea, 11-13 November 2002, organized by United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP). The papers presented at the conference give us some insight to the efforts and initiatives undertaken by individual countries.

3.4.1 Singapore

Singapore was an early and fervent adopter of ICT. Now, with one of the highest penetration rates of ICT usage among nations, Singapore finds itself having a large stake in the well-being and safety of cyberspace. Legislation has been enacted to protect the users of cyberspace. A combination of legislation by the Government, self-regulation by the industry and continuous education of consumers is Singapore's approach to the challenges posed by this new age (Chan, 2002).

Many initiatives taken in tackling cyber security issues aimed at improving confidence in the local electronic commerce scene and hence promoting the use of e-commerce. Other initiatives are aimed at enlarging the pool of quality ICT security expertise in Singapore that is able to feed corporate demands and sustain local research and development efforts. Consortia are formed by industry and supported by the Government to provide the focus for self-regulation and platforms for reflective discussions between industry players and the Government. Along with the institutions set up to acquaint citizens with the benefits of cyberspace, campaigns are conducted to inculcate safe habits online.

Public Awareness and Professional Competency

The Infocomm Development Authority (IDA) of Singapore envisages an infocomm-savvy Singaporean society and has initiated several initiatives in this direction. In particular, IDA implemented the e-Lifestyle & Marketing Programme (ELM), a 3-year programme to demystify infocomm technology and enable Singaporeans to use infocomm technology to enhance their quality of life and standard of living in the information society in more ethical manner.

On the infocomm security front, IDA initiated, in November 2001, a yearlong public awareness campaign aiming at the public and private sectors as well as the general public to inculcate safe computing practices. The Singapore Computer Emergency Response Team (SingCERT) regularly conducts workshops, seminars and courses on more technical topics of ethics.

The National Infocomm Competency Centre (NICC) is an industry-led, government-supported, organization that aims to provide assistance to individuals and organizations to enable them to maintain a high level of infocomm technology competency.

ICT Security Developers in Singapore

The Government supports local companies offering infocomm security consultancy, services and products. Some samplings of the security framework developers in Singapore that encourages ethical manner of ICT:

- CE-InfoSys (www.ce-infosys.com)
- D'Crypt (www.d-crypt.com)
- DigiSAFE (www.digisafe.com.sg)
- PrivyLink (www.privilink.com.sg)
- Transparency (www.transparency.com.sg)

Cyber-crime Investigation Capabilities

The Criminal Investigation Department (CID) is the premier investigation agency in Singapore vested with the staff authority for all criminal investigation matters within the Singapore Police Force (SPF). Apart from investigating all major and specialized crime cases, CID houses a Technology Crime Division (TCD). As the authority on technology crimes, TCD is the investigation specialists, forensic specialists as well as builders of technology crime capability for the entire police force. Its scope of operation goes beyond computer crime and includes traditional crimes committed with the use of technology such as encrypted mobile devices, Internet and even the wireless platform. In order to ensure that the nation is ready for such crimes of the future, the approach adopted by TCD was also to build capabilities through research, alliance building and education.

Institutions

The local universities are tapped to provide the research capabilities, allowing researchers to gain more field exposure in the process. For example, the Singapore Police Force and the Nanyang Technological University are collaborating to tackle the increasingly prominent role of technology in crimes, particularly in the area of forensics.

Public Incident Response Capabilities

SingCERT is established to facilitate the detection, resolution and prevention of security-related incidents on the Internet. SingCERT also issues advisories and alerts when incidents or events occur. SingCERT maintains a website and a hotline to facilitate the reporting and dissemination of advisories.

SingCERT is also a founding member of the Asia-Pacific Security Incident Response Coordination Working Group (APSIRC-WG). The APSIRC-WG is staffed by volunteers from the national Incident Response Teams (IRTs) from Japan, Korea and Singapore and aims to promote collaborations with other international IRTs and security groupings such as the Forum of Incident Response and Security Teams (FIRST). Furthermore, APSIRC-WG provides assistance when regional countries would like to establish their own IRTs.

SingCERT is working with the Japan Computer Emergency Response Team (JPCERT/CC) and the Australian Computer Emergency Response Team (AusCERT) on future activities for the APSIRC-WG.

Cyberlaw

Electronic Transactions Act

In Singapore, the Electronic Transactions Act (ETA) establishes the supporting legal infrastructure for the PKI. It was enacted in 1998 to provide a legal infrastructure for electronic signatures and electronic records, and to give predictability and certainty to electronic contracts. It is modelled after the Illinois Electronic Commerce Security Act and the UNCITRAL Model Law on Electronic Commerce, which sets the framework for electronic commerce laws in many countries.

The ETA addresses the following issues:

- Commercial code for electronic commerce transactions: This creates a predictable legal environment for electronic commerce and deals with the legal aspects of electronic contracts, use of electronic signatures and electronic records and authentication and non-repudiation concerns. It is noteworthy that electronic signatures have the same legal binding effect as that of written signatures.
- Use of electronic applications and licences for the public sector: This allows government departments to accept electronic applications and to issue electronic licences and permits without amending their respective Acts.
- Liability of service providers: This exempts network service providers from criminal or civil liability for content that they merely provide access to.
- Provision for a PKI: This provides for the appointment of a Controller of Certification Authorities (CCA) to enable regulations to be made for the licensing of Certification Authorities (CA). The Infocomm Development Authority (IDA) is currently appointed the CCA of Singapore. The Act provides for certain minimum standards for all certification authorities, whether or not they are licensed, as well as higher standards for licensed authorities.

Electronic Transactions (Certification Authority) Regulations

In 1999, the Electronic Transactions (CA) Regulations were made to establish a voluntary licensing scheme for CAs. Public CAs are strongly encouraged to obtain licenses.

Computer Misuse Act

The Computer Misuse Act (CMA) was first enacted in 1993 and amended in 1998. It is aimed at protecting computers, computer programmes and information stored in computers from unauthorized access, modification, use or interception. The CMA also applies to any person, irrespective of his physical location, who hacks into computers located in Singapore. It also applies to any person in Singapore who hacks into computers outside Singapore.

The 1998 amendments ensure that newer forms of cybercrime (such as Trojan horses, password trafficking or denial of service attacks) are addressed. It also provides enhanced penalties for computer crime proportionate to the potential and actual harm caused. The amendment also gives the police powers to gain lawful access to computer material including the decryption of materials that are encrypted.

Evidence Act

The Evidence Act was amended in 1996 to permit the use of electronic records as evidence in courts. The provisions are modern and adapted to the network and Internet environment. The Act also allows the use of litigation support systems and the use of video-conferencing in Singapore courts.

3.4.2 China

China has made national initiatives in devising policy and framework to manage the onslaught of ICT activities at the national, provincial, and regional levels. Among the initiatives taken by the government are (PRC, 2002):

- i. Institutional framework of public information network security supervisory
 - Public Information Network Security Supervisory Bureau of Ministry of Public Security;
 - Provincial Public Information Network Security Supervisory Department;
 - Regional Public Information Network Security Supervisory Department.
- ii. Fundamental policy
 - Ensuring Preventive Measures:
 - Protect important computer systems

Strengthen education and propaganda for the prevention of computer crime

Deter computer crime before it occurs

- Attack cybercrime as a means of prevention
- iii. Cooperation with other organizations
- Educational institutes
 - Computer technology companies
 - Internet Services Providers (ISP)
 - Other countries in the region
- iv. Modernize network police group
- Periodical education:
 - To refresh knowledge;
 - To keep up with the current situation;
 - To master new technology.
 - Temporary education:
 - To cope with emergence of incidents, such as an outburst of a virus.
- v. Legislation
- Regulation of Security and Protection of Computer Information systems of the People's Republic of China (1994)
 - Management Regulation of Security and Protection of Computer Information Networks Connected with INTERNET (1997)
 - Criminal Law of the People's Republic of China (1994)

3.4.3 Korea

As most social activities heavily rely on the information and communication infrastructure, Korean societies are very exposed to cybercrimes such as cracking, virus incidents, obscenity, violent images, infringement of copyright and violations of human rights (Cha, Y. 2002).

Cyber threats include hacking, viruses, spam mail, logic bombs, manipulation of insiders, leaks of personal information, etc., as indicated in the table below:

Table 3.2. Cyber Threats

<i>Crime</i>	<i>Incidents</i>	<i>Rate (%)</i>
Leaks of personal information and invasion of privacy	870	43.5
Spam mail	659	33.0
Virus and cracking	219	11.0
Obscene and violent images	181	9.1
Alienation and digital divide	50	2.5
Infringement of copyright and illegal copy of S/W	15	0.8
Others	6	0.3
Totals	2 000	100.0

Source: KISA (Korea Information Security Agency), 2001.

Korea has adopted initiatives in the formation of the Information Security Policy and Strategies which encompass the following matters:

- Information Infrastructure Protection
- Anti-Hacking and Virus activities
- Promotion of a Culture of Security
- Distribution of Electronic Signatures
- Privacy Protection and Ethical cyberspace
- Technology and Industry

A summary of initiatives that have been carried out in Korea is given under the headings as follows:

- Information Security System at the national level
 - ◆ Governmental system for information security to establish the information security system at the national level.
 - Government established Committee on Protection of Information Infrastructure (with the Prime Minister as the Chairman) including Ministers of Finance and Economy, Justice, National Defence, Information and Communication according to Regulation on Protection of Information and Communication Infrastructure enacted in January 2001.
 - Government established (April, 1996) KISA (Korea Information Security Agency), to provide for the safe use of information and communication technology at the private level. The agency establishes policy, systems and techniques of information security.
 - Government established ICEC (Information Communication Ethics Committee) to control the circulation of harmful information and to keep cyber environments safe and sound.

- ◆ Cooperation with private sectors
 - Government closely cooperates with private CERT and ISAC in various fields, such as the communications and financial fields, and information security companies to cope with cybercrime.
 - Government is supporting self-regulation of civic and business organizations that can complement governmental regulations coping with the rapid spread of illegal and harmful information.
- Advancement of security through a campaign to enhance a “culture of security consciousness”
 - ◆ Private sectors formed the Information Security Implementation Council to enhance information security (July, 2002).
 - ◆ Government is acting to impress individuals, businesses and government agencies with the importance of information security, through a campaign to enhance the culture of security.
 - ◆ Information ethics programmes including support of lecturers and programmes, been run targeting adolescences, adult and teachers to improve information utilizing capability and cultivate information ethics.
- Policies for Information Security Technologies
 - ◆ Technology and Manpower Development
 - Considerable investment shall be made in the technology of information security. For example, 279 billion Korean Won (Including 84.5 billion Korean Won from private sectors) needs to be invested over the next 5 years from 2003 to 2007.
 - Collaborative study shall be promoted among three sectors: academic, business and research institutes, to contribute to the development of the information security industry.
 - Support for international standardization of international organizations.
 - Encourage colleges and universities (including graduate schools) to open more new courses relating to information security, and support the nurturing of human resources for information security by offering more specialized education and training.
 - Certificate for information security experts and internet security experts shall be established and upgraded to be a national examination to promote manpower supply in the information security field.
- Consolidation of reliability in e-Commerce through wide use of electronic signatures
 - ◆ Digital Signature Act was enacted in February 1999 to provide a legal basis for safe use of electronic signature and authentication services.

- ◆ As of October 2002, 6 certification authorities are providing certification service.
 - ◆ The use of electronic signature in various transaction fields, such as internet banking, e-procurement and cyber stock market, is increasing. The number of electronic signature users increased to 4.24 million in September 2002, up from 50 thousand in the fourth quarter of 2000.
 - ◆ To secure the reliability in e-commerce between nations, offices concerned are proactively participating in the Asia PKI forum addressing international interoperability, and have been proceeding with an Electronic Signature Interoperability Pilot Project together with Japan and Singapore since June 2001.
- Nationwide forecasting/warning system of electronic infringement
 - ◆ Ministry of Information and Communication, major vaccine companies and KISA has deployed a real-time forecasting/warning system for cracking and virus incidents.
 - ◆ CERT is organized to operate the system for coping with electronic infringements in each field, while ISAC is teamed up for that in public sectors, such as finances and communications.
 - Monitoring and Reporting of Personal Data Infringements and Harmful Information
 - ◆ Reports and consultations regarding personal data infringements and illegal spam mails
 - Personal Data Protection Centre has been established to receive reports of personal data infringements and to provide consulting services for victims.
 - Spam Mail Complaint Centre (www.spamcop.or.kr, opened in July, 2002) has been operating as an organization exclusively charged with spam mail reports and counseling services. This organization helps victims of spam mail and teaches how to block unsolicited spam mails.

3.4.4 Mongolia

The Mongolian Government has established the followings approaches to combat cybercrime and provide for information security at the national level in the following areas (Mongolia, 2002):

Prevention of cybercrime

The Mongolian Government has declared that one of its priorities is the development of information and communication technology. But, combating

cybercrime and enhancing information security has not been mentioned. So, there is no master plan/policy or strategy on how to combat cybercrime. Of course, user awareness is very poor in the country because no systematic information is given on these issues. Local companies, such as DataCom, InfoCon, BodiCom, InterActive, are developing quite good security systems on their financial programmes, and also on their local area networks. However, there is no active, special information security agency operating on these issues in broadband. Regarding human resources, there are no employees being prepared on information security issues. Unfortunately, there is no special agency that can utilize engineers effectively to fight against cybercrime.

Monitoring, detection and investigation

Currently, there is no record of what Mongolia has done regarding cooperation with other states on law enforcement for cybercrime. Also, cooperation between internet service providers and law-enforcement officials has been very weak in the country. Law enforcement has granted the internet service providers a license for their operation; this is the only preventive measure. There are no national law-enforcement focal points for cybercrime.

Legal systems that permit the preservation of and quick access to electronic data pertaining to particular criminal investigations is well established in the Mongolian code of criminal procedures. Although many things regarding information security are covered by Mongolian criminal procedures, there are no skilled specialists who can monitor, detect and investigate information security and cybercrime issues.

Effective prosecution

In order to stop or reduce the misuse of information technology, it has been suggested that Mongolia establish a work group to make a master plan on Information Security. The first step for this measure is to encourage the Information Security law work group to continue its work on that issue. The following have been included in the plan:

- a) To develop a project to train information security/cybercrime specialists, and establish a separate police department to fight cybercrime;
- b) To publish guide books on these issues in Mongolian language;
- c) To establish a mechanism for effective exchange of information on security issues between countries in the future;
- d) To establish a permanent agency inside Mongolian government structure;

- e) To attract foreign partners and support on this issue;
- f) To develop a plan to support private sector and NGO activities on information security issues; and
- g) To learn and introduce methodologies of cybercrime fighting in Mongolia from the experiences of other countries, such as Korea.

3.4.5 Philippines

During the incidence of the “Love Bug Virus,” the Philippines had no law specifically governing computer crimes; the applicable laws used in that instance were RA 8484 (Access Device Regulation Act) and the Article 327 of the Revised penal Code (Malicious Mischief). The Access Device Act law was designed to penalized credit card fraud. The “Love Bug” incident put pressure on the Philippines Congress to pass a Bill regulating the use of computers and penalizing hacking, launching of viruses and other cybercrimes (Borje, 2002).

E-Commerce Regulation

The Electronic Commerce Act of 2000 (RA 8792) was imposed to penalize the following:

- a) Hacking or cracking, referring to unauthorized access into or interference in a computer system/server or information system, or any access in order to corrupt, alter, steal or destroy, introduce computer virus and/or loss of electronic data documents; and
- b) Piracy, or the unauthorized copying, reproduction, dissemination, removal, distribution, importation, use, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting, of protected materials, electronic signatures or copyrighted works, including legally protected sound recordings, phonograms and information material on protected works, in a manner that infringes on intellectual property rights.

The penalty regarding the above acts is a fine of a minimum of P100,000 fine and a maximum as commensurate to the damage incurred, and from 6 months to 3 years imprisonment.

As a framework for combating cybercrime, the Philippines government has established a council known as Information Technology and E-Commerce Council (ITEC). To achieve their aims, the following goals were marked as points of concern:

- Information Infrastructure Development
- Human Resource Development
- Business Development
- E-Government Implementation
- Create enabling Legal and Regulatory environment.

The government agencies that are involved in the framework and their responsibilities are listed below:

- National Bureau of Investigation (Anti-Fraud and Computer Crimes Division): Investigation of all computer-related crimes and other offences which make use of advances in technology;
- Intellectual Property Office: Handles intellectual property rights violations;
- National Telecommunications Commission: Supervizes and regulates the telecom and broadcast industry; and
- Department of Trade and Industry: Implements E-Commerce Act and Handles consumer complaints.

3.4.6 Thailand

In December 1998, the Thai Cabinet approved the Information Technology Laws Development Project, as proposed by the Ministry of Science Technology and Environment. The project has a mandate to research and develop six IT laws that will serve as an infrastructure for electronic commerce, and to enhance confidence among the members of the electronic transactions playground by providing rules and regulations (Kaewjumngong, 2002).

The above-mentioned ICT laws are as follows:

- a) Electronic Transactions Law: To recognize the legal effect of data messages by treating them as the functional equivalent of written messages, or evidence in writing, with a view to promote electronic transaction reliability.
- b) Electronic Signatures Law: To enable reliability of the use of electronic signatures.
- c) Electronic Fund Transfers Law: To facilitate the electronic transfer of funds.
- d) Computer Crime Law: To criminalize the new type of offences made possible by the borderless virtual world.
- e) Data Protection Law: To protect right of privacy in the information society.
- f) National Information Infrastructure Law (NII): To provide equitable and thorough information infrastructure and enable universal access by promoting more equitable and affordable rights and opportunities to access information and communication services. The purpose of NII Law focuses on reducing Thailand's digital divide.

Computer Crime Law

Thailand's computer crime law was drafted according to the framework of the Cybercrime Convention Council of Europe since a common purpose of the convention is to harmonize national laws. Apart from the Criminal Procedural Code which provides for the power and duty of administrative of police officers to collect

or obtain evidence in a criminal case, the Computer Crime Law also stipulates some powers, as following:

Search and seizure without warrant

Permitted where there is a reasonable grounds to believe that an offence prescribed under the Bill has been committed, and if left delayed until a search warrant is issued, the article whether being tangible or not or the evidence related to such offence may be removed, hidden, destroyed or altered from its original state, the competent authority shall have the power to enter at any time into a dwelling place or a place where there is a reasonable grounds to suspect that property, or the evidence connected with commission of an offence, is hidden or kept therein, for the purpose of accessing and investigating a computer system or any other article with reasonable grounds to believe that it is involved in the commission of an offence. Seizing, attaching, making a copy of or performing any other act on the said computer system or computer data, to use as evidence in connection with the commission of such offence, is also allowed.

Powers to demand traffic data and others

For the purpose of seeking facts and the collection of evidence, the competent authority shall have the power to demand computer traffic data from a service provider involving communications on a computer system, or other involved persons. In case the computer data has been encrypted, the authorities can order a person concerned with such computer data to decrypt it.

In April 2001, Thai Computer Emergency Response Team (ThaiCERT) was established as an electronic discussion forum on cyber security to encourage people to be aware of the security problem. Its members include government agencies, as well as companies in the private sector that are more conscious about cyber security.

3.4.7 Vietnam

With respect to laws concerning internet activities, it was reported that up to 2002 Vietnam had no laws concerning computer crimes and ICT intellectual properties rights. As far as cryptography is concerned, it is used only by organizations of the Communist Party and the Government.

Information security and cybercrime are under the jurisdiction of state bodies. The Ministry of Public Security is in charge of information security and cybercrime, the Ministry of Culture and Information regulates and censors content of information before they are placed on the internet, and the Ministry of Post and

Telecommunications is in charge of licensing and regulating internet services. Vietnam plans to establish cyberlaws like other countries in the region.

3.4.8 Malaysia

Malaysia government has come up with lots of security measures to inculcate the ethical culture to all ICT users with the concerted cooperation of the private sectors. Below are some underline laws and policies Malaysia has adopted to prevent malicious act.

Cyberlaws

The development of IT and multimedia, without parallel development of laws, can result in abuses and, in turn, discourage the use of such technologies. Being aware of these issues, the Malaysian Government has already approved and passed its own set of cyberlaws:

- Digital Signature Act 1997
- Computer Crimes Act 1997
- Telemedicine Act 1997
- Communications and Multimedia Act 1998

Communications and Multimedia Act 1998 (CMA)

To ensure information security and network reliability and integrity, under the CMA, the Commission is entrusted to ensure information security and the reliability and integrity of the network. Legal issues relating to network security are addressed in the Communications and Multimedia Act and the Computer Crimes Act 1998. Thus, the CMA provides for a restructuring of the converged ICT industry. It creates a new system of licenses and defines the roles and responsibilities of those providing communication and multimedia services. Though intended to allow the converged ICT industry to be self-regulating, the Act also provides for the existence of the Communication and Multimedia Commission (the roles and powers of which are more clearly defined by the Communications and Multimedia Commission Act 1998) as a new regulatory authority to oversee the converged ICT industry. The Communications and Multimedia Act was brought into force on 1st April 1999. (http://www.cmc.gov.my/akta588/eng/legis_cma1998_pg3.htm).

Malaysian Communications and Multimedia Commission (MCMC)

MCMC is a statutory body established under the Malaysian Communications and Multimedia Commission Act 1998 to regulate and nurture the communications and multimedia industry in Malaysia in accordance with the national policy objectives set out in the Communications and Multimedia Act 1998 (CMA). Apart from regulating and nurturing the communication and Multimedia industry in accordance

with the CMA, the MCMC is also the “Controller” for the Certification Authorities under the Digital Signature Act 1998.

The MCMC is also charged with overseeing the new regulatory framework for the converging industries of telecommunications, broadcast and online activities. The 10th National Policy Objective, as stated in the CMA, requires the Commission to ensure information security and the integrity and reliability of the network for the country.

Police

The police have “sweeping” enforcement powers. They have jurisdiction over the CMA and also the CCA. All complaints relating to network security matters will be passed to either the MCMC and/or to the police.

Computer Crimes Act 1997 (CCA)

As computers become more central to people’s lives and work, they become both targets and tools of crime. This Act serves to ensure that misuse of computers is an offence. Under the Computer Crimes Act 1997, acts such as unauthorized access to computer material with intent to commit or facilitate the commission of a further offence, unauthorized modification of contents of any computer and/or wrongful communications, abetment and presumption are addressed. Thus, legal issues identified, such as fraudulent use of a network, improper use of network facilities/services and interception of communications, are described in the CMA. The Computer Crimes Act was brought into force on 1 June 2000 (<http://www.mycert.mimos.my/crime.html>).

Digital Signature Act 1997

Transactions conducted via the internet are increasing. As identities in cyberspace can be falsified and messages tampered with, there is a need for transacting parties to ascertain each other’s identity and the integrity of the messages, thereby removing doubt and the possibility of fraud/unethical manners when conducting transactions online.

The Act mainly provides for the licensing and regulation of Certification Authorities (CA). CAs issue Digital Signatures and will certify the identity (within certain limits) of a signor by issuing a certificate. The Act also makes a digital signature as legally valid and enforceable as a traditional signature. The Digital Signature Act was brought into force on 1 October 1998 (<http://www.cca.gov.my/legislat.htm>).

The Copy Right Act 1997

Copyright serves to protect the expression of thoughts and ideas from unauthorized copying and/or alteration. With the convergence of Information and Communication

Technologies (ICT), creative expression is now being captured and communicated in new forms (example: multimedia products, broadcast of movies over the Internet and cable TV). These new forms need protection. The Copyright (Amendment) Act amends the Copyright Act 1987 to extend copyright law to the new and converged multimedia environment. The transmission of copyright works over the internet now clearly amounts to infringement. Technological methods of ensuring works and authorship info are not altered or removed is also protected to ensure an ethical manner. The Copyright (Amendment) Act 1997 was brought into force on 1 April 1999 (<http://www.mycert.mimos.my/copyright.html>).

The Telemedicine Act 1997

Healthcare systems and providers around the world are becoming interconnected. People and local healthcare providers can gain access to quality healthcare advice and consultation from specialists from around the world, independent of geographical location. The Act serves to regulate the practice of tele-consultations in the medical profession. The Act provides that any registered doctor may practise “telemedicine,” but other healthcare providers (such as a medical assistant, nurse or midwife) must first obtain a license to do so. Patient’s consent and regulations must be handled in an ethical manner (<http://www.mycert.mimos.my/telemeng.html>).

Malaysian Administrative Modernization and Management Planning Unit (MAMPU)

Security issues in the public sector is administered by MAMPU (Malaysian Administrative Modernization and Management Planning Unit). Within MAMPU is the ICT Security Division. They operate a CERT for the Government. They recently launched The Malaysian Public sector Management of Information and Communications Technology Security Handbook (myMIS). The handbook is a set of guidelines concerning compliance and adherence to best practices and measures leading to information and network security. (<http://www.mampu.gov.my/ICT/MyMIS/MyMIS.htm>)

The National IT Council (NITC) and National ICT Security and Emergency Response Centre (NISER)

The National Information Technology Council of Malaysia (NITC Malaysia) functions as the primary advisor and consultant to the Government on matters pertaining to IT in Malaysia’s national development. Its main objectives are to:

- Promote the sustainable growth of IT development and application via R&D planning and technology acquisition strategies;
- Ensure the smooth integration of new technologies into social and economic development;

- Determine the likely impact of IT on the economy and society; and
- Explain and promote the potential of IT in transforming societies in its entire dimension (http://www.nitc.org.my/nitc_objectives.shtml).

NITC gave birth to the National ICT Security and Emergency Response Centre (NISER) to address e-security issues of the nation and as to act as Malaysia's CERT (MyCERT). They offer their services in research in vulnerability detection, intrusion detection and forensic technology. Presently, they offer their services to both public and private sectors (Abas, 2001).

3.4.9 Afghanistan

The goal for Afghanistan is to build a high-quality, low-cost ICT network, in order to give all Afghans access to the employment, educational, business, health care and entertainment opportunities of the digital age. The government, in consultation with all stakeholders, developed a national ICT strategy that will ensure an appropriate balance between commercial and public interests, including the needs of large and small business, public institutions and individual Afghans (UNESCAP, 2002).

The report further seeks to propose a strategy for the development and implementation of a national ICT policy for Afghanistan. The Afghanistan ICT strategy must be flexible to help address and adapt to a complex and rapidly changing environment. Informed participation of all strategy stakeholders and coordinated investment of the collective resources of Afghanistan will be essential if the benefits of ICT are to be realized. Government leadership is required to develop and implement a national strategy. The national ICT policy should be made in Afghanistan, by Afghans, for Afghans. It should be consistent with Afghanistan's history, economic realities, the international context, and the country's unique cultural and social requirements. Recognizing the economic, cultural and social implications of a national ICT policy, three basic objectives will be pursued by the strategy:

- (i) Network Access – ICT networks must be accessible and affordable to all Afghans.
- (ii) Information and Knowledge Access – ICT policies for universal access to information and knowledge are crucial if Afghans are to take their rightful place in the global economy.
- (iii) Government Use of ICT – Government must use ICT to improve its operations and services.

3.4.10 Hong Kong

National ICT Policies

The Hong Kong Government has adopted a multi-prong approach in its ICT policy to promote further deregulation of the IT sector, construction of telecommunications-related infrastructure, the growth of e-business and e-government, investment in IT education, investment in cyber cities and technology parks, reform in legal framework concerning intellectual property rights and e-business, as well as international IT cooperation. The blueprint of Hong Kong's ICT policy is known as Digital 21' IT Strategy (<http://www.american.edu/initeb/cc9979a/PAGE3.HTM>).

Digital 21' IT Strategy

In May 2001, the Hong Kong Government released its updated 'Digital 21' IT Strategy to outline future IT development in Hong Kong. The objective is to position Hong Kong as a leading global e-business community and digital city by targeting e-business, e-government, IT manpower, building a digital society, and by exploitation of enabling technologies.

ICT Legal Environment

Hong Kong actively promotes the protection of software copyrights, privacy and security in its ICT Policy framework. Still, Hong Kong has an enviable track record of maintaining a censorship-free society. A well-developed and properly functioning legal system enables the city to actively contribute to the latest international development on IT issues. Hong Kong has enacted the following laws related to ICT legal framework:

- Freedom of Information Act
- Privacy Act
- Privacy Protection Act
- Computer fraud and Abuse Act
- Electronic communications privacy Act
- Computer Matching and Privacy Protection Act
- Protection of Intellectual property

Software Copyright

A survey in 2000 revealed that 56 percent of the software sold in Hong Kong was pirated or illegal, lower than some countries in the region. The Hong Kong Government has criminalized copyright piracy on a commercial scale, including the deliberate use of software in a business environment, and employees who

knowingly use pirated software will be subjected to legal liabilities. The Intellectual Property Ordinance 2000 extends criminal penalties for unlicensed software from sellers to corporate users.

A recent high-profile local court case illustrates Hong Kong's commitment in protecting software copyright. On October 11, 2002, a high court judge ordered the authorized Microsoft computer retailer Able System Development to pay Microsoft USD 4.5 million in damages for copyright infringement. Able had illegally pre-loaded unlicensed copies of the Office and Windows programmes onto computers it sold between 1996 and 1998 without permission from Microsoft.

Privacy

Hong Kong has enacted ICT legislation, such as the Personal Data (Privacy) Ordinance, which covers Code on Access to Information, based on the European Union (EU) Directive. In the meantime, the Office of Privacy Commissioner for Personal Data focuses on privacy aspects of identity cards and health databases.

Censorship

The freedom from internet censorship has been seen as one of Hong Kong's economic competitive strengths. Freedom of speech is a constitutional guarantee under the Basic Law of Hong Kong.

3.4.11 India

India's efforts in promoting the adaptation of ICT and in combating cybercrime can be summarised by the following legal enactments and initiatives:

- The Information Technology Act 2000
- Rules under the Information Technology Act
- The Semiconductor Integrated Circuits Layout-Design Act
- The Semiconductor Integrated Circuits Layout-Design Rules
- The Communication Convergence Bill
- Computers and the Indian Law
- Hacking and the Indian Law
- Network Service Providers and the Indian Law
- Cybercrime Police Station established in Bangalore, India: a first in Asia-Pacific
- Cybercrime Cells established in different states in India for investigating cybercrime.

National Task Force on Information Technology and Software Development has implemented an appropriate legal framework for the creation of an IT-based society,

with due focus on intellectual property rights (IPR), secrecy, security and safety of information.

India also established the Asian School of Cyber Laws (ASCL) in 1999 to facilitate awareness, study and advanced research in cyberlaw and information security. It provides education and training programmes in cyberlaw, information security and cybercrime investigation. In these fields, they have been working closely with several educational institutions, corporate houses, law enforcement agencies and Government departments, both within India and abroad.

3.4.12 Bangladesh

The Bangladesh government, in response to a broad range of benefits of Information Communication Technology (ICT) in all sectors of economy and human development, developed a national policy framework for the development of the ICT sector with all its ethical norms (BCC, <http://www.bccbd.org/html/itpolicy.htm>).

This Policy aims at building an ICT-driven, knowledge-based society by the year 2006. It calls for a country-wide ICT-infrastructure to be developed to ensure access to information by every citizen.

Legal Issues Addressed

Software copyright provisions embodied in the Bangladesh Copyright Act 2000 were implemented by establishing appropriate enforcement bodies, as mentioned in the Act, to protect against computer crimes, such as computer fraud, hacking, damaging programmes and data, and introducing/spreading computer viruses.

To enhance the capacity of the judiciary, Computer-based Management Information System (CMIS), with suitable Wide Area Network (WAN) and Local Area Network (LAN) was planned to be established for the Supreme Court and for the District Courts and Tribunals. It consists of three inter-related modules, namely, (i) a case management module, (ii) a legal framework module, essentially covering two basic sources of updates, namely the Bangladesh legislative code and the Bangladesh case law database and (iii) a court administration module, whose areas of application may include court inspections, planning and budgeting, transactions, financial accounts, staff-related information and reporting, statistical applications and records management.

Furthermore, in order to utilize ICT fully, exploiting its immense potential in the economic, social, commercial, and scientific fields, a National ICT Task Force has been formed whose objectives include the following:

- Promote and facilitate the use of ICT in all sectors of the economy for transparency, good governance and efficiency improvement.

- Develop a large pool of world-class ICT professionals to meet the needs of local and global markets.
- Promote the use of ICT by providing special allocations for ICT project implementation in the public sector. Train the decision makers in ICT use and promote an ICT culture.
- Provide effective incentives for development of an ICT sector to both local and foreign entrepreneurs.
- Develop an efficient ICT infrastructure that provides open access to international and national networks.
- Establish a legislative and regulatory framework for ICT issues like IPR, data security and protection, digital signatures, e-Commerce, ICT education, etc., as well as to ensure quality ICT education provided by different private organizations.
- Set up national databases that are reliable and easily accessible by all the people of the country.
- Set up an ICT organization at the highest level to continuously promote and foster ICT Industry.
- Enact Laws and Regulations for uninterrupted growth of ICT, in conformity with World Trade Organization (WTO) stipulations.

3.4.13 Cambodia

A national ICT policy for Cambodia was recently proposed within the framework of the eASEAN Agreement. The four main areas of the proposed policy are: 1) enhancing information infrastructure, 2) developing human resources, 3) developing local content, and 4) creating the necessary legal and regulatory environment. As evidence that Cambodia is fully aware of the importance of ICT, the National Information Communications Technology Development Authority (NiDA), chaired by Prime Minister, was established on 23 August 2000. The responsibilities of this authority are to formulate IT promotion and development policy for the short, medium and long term, to implement IT policy to ensure maximum economic growth, and to monitor and audit all IT-related projects in Cambodia. The ICT policy related goals include creating mass awareness among selected groups by sensitizing decision makers and government workers to ICT, and introducing the use of computers in the schools (NiDA, <http://www.nida.gov.kh>).

On the 10th of July, 2003, the Cambodian government made a decision on the Establishment of Technical Working Groups on Policy and Strategy for Developing Information Communications Technology Sector, which comprises the followings:

- Appointment of officials of the NiDA Secretariat and related ministries to be members of Technical Working Groups for policy and strategy.
- Responsibilities and duties of the groups to develop ICT policy and strategy.

3.4.14 Australia

The Telecommunications Act 1997

The Telecommunication Act 1997, and associated legislation, is the third complete overhaul of Australian telecommunications regulatory shifts in the provision of communications services to Australians. The transition to competition has brought with it a heightened concern for consumer protection and the provision of services to people out of metropolitan centres in all its ethical forms. Among the important consumer protection measures are the safeguards set out in the Consumer Protection and Service Standards Act 1999. The main objective of this Act, is to provide a regulatory framework that promotes the following:

- Provision of appropriate community safeguards in relation to telecommunications activities, and adequate regulation of participants in sections of the Australian telecommunications industry;
- The development of an Australian telecommunications industry that is efficient, competitive and responsive to the needs of the Australian community; and
- The equitable distribution of benefits from improvements in the efficiency and effectiveness of the provision of telecommunications networks and facilities; and the supply of carriage services.

Radio Communications Act 1992

The objective of this Act is to provide for management of the radio frequency spectrum in order to:

- (a) Maximize, by ensuring the efficient allocation and use of the spectrum, the overall public benefit derived from using the radio frequency spectrum;
- (b) make adequate provision of the spectrum for use by public or community services;
- (c) provide a responsive and flexible approach to meeting the needs of users of the spectrum;
- (d) encourage the use of efficient radio communication technologies so that a wide range of services of an adequate quality can be provided;
- (e) provide an efficient, equitable and transparent system of charging for the use of spectrum, taking account of the value of both commercial and non-commercial use of spectrum;
- (f) support the communications policy objectives of the Commonwealth Government;
- (g) provide a regulatory environment that maximises opportunities for the Australian communications industry in domestic and international markets; and

- (h) promote Australia's interests concerning international agreements, treaties and conventions relating to radio communications or the radiofrequency spectrum.

Institutions/framework relating to ICT Ethics

Australian Institute of Computer Ethics (AICE)

AICE is a multi-disciplinary resource and research centre composed of a diverse group of people who care about the social effects of information and communications technology and seek to identify associated ethical problems and guidelines. AICE is based at Swinburne University of Technology in Hawthorn, Melbourne, Victoria and Charles Sturt University in Wagga Wagga, New South Wales.

Australia's National Computer Emergency Response Team (AusCERT)

AusCERT, as Australia's national Computer Emergency Response Team (CERT), is an independent, not-for-profit organization, based at the University of Queensland. AusCERT covers its operating costs through member subscriptions and the provision of affordable computer security training and education, and consultancy services. The Commonwealth government currently provides funding for certain parts of AusCERT's operations. AusCERT monitors and evaluates global computer network threats and vulnerabilities from numerous sources throughout the year, including after hours when Coordination Centre staff remain on-call to respond to new information in a time critical manner. As a result, AusCERT publishes security bulletins, drawing on material from a variety of sources, with recommended prevention and mitigation strategies. AusCERT has access to accurate, timely and reliable information about emerging computer network threats and vulnerabilities on a global basis. Additionally, AusCERT maintains a large network of CERT contacts in North America, the United Kingdom, Europe and throughout Asia (<http://www.auscert.org.au/render.html?cid=2>).

Business Ethics Research Unit

The Business Ethics Research Unit (BERU), based at Victoria University, runs frequent seminars, concentrating on ethics in the business context. BERU has existed for several years and has member-level links with AICE.

Ethical Enterprise Network

The Ethical Enterprise Network (EEN) aims to help members adopt ethical practices within their own enterprises and build awareness in the community about ethical, sustainable and just business practices. EEN also aims to build networks between ethical enterprises through membership, a regular newsletter, meetings and sharing of information about ethical activities, internal and external. (EEN, 2000)

3.4.15 Japan

The main cyberlaws of Japan are:

- ***Unauthorized Computer Access Law of 1999***

The Law prohibits acts of unauthorized computer access and stipulates penal provisions for such acts. It calls for assistance measures to be taken by the Metropolitan or Prefectural Public Safety Commissions to prevent a recurrence of such acts, as well as computer-related crimes committed through telecommunication lines. They are also to maintain the telecommunications-related order that is realized by access control functions, and, thereby, contribute to the sound development of the advanced information and telecommunications society.

- ***Copyright Law of 2002***

The purpose is to provide for the rights of authors and the rights neighbouring thereon with respect to works, as well as performances, phonograms, broadcasts and wire diffusions, to secure the protection of the rights of authors, etc., having regard to a just and fair exploitation of these cultural products, and thereby to contribute to the development of culture.

- ***Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (IT Basic Law)***

The purpose of this Law shall be to promote measures for the formulation of an advanced information and telecommunications network society expeditiously and intensively by stipulating the basic ideas and the basic policy for formulating measures, clarifying the responsibilities of the State and local governments, and providing stipulations on the development of a priority policy programme for the formation of an advanced information and telecommunications network society.

Japan also has a Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure which view that cyber terrorism has the potential to have a large impact on people's lives and on the economic activities of business using telecommunications networks and information systems. The goal is to protect the critical infrastructure from such attacks. (http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html).

Framework relating to ICT Ethics

Foundations of Information Ethics, Japan (FINE)

This project is five-year joint effort, funded by the Japan Society for the Promotion of Science, and by researchers from Kyoto, Hiroshima and Chiba Universities for the construction of philosophically tenable thinking of ethical issues in the ever

increasing variety of uses of computers and information technology and their impacts on society.

3.4.16 New Zealand

New Zealand represents the Asia-Pacific region well in terms of their IT legal environment. They have memberships with several worldwide organizations dedicated to internet and DNS regulations, information sharing, privacy protection, and combating piracy. These organizations include the World Intellectual Property Organization, International Corporation for Assigned Names and Numbers, and Privacy International.

The following are examples of laws in New Zealand that are related to cyberlaw, either directly or indirectly:

Model Freedom of Information Law (2001)

New Zealand is one of the countries that subscribe to the Model Freedom of Information Law which provides for an enforceable legal right to access information held by public bodies upon submission of a request. Everyone may claim this right, and both information and public bodies are defined broadly. The Law also provides for a more limited right to access information held by private bodies, where this is necessary for the exercise or protection of any right. In this respect, it follows South African legislation in recognizing that private bodies hold much important information, and that to exclude them from the ambit of the law would significantly undermine the right to information. The right to information is guaranteed in international law, included as part of the guarantee of freedom of expression in Article 19 of the International Covenant on Civil and Political Rights. (<http://www.american.edu/initeb/sf9412a/legal.htm>).

Electronic Transactions Act 2002

The ETA does three things in order to facilitate the use of electronic technology:

- It confirms that electronic methods of communication are legally effective;
- It sets default rules for the time and place of dispatch and receipt of electronic communications (whether or not the communications are used to meet statutory requirements); and
- It provides that certain paper-based legal requirements may be met by using electronic technology that is functionally equivalent to those legal requirements.

Copyright Act 1994

This Act allows copyright owners to control certain activities relating to the use and dissemination of copyright works. Under the Act, the owner of copyright in a work has the “exclusive right” to do certain “restricted acts” in relation to the work.

Personal Properties Securities Act 2002

The Act affects all security interests in personal property, such as cars, computers and boats (under 24 metres in length), but does not apply to land. A security interest over these items secures the payment of money, or the performance of an obligation.

Frameworks at Regional Level

Centre for Asia-Pacific Technology Law and Policy @ Nanyang Business School (CAPTEL). <http://captel.ntu.edu.sg>

CAPTEL is a centre for research and consultancy in technology law and policy to promote ICT ethics development in Asia-Pacific. The core objective of the centre is to conduct developmental research on technology law and policy. To achieve their objective, the centre has multi-track themes to reflect the diverse expertise from the School and associate fellows. Among the areas of focus of the Centre are:

- a) Protection Regimes for Intellectual Property Rights – The laws relating to the protection of intellectual property of new technologies and to the new property developed by the use of new technologies.
- b) Legal Infrastructure for E-Business – Research on the development of International Treatises, Codes and Model Laws and their impact on E-Commerce.
- c) Regulation of the Internet – Researching the development of Standards for Internet Regulation to manage Internet conduct in Asia-Pacific; Content regulation.
- d) ICT Laws – Cybercrime, Technology Security, Privacy and other ICT laws.
- e) Telecommunications Law – Access Issues.
- f) Biotechnology Law & Ethics – Research in related laws and policy and regulatory infrastructure.
- g) ICT Competition Law.
- h) Development of a repository database of relevant laws and cases in the region for further research – Collecting and sharing with the Public information on the region’s reported cases and developments affecting technology.

3.5 Women and ICT

3.5.1 Asian Pacific Women's Information Network Centre (APWINC)

The Asian Pacific Women's Information Network Centre or APWINC promotes the use of multimedia applications and information technologies among women. APWINC is a young organization; it is an offshoot of the desire of many individual women and women's organizations to work together towards developing ways to promote positive portrayal of women in the mass media.

3.5.2 Asian Women's Resource Exchange (AWORC)

The Asian Women's Resource Exchange (AWORC) is an internet-based women's information service and network in Asia. It is an initiative geared towards developing cooperative approaches and partnerships for increasing access to, and exploring applications of, the new information and communication technologies for women's empowerment. AWORC aims to help expand existing regional networks in the women's movement, promote electronic resource sharing and build a regional information service that will support various women's advocacies specifically those that are very critical for the women in our region. AWORC aspires to contribute to global efforts to address gender disparity on the Internet. It is geared towards building sustainable, as well as promoting Net literacy and enhancing social activism among individual women and women's organizations. The members of the growing AWORC community include women's information, resource and documentation centres, women's information providers and users; as well as communications organizations working closely with women's networks.

3.5.3 Women's Electronic Network Training (WENT)

Since 1999, AWORC has been holding an annual training workshop on electronic networking open to women and their organizations in Asia and the Pacific. The Women's Electronic Networking Training (WENT) is open to all women whose organizations play, or will play, a significant role in promoting the use of information and communication technology to enhance women's role and capacity in ethics, social and policy advocacy, as well as to strengthen women's organizations and networks in Asia and the Pacific.

From the first workshop in 1999 which trained 23 women from 11 countries to use email and Web-based services to promote and enhance their participation in the review process for the Beijing Platform for Action (popularly known as the Beijing Plus Five review), WENT has diversified its training courses to respond to various information and communication needs of women in Asia and the Pacific. Since 2000, WENT has parallel instructional tracks on Web-based Information Management, Using ICT for Advocacy, and Managing information using Database.

3.5.4 Asian Pacific Women’s Information Network Centre (APWINC) South Korea

The Asian Pacific Women’s Information Network Centre or APWINC promotes the use of multimedia applications and information technologies among women. It sees its participation in AWORC as one important step towards enabling women in the Asia-Pacific region to use information and communication technologies to advance their status and rights in society.

3.6 Asian-Pacific Development Information Programme

The Asia-Pacific Development Information Programme (APDIP) is an initiative of the United Nations Development Programme (UNDP) that aims to promote the development and application of new ICT for poverty alleviation and sustainable human development in the Asia-Pacific region. It does so through three core programme areas, namely: Policy development and Dialogue; Access; Content Development and Management (<http://www.apdip.net/documents/>).

APDIP delivers its objectives through activities that involve awareness raising and advocacy, building capacities, promoting ICT policies and dialogue, promoting equitable access to tools and technologies, knowledge sharing, and networking. Strategic public-private sector partnerships and opportunities for technical cooperation among developing countries (TCDC) are the key building blocks in implementing each programme activity. APDIP has also lunched programmes like International Open Source Network (IOSN), in the developing countries in the Asia-Pacific Region to achieve rapid and sustained economic and social development by using affordable yet effective Open Source ICT solutions for bridging the digital divide Wong.

In line with APDIP’s goals of improving access to developing countries, the overall objective of this project is to create a Centre of Excellence on Open Source technologies and applications. It also aids countries in sharing information on Open Source (OS), assist with the development of needed toolkits and resource materials, support “localization” efforts and, generally, help facilitate and coordinate OS programmes and initiatives through networking.

Table 3.3. Top 15 Countries in Internet Penetration Rate at Year-End 1999

<i>Rank</i>	<i>Country</i>	<i>Users/1 000 Population</i>
1	Canada	428.20
2	Sweden	414.15
3	Finland	408.04
4	US	406.49
5	Iceland	403.46
6	Denmark	395.97
7	Norway	379.59
8	Australia	343.27
9	Singapore	310.77
10	New Zealand	264.90
11	Netherlands	255.55
12	Switzerland	245.81
13	United Kingdom	236.41
14	Taiwan, China	216.82
15	Hong Kong, SAR China	212.91
	Average of Top 15 Countries	328.16
	Worldwide Average	46.75

Source: Computer Internet Industry Almanac, October 2000:
<http://www.c-i-a.com/200010iu.htm>.

Table 3.4. Top 15 Countries in Internet Use at Year-End 1999

<i>Rank</i>	<i>Country</i>	<i>Users (Millions)</i>
1	USA	110.8
2	Japan	18.2
3	UK	14.0
4	Canada	13.3
5	Germany	12.3
6	Australia	6.8
7	Brazil	6.8
8	China	6.3
9	France	5.7
10	South Korea	5.7
11	Taiwan, China	4.8
12	Italy	4.7
13	Sweden	4.0
14	Netherlands	2.9
15	Spain	2.9

Source: Computer Industry Almanac, <http://www.c-i-a.com/199911iu.htm>.

Table 3.5. Length of Time to Reach 30% Penetration in USA

<i>Technology</i>	<i>No. of Years to Reach 30% Penetration</i>
Internet	7
Television	17
Telephone	38
Electricity	46

Source: US Internet Council, April 1999.

4. CHALLENGES AND ISSUES

There are many challenges and issues that need to be addressed by governments, NGOs, communities, professional organizations, and individuals at large in the process of embracing ICT as a tool for the development and progress of humanity in general. The main challenges and issues that we going to be engaged with include the digital divide, poverty, privacy, cybercrime, human rights, and gender inequality.

4.1 Digital Divide

The ethical implications of ICT pose considerable issues and challenges in the Asia-Pacific region. ICT represents an unprecedented opportunity to provide new knowledge, services, and opportunities in rural and underserved areas. Both urban and rural consumers may benefit from ICTs by receiving: (i) enhanced access to information and communication across large distances, (ii) improved access to governmental and quasi-governmental resources and services, (iii) new credit and financial services available through palmtops and information kiosks, (iv) new opportunities to design, manufacture and market their products through ICT-technological systems, (v) more and better education through computers, and (vi) superior medical advice, diagnosis or knowledge in their own region. In the long term, the region ICT projects could prove to be the most effective means of driving change in the urban/rural areas of the region: *socially*, by ensuring equal access for underprivileged groups, *economically*: by creating new kinds of work and financial transactions, and *politically*: by improving the quality, speed, and sensitivity of the state apparatus to the needs of region citizen-consumers.

Table 4.1, provided by the Computer Internet Industry Almanac, shows the internet penetration rate at the end of 1999. They show a world average of 46.75 as compared to 428.20 per 1,000 population in Canada. These figures confirm the existence of a digital divide between developed and underdeveloped nations. Actions to bridge this gap need to be implemented expeditiously. Table 4.2 shows that the length of time to reach 30% internet penetration rate in USA is less than 7 years as compared to 48 years in the case of electricity supply. This calls for more aggressive actions from the governments of underprivileged nations to intensify their promotion of the use of ICT. Table 4.3 notes ICT indicators of penetration of a few selected countries.

The countries of the Asia-Pacific region have wide diversity in geography, economics, politics, culture, language and many other aspects. The region has about 61 percent of the world population, and 5 of the 9 highest population developing countries are in the region, namely, Bangladesh, China, India, Indonesia, and Pakistan.

Table 4.1. Top 15 Countries in Internet Penetration Rate at Year-End 1999

<i>Rank</i>	<i>Country</i>	<i>Users/1 000 Population</i>
1	Canada	428.20
2	Sweden	414.15
3	Finland	408.04
4	US	406.49
5	Iceland	403.46
6	Denmark	395.97
7	Norway	379.59
8	Australia	343.27
9	<i>Singapore</i>	<i>310.77</i>
10	<i>New Zealand</i>	<i>264.90</i>
11	Netherlands	255.55
12	Switzerland	245.81
13	United Kingdom	236.41
14	<i>Taiwan, China</i>	<i>216.82</i>
15	<i>Hong Kong, SAR China</i>	<i>212.91</i>
	Average of Top 15 Countries	328.16
	Worldwide Average	46.75

Source: Computer Internet Industry Almanac, October 2000:
<http://www.c-i-a.com/200010iu.htm>.

Table 4.2. Length of Time to Reach 30% Penetration in US

<i>Technology</i>	<i>No. of Years to Reach 30% Penetration</i>
Internet	7
Television	17
Telephone	38
Electricity	46

Source: US Internet Council, April 1999.

The Information Society is so called because of the pivotal role played by ICT in dissemination of information-intensive services (business and property services, communications, finance and insurance) and the public sector services (education, public administration, and health care). The digital divide comes into existence due to the gap between those who have access to, and use of ICT, and those who do not. Digital divides exist both between countries in Asia-Pacific, and between countries in the world. Furthermore, the concept of the digital divide is extended to encompass the issue of disparity between how different nations are using information and communication technologies as a tool for human development, intellectually, socially and economically.

Table 4.3. ICT Indicators of Selected Countries

<i>Country</i>	<i>Telephone Mainlines Per 1 000 People 1999</i>	<i>Mobile Telephones Per 1 000 People 1999</i>	<i>Personal Computers Per 1 000 People 1999</i>	<i>Internet Host Per 1 000 People 1999</i>
Indonesia	29.1	9.83	13.4	0.18
Philippines	37.9	36.97	19.5	0.23
Thailand	84.5	39.57	40.4	0.49
Brazil	152.2	84.70	52.9	1.93
Malaysia	219.3	145.05	94.5	2.80
Argentina	213.8	109.72	59.9	3.08
South Africa	126.9	101.06	54.1	4.21
Korea	449.7	499.04	181.3	6.03
Ireland	472.4	360.59	352.6	15.95
Singapore	484.1	381.45	390.9	22.19
Hong Kong, SAR	559.6	551.02	360.2	66.40
Finland	557.2	678.10	507.8	117.25

Source: World Development Report, 1999/2000.
World Competitiveness Yearbook, 2000.

The digital divide is a new gap created by ICT between insiders and outsiders of the info-sphere. The info-sphere is not a geographical, political, social, or linguistic space. It is the space of mental life, from education to science, from cultural expressions to communication, and from trade to recreation. The borders of the info-sphere cut across North and South, East and West, industrialized and developing countries, political systems and religious traditions, younger and older generations, even members of the same family.

It seems more accurate to say that the digital divide occurs between individuals rather than between countries or whole societies, between the computer literate and the computer illiterate, between the information rich and the information poor, whatever their nationality or neighbourhood. Currently, only 5 percent of the world's populations have access to information and communication technologies (ICTs). The remaining 95 percent are "disadvantaged" or "underprivileged." They live under the shadow of the new digital reality, which allows them no interaction or access, but which profoundly influences their lives.

The digital divide is the source of most of the ethical problems emerging from the evolution of the Information Society. The digital divide disembowels, discriminates, and generates dependency to the underprivileged. It can create new forms of colonialism and apartheid that must be prevented, opposed and ultimately destroyed. This is the main challenge of the Asia-Pacific region in the era of the Information Society.

4.2 Poverty

ICTs are increasingly central in the effort to escape poverty. Few would argue that lack of access to information and communications technologies is an element of poverty in the way that insufficient nutrition or inadequate shelter is. ICTs have repeatedly demonstrated their potential for alleviating poverty in the Asia-Pacific region, and in developing countries around the world. For example, poor people have experienced benefits in the form of: increased income; better health care; improved education and training; access to job development opportunities; engagement with government services; contacts with family and friends; enterprise development opportunities; increased agricultural productivity, and so on. However, in probably all cases, these experiences have arisen from highly focused and locally intensive pilot projects that were experimental in nature. Whilst doubts and uncertainties continue to exist with regard to the applicability of ICTs to the problems of the poor, such projects contribute immeasurably to the growing body of knowledge and experience that is required in order to understand the conditions under which ICTs can be usefully applied towards the alleviation of poverty.

The tables in Appendix B show the correlation between per capital income, the technology index and ICT diffusion in a few selected countries in the region. These two tables indicate some correlation between per capital income and ICT diffusion. The question is: “Can the use of ICTs alleviate poverty and overcome the digital divide?”

The global problem of poverty alleviation is enduring and massive. Achieving the millennium development goal of halving global poverty by 2015 will require an enormous undertaking many orders of magnitude greater in resource mobilization and complexity. In terms of their global impact on the world’s poor populations, and the Asia-Pacific region, in particular, the effect of the existing initiatives is undetectable. But, in many cases, their contribution is to indicate areas of activity that have emerged as critical factors for improving the lives of the poor through the application of ICT. Take, as an example, the application of ICT in teaching and learning, referred to as Smart Schools or e-learning. We are now beginning to understand the critical role of community participation, in addition to institutional transformation, culture specificity, policy-making telecommunications reform, openness in government, the need for a suitable legal framework and the development of human resources that are also necessary.

A lack of national policies promoting ICT as a tool for development may be deduced from the poor ICT infrastructure, such as inefficient telephone services or absence of electricity, in many rural and remote areas in Asia-Pacific. The natural geographical features, such as vast expanses of land, scattered islands, and difficult terrain have contributed to denying the benefits of the new technology to a vast majority of lower income communities in countries like India, Nepal, Indonesia and the Philippines. The costs of computer hardware and software,

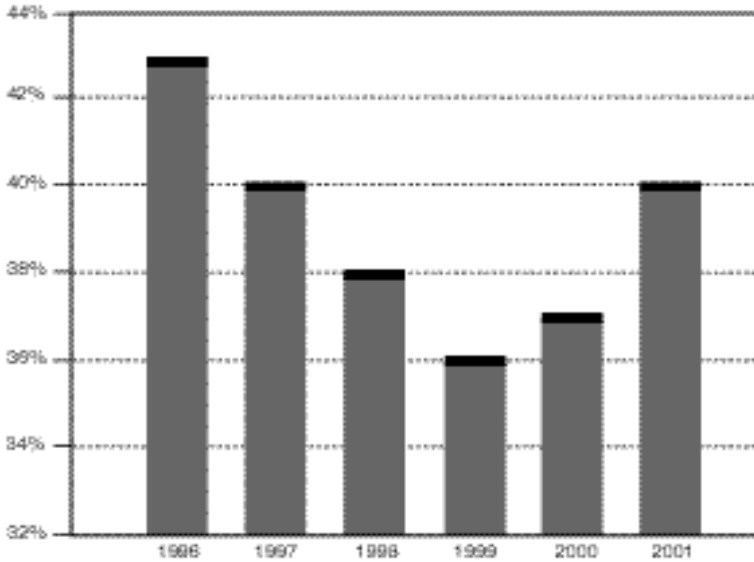
especially licensed software, and costs of maintenance and connectivity is beyond the affordability for these communities. The average monthly charge for an internet account in the Pacific countries studied is US\$50. On an annual basis, this amounts to one quarter to one half of the annual per capita GDP of many countries in the Pacific and is clearly unaffordable by the majority of people (Cabrere-Balleza, 2002). To offer a comparison, a typical US user will pay 1.2 percent of the per capita GDP in the US every month to access the internet while a user in Madagascar will pay 614 percent of per capita GDP (S. Nanthikesan, Trends in Digital Divide, Harvard Centre for Population and Development Studies).

The underprivileged need to be made aware the importance of ICT. They need to be given access to the infrastructure and services available, and provided with the skills for using ICT, in order to establish their presence in the world, and, ultimately, be able gain the benefits provided by ICT for wealth creation through e-commerce and services industries. This might help in achieving the millennium development goal of halving global poverty by 2015. But, the challenge is how to do it?

4.3 Piracy

The results from the annual BSA Global Piracy Study for 2001 indicate that for the first time in the study's history, the world piracy rate increased in two consecutive years, i.e. in the year 2000 and 2001 (see Figure 4.1, same as Figure 2.1). The 2001 piracy rate of 40 percent is a marked increase from 37 percent in 2000. And, both years were up from the low set in 1999 at 36 percent. Since the study began in 1994, a steady decrease in the rate of software piracy was observed. In 2001, the effect of a worldwide economic slowdown has hit technology spending particularly hard. The results of this year 2001 study indicate that software piracy rose in response to the pressure of the curtailed spending of the economic downturn. This is the first period of a general global economic slowdown since the study began in 1994. The results presented here suggest that the progress against piracy that was made in the 1990s is conditional. Compliance with software licensing is at risk of being considered an economic luxury that can be abandoned in difficult times.

Factors like economic downturns and low standards of living crudely indicate that poverty is the main reason for the high rate of piracy in underdeveloped countries, and especially in the Asia-Pacific region where per capital incomes are much lower than in developed nations. In fiscal year 2001, Malaysia and India experienced piracy rate increases, 70 percent for both countries (see Table 4.4). The Philippines' rate increased to 63 percent. Indonesia had an 88 percent piracy rate, down from 89 percent in 2000. Vietnam, with a piracy rate at 94 percent, continued as the country with the highest piracy rate in the region. China, with 92 percent, followed as the country with the second highest piracy rate. In order not to be left outside the info-sphere during difficult times has forced individuals and corporations to resort to piracy because ICT is considered as luxury during those difficult periods.



Source: BSA Global Piracy Study for 2001.

Figure 4.1. World Piracy Race

The prices of software listed in the Asia-Pacific region do not encourage individuals to buy originals because their incomes do not permit them to do so. Piracy seems to be unavoidable in order to be in the info-sphere, regardless of the religious belief or ethical values one holds. If piracy persists in a country, it will affect the local software industry and wealth creation through ICT investments. Local companies and venture capitalists will not want to invest in ICT there because they will lose to piracy. Thus, the country remains poor and the society promotes piracy, which then kills any indigenous ICT industry. This vicious circle then continues. The challenge is how to stop the vicious circle?

4.4 Cybercrime

Regional and international trends in cybercrime take various forms, including theft, fraud, extortion, crimes against persons, sales of drugs and contraband, intellectual property piracy, theft of information, spread of malicious codes, denial of service attacks and cyber-terrorism. There have been no detailed studies conducted exclusively on the issue of Cybercrime and Information Security in Asia-Pacific as a whole. The 2002, a Computer Crime Survey conducted by the Computer Security Institute confirmed that the threat from computer crime and information security breaches continued unabated, and that the financial toll was mounting. The systems that are particularly vulnerable to cybercrime are national critical infrastructures, computer networks, electronic governance systems, online justice and medical emergency systems. There are numerous international and regional

Table 4.4. Piracy Rate in Asia-Pacific

Asia-Pacific	Piracy Rates						Retail Software Revenue Lost to Piracy (1 000)					
	1996 %	1997 %	1998 %	1999 %	2000 %	2001 %	1996 \$	1997 \$	1998 \$	1999 \$	2000 \$	2001 \$
Australia	32	32	33	32	33	27	128 267	129 414	192 237	150 390	132 533	91 011
China	96	96	95	91	94	92	703 839	1 449 454	1 193 386	645 480	1 124 395	1 662 404
Hong Kong, SAR	64	67	59	56	57	53	129 109	122 169	88 627	110 190	86 195	164 040
India	79	69	65	61	63	70	255 344	184 664	197 333	214 557	239 629	365 318
Indonesia	97	93	92	85	89	88	197 313	193 275	58 756	42 106	69 991	79 463
Japan	41	32	31	31	37	37	1 190 323	752 598	596 910	975 396	1 666 331	1 721 050
Korea	70	67	64	50	56	48	515 547	582 320	197 516	197 269	302 938	186 574
Malaysia	80	70	73	71	66	70	121 488	82 552	79 268	84 154	95 567	94 544
New Zealand	35	34	32	31	28	26	29 271	20 284	21 758	19 656	12 373	11 445
Pakistan	92	88	86	83	83	83	23 144	20 395	22 667	18 913	31 379	11 429
Philippines	92	83	77	70	61	63	70 735	49 151	31 138	33 163	27 091	24 655
Singapore	59	56	52	51	50	51	56 553	56 599	58 262	61 758	44 299	41 802
Taiwan, China	66	63	59	54	53	53	116 980	136 850	141 274	122 946	154 754	136 735
Thailand	80	84	82	81	79	77	137 063	94 404	48 613	82 183	53 082	41 123
Vietnam	99	98	97	98	97	94	15 216	10 132	10 328	13 106	34 938	32 246
Other Asia-Pacific	86	83	74	71	75	70	49 113	31 974	16 739	20 262	7 566	62 616
Totals	55	52	49	47	51	54	3 739 304	3 916 236	2 954 812	2 791 531	4 083 061	4 726 454

Source: BSA Global Piracy Study for 2001.

initiatives which have laid the foundation for the further development of mechanisms for enhancing information security and preventing cybercrime. Factors which have hampered efforts to promote information security in the region include: lack of awareness, capacity, technology and insufficient regulatory protection. Still, few countries in the region have enacted cyberlaws (United Nations Economic and Social Commission for Asia and the Pacific [UNESCAP] Asia-Pacific Conference on Cybercrime and Information Security 11-13 November 2002, Seoul, Republic of Korea.)

The lack of legal instruments notwithstanding, the incidence of malicious attacks on the confidentiality, integrity and availability of computer data and systems, computer-related offences such as forgery and fraud, content-related offences such as those related to child pornography and intellectual property rights (IPRs) violations, are considered to be significant. Threats to critical infrastructure and national interests arising from the use of the internet for criminal activity are of growing concern. The statistics of cybercrime reported by Thailand and Korea, Table 4.5, are enough to explain the increasing concern about cybercrime in the region.

**Table 4.5. Cybercrime Report of Thailand
(April 2002 to November 2002)**

<i>Incidents</i>	<i>Cases</i>	<i>%</i>
Pornography Website (Thai Language)	1 419	38.98
Pornography Website (Foreign Language)	832	22.86
Child Pornography	63	1.73
Pornography Products Website (Thai Language)	443	12.17
Pornography Products Website (Foreign Language)	36	0.99
Intellectual Piracy Website	187	5.14
Other Illegal Material	175	4.81
Prostitution	89	2.45
Gambling (Thai Language)	96	2.64
Gambling (Foreign Language)	30	0.82
National Security	270	7.42
Total	3 640	

Source: Royal Thai Police Agency <<http://www.police.go.th/crimewebpost/report/sum.php>>

Table 4.6. Cybercrime Report of Korea

<i>Crime</i>	<i>Incidents</i>	<i>Rate (%)</i>
Leak of personal information and invasion of privacy	870	43.5
Spam mail	659	33.0
Virus and cracking	219	11.0
Obscene and violent image	181	9.1
Alienation and digital Divide	50	2.5
Infringement of copyright and illegal copy of S/W	15	0.8
Others	6	0.3
Total	2 000	100.0

Source: KISA (Korea Information Security Agency), 2001.

Table 4.7. Report on cracking and virus incidence in Korea

<i>Crime</i>	<i>1997</i>	<i>1998</i>	<i>1999</i>	<i>2000</i>	<i>2001</i>	<i>2002</i>
Cracking (Case)	64	158	572	1 943	5 333	5 252
Virus (Case)	–	–	–	–	65 033	27 561

Source: Korea Information Security Agency.

Countries of the Asia-Pacific region have started to have appropriate legal and regulatory frameworks to meet these challenges, (see Table 4.8). Awareness is growing, but even where legislation may be adequate, the capability to use information security technologies and related procedures to protect against human right abuses, and to assist other countries, is still considered low. As a result, reported cybercrime may represent only a small fraction of the total incidence. There is a need for more accurate estimates of the prevalence of such malicious attacks on human development.

Table 4.8. Cyberlaw Initiatives in Asia-Pacific Countries

<i>Country</i>	<i>Law</i>	<i>Year</i>	<i>Purpose</i>
Australia	Copyright Act 1968	1968	Protect intellectual property rights
	Copyright Amendment (Digital Agenda) Act 2000 (which amended the Copyright Act 1968)	2000	Balanced copyright regime that encourages creativity, investment and innovation in the development of new content as well as promoting reasonable online access to research, cultural and educational materials
	Copyright Amendment (Moral Rights) Act 2000	2000	“Moral rights” to the original creators of copyright material, whether or not they are also still the owners of copyright of the material.
New Zealand	Digital Technology and the Copyright Act 1994	1994	
	Copyright Act 1994	1994	
Hong Kong, SAR	The Intellectual Property Ordinance 2000 (Fulfil World Trade Organization (WTO) Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights)	2000	Extends criminal penalties for unlicensed software from sellers to corporate users
	Personal Data (Privacy) Ordinance		Covers privacy in public and public sectors
	Code on Access to Information (European Union (EU) Directive)		
	Control of Obscene and Indecent Articles Ordinance		Deals with sexually explicit materials
	Digital Signature (Electronic Transactions Ordinance 2000)	2000	Whether the transformation was generated using the private key that corresponds to the signer’s public key Whether the initial electronic record has been altered since the transformation was generated

Table 4.8. (continued)

<i>Country</i>	<i>Law</i>	<i>Year</i>	<i>Purpose</i>
Indonesia	Patents	August 1, 1991	Compulsory licensing provisions, a relatively short term of protection (14 years), and a provision, which allows importation of 50 pharmaceutical products by non-patent holders
	Trademarks	April 1993	The law provides protection for well known marks. Marks must actually be used in commerce, and cancellation actions must be lodged within five years of the trademark registration date
	Copyrights <ul style="list-style-type: none"> • Act No. 6 of 1982 regarding Copyrights • Act No. 7 of 1987 regarding the Amendment of Act No. 6 of 1982 • Act No. 12 of 1997 regarding the Amendment of Act No. 6 of 1982 as Amended by Act No. 7 of 1987 • Government Regulation No. 14 of 1986 regarding Copyright Council; as Amended by Government Regulation No. 7 of 1989 • Circular Letter of Minister of Justice No. M.01-PW.07.03 of 1987 regarding the Authority to Investigate Copyright Criminal Infringement 	1987	Provides conformity with international standards for copyright protection. A bilateral copyright agreement between the United States and Indonesia went into effect in August 1989 extending national treatment to each other's copyrighted works. The government has demonstrated that it wants to stop copyright piracy and that it is willing to work with copyright holders to this end.
Korea	Patent & Utility Model Protection		
	Copyright Protection		
	1 Copyright Protection in Multimedia		

Table 4.8. (continued)

<i>Country</i>	<i>Law</i>	<i>Year</i>	<i>Purpose</i>
	Trademark Law	1997	A trademark under the Trademark Act is “a sign, character, figure, three-dimensional shape or any combination thereof or those with colour which are used on goods or service by a person who produces, manufactures, processes, sells or certifies such goods or services in order to distinguish his goods or services from those of others.”
	Design Law		
	Unfair Prevention and Trade Secret Protection Law	February 2001	Broader protection of well-known trademarks.
	New Plant Varieties	1995	A special law to provide protection for new plant varieties.
	Database In Copyright Act	1993 and 1995	For the Databases and certain neighbouring rights of copyrighted works have been afforded protection by amendments to the Copyright Act in.
	Semiconductor Chip Layout Designs	1992	The Government passed the Semiconductor Chip Layout Design Act in 1992, which became effective in September 1993 to protect of semiconductor chip layout designs.
	Trade Secrets	1991	In 1991, a statutory basis was provided for the protection of trade secrets, by an amendment to the Unfair Competition Prevention Act. Various Korean law and regulations requires foreign business to submit detailed information on business plan or product to government for mandatory approval.

Table 4.8. (continued)

<i>Country</i>	<i>Law</i>	<i>Year</i>	<i>Purpose</i>
Philippines	The Intellectual Property Rights Code <ul style="list-style-type: none"> • Copyright and Related Rights; • Trademarks and Service Marks; • Geographic Indications; • Industrial Designs; • Patents; • Layout-Designs [Topographies] of Integrated Circuits; and • Protection of Undisclosed Information 	January 1, 1998	Imposes higher penalties and fines for the manufacture, distribution and use of unlicensed software.
	House Resolution 890		Pushes for the interconnection of local Internet Service Providers into one Internet exchange.
	Wiretapping Laws		Wiretapping is not allowed unless ordered by the court. The Anti-Wiretapping Law requires a court order to obtain a telephone tap.
	Cryptography and Liberty 1999 An International Survey of Encryption Policy		The use of cryptographic hardware and software is not currently controlled in the Philippines and so the domestic use of encryption by citizens is not restricted. This is a forward step for the Philippines as the government has noted the importance of security of electronic information for electronic commerce, the threats of economic espionage, and the need to protect privacy online.
Singapore	Copyright Act (Cap 63) of 1987 Layout-designs of	1987 was amended in 1994, 1998 and 1999	

Table 4.8. (continued)

<i>Country</i>	<i>Law</i>	<i>Year</i>	<i>Purpose</i>
	Integrated Circuits Act 1998	1988	Protection for original layout-designs that are created after the issuance of the Act (i.e. 15 February 1999).
Thailand	Copyright law 1994	1994	Extends a criminal penalty for unlicensed software from sellers to corporate users.
	Official Information Act	1997	
	The Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS)	1995	
	Most enforcement activities remain under the jurisdiction of the Economic Crimes Investigation Division (ECID) of the Royal Thai Police.		
	Electronic Transaction Act	2002	
Japan	Copy right law 1899	Amendment 1969 updated 1998, 1999, 2000	Provides criminal penalties for unlicensed software from sellers to corporate users.
	Science & Tech. basic Laws Law No. 130	1995	
	Patent Law		Facilitates the spread of online business by enhancing the protection of intellectual rights by internet firms
	Law on the Formation of Advances Information & Telecommunications Network Society.	Jan 2001	
	Electronic media – IT comprehensive law	April 2001	
	Unauthorized Computer Access Law		Prohibits acts of unauthorized computer access in order control computer crime
	Law of data protection	2000	
	Law Concerning Electronic Signatures & Certification Services	2001	
	Spam Blocking Law	Proposed soon 2003	

There are a few countries in the region that have governmental policies on development and human resources development programmes, and that have built significant capacity, experience and know-how, which can be shared with less developed countries. Cybercrime does not respect national borders; therefore, it requires cooperative, pro-active approaches in support of the less developed countries of the region. New ethical policies for this information age are urgently required to fill the rapidly multiplying “policy vacuums” (Moor, 1985). But filling such vacuums is a complex social process that requires the active participation of individuals, organizations, and governments, and ultimately the Asia-Pacific communities, at large, in a concerted organized effort (Bynum, 1995).

4.5 Human Rights

Human Rights, in terms of freedom of expression and the protection of confidentiality of personal data, should be the fundamental principle of any democratic society in the ICT world. However, the exercise of this principle should not undermine respect for others and human dignity, and it should be in line with the law. The meaning of freedom of expression, personal freedom, right to use personal data and its secrecy, are not at all firmly established among the different nations in Asia-Pacific and, thus, ICT users in different countries have different ideas regarding these issues.

The notion of freedom of expression is a principle widely recognized as one of the foundations of a democratic functioning of society, taking into account the Universal Declaration of Human Rights, the Protection of Human Rights and Fundamental Freedoms, and the First Amendment of the Constitution of the United States of America. It is linked with the values of each society, and, thus, it presents many difficulties in establishing a regional standard.

Penalty for the abuse of the freedom of expression is clearly an issue of parallel importance. Such penalties are, at present, foreseen for infringements of personal freedoms, through defamation, insult, infringements of private life, racial hatred, political abuses, business rivalry, as well as a threat towards law and order, e.g., terrorism, trafficking, and gambling. The limits of freedom of expression for employees, through the employer’s power to control the means of communication, as in the case of infringement of employees’ private electronic correspondence, is another matter of concern. It appears clear that penalization is sometimes difficult to put into practice. Such is the case with regard to technical obstacles. For instance, the identification of electronic culprits is difficult, or even impossible, with the present technology of information filtering and safeguarding of personal identity. Furthermore, an obvious question remains open concerning how to legally act when the authors of such malpractice live abroad, or when their actions (e.g., posting specific materials on a website) are totally legal in their own countries, but illegal in those from where access is possible. The fundamental issue is, thus, to overcome the paradoxical situation in which each national authority wishes to

limit access according to its own rules, while at the same time maintaining the freedom of expression and the right to personal privacy for each individual. A real example is the paradox between the Malaysia Multimedia Super Corridor's Bill of Guarantee (of no censorship on the content of the internet) and the distribution of pornographic materials to the public.

The use of multipurpose smart cards in many areas of human economic, social, political, and personal activities marks the beginning of a wide range of uses of personal information on a single card. These cards can contain data of the most sensitive kind about an individual. They may not only contain an individual's medical history and financial status, but also behavioural patterns and possibly even sex life. At the same time, they are used in a wide range of contexts and purposes other than clinical care and business transactions. The Human Right of respect for privacy requires that confidentiality of personal data should be guaranteed at all times. All users of personal data must be able to show a legitimate purpose in collecting and processing such data on individuals. The challenge is how to guarantee the legitimate collection and use of personal information about individuals and still honor the Human Rights philosophy?

Respect for security and privacy requires the use of encryption technology where appropriate, the use of closed networks for the transfer of personal data and organizational measures to support security. As personal data security is necessary, an Asia-Pacific region security standard should be observed wherever an electronic transfer of personal, identifiable, data occurs. Such transfers must be transparent and subject to evaluation by independent bodies.

The right of each individual to participate in the development and use of any system of private personal record-keeping is a key part of the concept of the citizen as stakeholder in democratic governance. The citizen must also been given access to any of his/her records that are kept electronically in databases. How many countries in Asia-Pacific recognize this right for their citizens?

4.6 Gender Equality

It is universally acknowledged that the ICT sector is the fastest growing area in the global economy, but the use of such technologies by women's organizations became noticeable only after 1995. As in most regions of the world, the spread and growth of ICT usage has been uneven across Asia and the Pacific. Women and men in different countries have not benefited equally. Women have to contend with ideological, systemic, and institutional barriers to access ICT (Cabrere-Balleza, 2002).

Getting reliable statistics on women's internet use in the Asia-Pacific region is very difficult. The standard indicators are not disaggregated by sex, and the available data is not very reliable or comparable. However, it is clear that the numbers are

small and the distribution limited. Most women ICT users in almost every developing country in the Asia-Pacific region are not representative of women in the country as a whole, but rather are part of a small, urban educated elite. The table below shows the percentage of women online, with South Korean women at 42 percent, in the 12 October 2000 survey by the Korean Information Centre.

Table 4.9. Women Online as a Percentage of the Total Internet Population

<i>Country</i>	<i>% of Women Online</i>	<i>Source</i>
Ethiopia	14	CABECA survey reported in World Bank (2000)
France	33.4	Media Metrix & Jupiter Communications; As of August 2000
Germany	31.7	Media Metrix & Jupiter Communications; As of August 2000
Latin America	38	Wall Street Journal
Senegal	17	CABECA survey reported in World Bank (2000)
<i>South Korea</i>	42	<i>Korean Network Information Centre, Reported in Nua Internet Surveys; Oct 12, 2000. http://www.nua.ie/surveys/?f=VS&art_id=905356101&rel=true</i>
Sweden	44.2	Media Metrix & Jupiter Communications; As of August 2000
United Kingdom	35.9	Media Metrix & Jupiter Communications; As of August 2000
United States	50.1	Media Metrix & Jupiter Communications; As of August 2000
Zambia	36	CABECA survey reported in World Bank (2000)

Source: S. Nanthikesan, Trends in Digital Divide, Harvard Centre for Population and Development Studies.

Table 4.10. Internet usage by working status (% of Internet users), year 2000, OEDC

<i>Working status</i>	<i>Information retrieval</i>	<i>email</i>	<i>e-commerce</i>	<i>Web pages</i>
Public workers	25.1	23.5	21.9	30.2
Private workers	28.7	32.9	34.4	32.1
Self-employed workers	17.9	17.1	15.5	22.6
<i>Housewives</i>	1.0	2.9	6.1	–
Students	18.5	18.2	15.8	11.3
Retired people	5.6	3.5	6.3	3.7

Source: Censis-Unicab.

Divide index *Divide index* *Divide index* *Divide index*
71.5 77.3 74.9 79.6

Table 4.11. Persons aged 10 and over who had used personal computer in the past 12 months by age and sex (Year 2000)

Age group	Male			Female			Overall		
	No. of persons ('000)	%	Rate*	No. of persons ('000)	%	Rate*	No. of persons ('000)	%	Rate*
10-14	155.8	11.6	73.0	147.8	11.4	72.6	303.6	11.5	72.8
15-24	339.2	25.2	76.1	374.8	29.0	81.7	713.9	27.0	78.9
25-34	348.2	25.8	63.6	407.1	31.5	66.2	755.3	28.6	65.0
35-44	347.1	25.8	48.6	286.0	22.1	40.4	633.0	24.0	44.5
45-54	127.5	9.5	25.2	66.8	5.2	14.6	194.4	7.4	20.2
55-64	25.9	1.9	9.1	9.1	0.7	3.7	35.0	1.3	6.6
>= 65	3.6	0.3	1.0	0.8	0.1	0.2	4.4	0.2	0.6
Overall	1 347.3	100.0	44.1	1 292.4	100.0	42.0	2 639.7	100.0	43.1

Source: Census and Statistics Department, Hong Kong.

Most women in Asia-Pacific region, especially in developing countries, use ICT only at work. Except in upper-income brackets, home access to an ICT is not a common phenomenon. Users at work generally divide up between those who use it as a tool of production (routine office work, data entry, manufacturing, computer industry jobs, programming, and related work) and those who use it as a tool of communication (creating and exchanging information).

But, time constraints, as well as bandwidth limitations, make Web use difficult for women. Few women are producers of ICT, whether as internet content providers, programmers, designers, inventors, or fixers of computers. In addition, women are also conspicuously absent from decision-making structures in ICT in the Asia-Pacific region, especially in the developing countries. Email is the major ICT application that women's organizations and individual women in developing countries use in the region. A series of factors, including literacy and education, language, time, cost, geographical location of facilities, social and cultural norms, and women's computer and information search, dissemination skills, as well as bandwidth limitations, constrain women's access to information and communication technology.

5. RECOMMENDATIONS

5.1 *Requirements for Holistic Integrated Policy and Framework*

Holistic, integrated, and cohesive policies need to be established at international, regional, and national levels to ensure effective and beneficial application of ICTs within the Asia-Pacific region, especially in the poorer and inadequately serviced areas. Given that different countries of the region have expertise in different parts of this new technology, collaboration efforts between countries in the region will bring greater benefits in the application of ICTs for development of the region. The most basic problems and challenges that public policymakers face trying to enhance ICT diffusion and development are the lack of both financial and trained human resources. The need for continuous collaboration in the development of ICT is vital. Recommendations in the following four areas are offered for collaborative work to ensure that the countries of Asia-Pacific are not left behind in embracing ICT for achieving competitive advantages:

1. Adoption of sound education programmes at all levels to 1) foster literacy, in general, and ICT literacy, in particular, 2) establish cybercrime free technology, and 3) provide for a secure information society within the region and info-sphere;
2. Promotion of human resource development programmes and collaborative Research & Development in priority areas of ICTs within each country and in the region as a whole;
3. Establishment of up-to-date, common, and mutually supporting cyber-laws for combating crime and protecting intellectual property rights towards the creation of cybercrime free information society, and to encourage further inventions and innovations to generate wealth; and
4. Adoption of ICT standards, regulations, and quality assurance to foster high quality and secure services and products that maintain competitiveness for the benefit of all communities within each country, in the region, and in the world.

5.2 *Addressing the Challenges*

5.2.1 **The Digital Divide**

Guarantee access by the greatest number of people to ICT facilities and services through the provision of:

- i. Basic infrastructure of electricity and communications to all rural and remote areas with special focus on rural areas utilizing the developing technology of wireless capabilities;

- ii. Community centres with basic hardware, software, access lines, and maintenance staff for free use by all underprivileged citizens regardless of age, gender, education, and social status;
- iii. Basic hardware, software, and access lines for all at affordable cost commensurate with local per capital incomes;
- iv. ICT facilities to guarantee computer literacy for every single pupil attending school;
- v. Special computer literacy programmes for underprivileged women and senior citizens;
- vi. Free access to the Internet in schools and public libraries;
- vii. Recognition in educational systems that computer literacy is a basic and necessary skill;
- viii. Multilingual content and interface to accommodate multilingual citizens of the world accessing common knowledge; and
- ix. Ensuring that ICT is not used to discriminate against, or disadvantage, those who would not or cannot participate (e.g. replacing humans with ATM's).

5.2.2 Human Rights

Adoption of common policies and principles for the information society in terms of:

- i. Freedom of expression and freedom of the press, with due respect to laws, order, and the common interest of every person;
- ii. Free, compulsory and universal primary education with special emphasis on ICT literacy;
- iii. Promotion of public domain information portals, services, and networks accessible to all;
- iv. Encouragement of public involvement in the development process of public ICT systems and services; and
- v. Opportunities for all to distance education and life-long learning opportunities offered by ICT.

5.2.3 Cybercrime

Provision of cyber-laws and enforcement through the attainment of the following goals (see Appendix A):

- i. High levels of awareness of information security and cybercrime issues amongst users at home, in government and educational institutions, in the private sector, and amongst legal officers;

- ii. Increased exchange of information on information security and cybercrime at the regional and national levels;
- iii. Policies and legal and regulatory frameworks at the national level that are consistent with existing or developing international legal instruments;
- iv. Effective regional mechanisms for preventing cybercrime and improving protection against, detection of, and responses to, cybercrime;
- v. Secure information systems, networks and transactions in the public and private sectors;
- vi. Safe and secure environments for users, especially children and young persons;
- vii. Effective mechanisms for detection of, and responses to, cybercrime at the national and regional levels, including the creation of environments that are conducive to the reporting of cybercrime;
- viii. Widespread adoption of, and compliance with, relevant codes of conduct and best practices at the national level; and
- ix. Increased capacity to conduct domestic electronic investigations and to assist with trans-national investigations.

5.2.4 Poverty

Global poverty can be reduced through the promotion of ICT programmes to the underprivileged as follows:

- i. Awareness programmes emphasizing the importance of ICT in the knowledge economy;
- ii. Providing access to ICT infrastructure, content, and services available;
- iii. Providing training of knowledge and skills in using ICT; and
- iv. Promoting utilization of facilities provided by ICT in wealth creation through e-commerce and services industries.

5.2.5 Piracy

Promotion of anti-piracy programmes through the following actions:

- i. Promotion of fundamental understanding of the destructive nature of piracy in terms of hindering the following: the progress in the ICT industry, wealth creation, employment opportunities, knowledge creation, and national status and reputation;
- ii. Regulation and control of software prices commensurate with national per capital incomes;
- iii. Enforcement of penalties for crimes committed against copyright and intellectual property protection laws; and

- iv. Encouragement of indigenous ICT to maintain availability of software products at local affordable price.

5.2.6 Gender Equality

Promotion of fair and equal access to ICT infrastructure, content, and services for human development, regardless of gender, through:

- i. Provision of awareness programmes on the importance of ICT in the knowledge society for disadvantaged, handicapped, and gender groups within each country, especially in underserved areas;
- ii. Provision of basic facilities to train basic skills and provide access to gender group;
- iii. Empowerment of gender group to be independent and able to take advantage of the benefits obtained from mastering skills in the application of ICT.

References

- Abas, G. 2001. ICT in Malaysia: Policy, Regulation & Industry Progress (1996-2000) and Prospects (2001-2005) Gazali Abas, ITU-Waseda University workshop for Regulations and Policymakers: “New Trends in ICT” 13-14 November 2001. Waseda University Tokyo, Japan.
- Borje, A.J. 2002. Cybercrime and Information Security in the Philippines, Country Report, Asia-Pacific Conference on Cybercrime and Information Security Seoul, Republic of Korea 11-13 November 2002, http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/Presentations/Session%203%20country%20and%20org.%20reports/Philippines/cybersecurity%20Philippines.ppt.
- Broadhurst, R. 2002. E-commerce & Cybercrime: issues, problems & prevention. Asia-Pacific Conference on Cybercrime and Information Security, Seoul, Republic of Korea, 11-13 November 2002.
- Bryneson, M. 2002. Sexual exploitation on the Internet. Asia-Pacific Conference on Cybercrime and Information Security, 10-12 November 2002, Seoul, Republic of Korea.
- BSA Global Software. 2001. Pricy Study. Sixth Annual BSA Global Software.
- Cabrere-Balleza. 2002. Women’sNGO@asia-pacific.net: ICT and Gender Issues in Asia and the Pacific, Know How Conference, Kampala, Uganda.
- Cha, Y. 2002. The Republic of Korea’s policies and strategies for enhancing information security. Asia-Pacific Conference on Cybercrime and Information Security, Seoul, Republic of Korea 11-13 November 2002.

- http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/Presentations/Session%202%20-%20Info.%20security%20-%20Korea/Yang-shin/Yang-shin%20Cha%20-%20Information%20Security%20Policy%20in%20Korea.ppt
- Chan, K.W. 2002. INFOCOMM security, Country Report on Singapore, Asia-Pacific Conference on Cybercrime and Information Security Seoul, Republic of Korea 11-13 November 2002. http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/
- CSI. 2003. CSI/FBI Computer Crime and Security Survey. Computer Security Institute.
- G8. 2002. Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations. G8 Justice and Interior Ministerial. USA. http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Fight_against_terrorism/Texts_&_documents/
- Johnson, D.G. 1994. *Computer Ethics*, second edition; Englewood Cliffs, NJ, Prentice Hall.
- Kaewjumnong, S. 2002. Thailand Country Report on Cybercrime and Information Security, Asia-Pacific Conference on Cybercrime and Information Security Seoul, Republic of Korea 11-13 November 2002. http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/Thailand/Thailand.doc
- Laudon, K. 1995. "Ethical Concepts and Information Technology," *Communications of the ACM*, December 1995 p 33-40.
- Laudon, K.C., Traver, C.G. and Laudon J.P. 1996. *Information Technology and Society*, pp.513.
- Mongolia. 2002. Asia-Pacific Conference on Cybercrime and Information Security Seoul, Republic of Korea 11-13 November 2002. http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/
- NiDA, National Summit on ICT Policy and Strategy, July 3rd 2003, Phnom Penh, Cambodia. <http://www.nida.gov.kh>
- PRC. 2002. The current situation of cybercrime and the countermeasures. Information Security Supervision Bureau of Ministry of Public Security of P.R.C. Asia-Pacific Conference on Cybercrime and Information Security, Seoul, Republic of Korea 11-13 November 2002. http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/China/China.ppt
- Tatsuzaki, M. 2002. Cyber Crime: Cross Border Enforcement in Cyber World. Transnational Organized Crime Conference, 19 March 2002.

- UNESCAP. 2002. Afghanistan Country Report. Asia-Pacific Conference on Cybercrime and Information Security Seoul, Republic of Korea 11-13 November 2002. http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/
- UNESCAP. 2002. Asia-Pacific Conference on Cybercrime and Information Security 11-13 November 2002, Seoul, Republic of Korea. (UNESCAP) Asia-Pacific Conference on Cybercrime and Information Security 11-13 November 2002, Seoul, Republic of Korea.
- UNESCAP. 2002. Vietnam Information Security and Anti – Cybercrime. Asia-Pacific Conference on Cybercrime and Information Security Seoul, Republic of Korea 11-13 November 2002. http://www.unescap.org/escap_work/ict/Cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/Vietname/Viet%20Nam.doc
- Yamaguchi, S. 2002. Joint efforts in incident response in AP region and future work with RIR, <http://www.apnic.net/meetings/14/sigs/db/docs/db-pres-suguru-apcert.ppt>

Websites (accessed during the period of July to October 2003):

- Ananova, <http://www.ananova.com/news/story/>
- Apec Telecommunications And Information Working Group Report On Economy Implementations of the Ten Measures Included In United Nations General Assembly Resolution 55/63 Combating the Criminal Misuse Of Information Technologies.
- Creating a Development Dynamic, Final Report of the Digital Opportunity initiative, Accenture, Markel Foundation & the United Nations Development Programme (UNDP). July 2001, <http://www.opt-init.org/framework/pages/appendix3Case5.html>
- Creating a Development Dynamic, Final Report of the Digital Opportunity initiative, accenture, Markel Foundation, & the United Nations Development Programme (UNDP). July 2001, <http://www.opt-init.org/framework/pages/appendix3Case5.html>
- Duggal, <http://www.cyberlaws.net/cyberindia/articles.htm>
- e-Japan Priority Policy Programme <http://www.kantei.go.jp/foreign/it/network/priority-all/index.html> March 29, 2001.
- e-Japan Priority Policy Programme <http://www.kantei.go.jp/foreign/it/network/priority-all/index.html> March 29, 2001.
- FIRST, <http://www.first.org/about/first-description.htm>

- General Manager, Industry Development Division, Malaysian Communications and Multimedia Commission. <http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf>
- INFOethics '98. Ethical, Legal and Societal Challenges of Cyberspace. Second International Congress (Monte-Carlo, Principality of Monaco, 1-3 October 1998) http://www.unesco.org/webworld/public_domain/legal.html
- IT TAKES MORE THAN ETHICS AICE2000 CONFERENCE PAPER by Chris Simpson <http://www.cm.deakin.edu.au/AICE/aice2000/sim.pdf> (09 October 2000).
- Leveraging Effective Ict Strategies For Sustainable Development. A Regional Initiative for Information and Communications Technology Strategies (RIFICTS) Putra World Trade Centre Kuala Lumpur, Malaysia (COMNET-IT). <http://www.comnet-it.org/strategies/criis2001/ma2001-w.pdf>
- Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (Summary) http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html
- The Japan Times, <http://www.japantimes.co.jp/>
- <http://www.apectelwg.org/apec/are/telmin5sub08.htm>
- <http://www.auscert.org.au/render.html?cid=2>
- http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html
- <http://www.nitc.org.my/resources/cyberlaw.shtml>
- <http://www.obi.giti.waseda.ac.jp/ITU/2001/Malaysia.pdf>
- http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Appendix A

Recommended Supporting Actions (Adopted at the Asia-Pacific Conference on Cybercrime and Information Security, held from 11 to 13 November 2002, in Seoul, Republic of Korea)

<i>Goal</i>	<i>Actions to Achieve Goal</i>	<i>Relevant initiatives and organizations that may cooperate</i>
<i>I. Increased stakeholder awareness and transfer of knowledge.</i>		
<p>1. High levels of awareness of information security and cybercrime issues amongst users at home, in government and educational institutions, in the private sector, and amongst legal officers.</p>	<p>1.1 Conduct national user awareness campaigns for the general user, including children and young people, educational institutions, consumers, government officials and the private sector, using different media.</p> <p>1.2 Target the media. Educate media professionals, and then encourage them to increase public awareness.</p> <p>1.3 Engage large private sector corporations and industry associations in the sponsorship of awareness programmes.</p> <p>1.4 Promote the concept of “Ethics for the Information Society.”</p> <p>1.5 Conduct seminars for high-level authorities (prime ministers, ministers and other senior government officials and legislators). Programmes should be tailored to requirements in each country.</p> <p>1.6 Support/initiate/expand capacity building programmes, including, in particular, national and regional professional workshops for the judiciary and other legal officers including those in NGOs, as well as specialist training in the field of information security. Use existing materials (e.g. material developed by APEC) adapted for local requirements and languages.</p> <p>1.7 Advise less developed countries on effective systems for protection against, detection of and responses to, cybercrime.</p> <p>1.8 Strengthen national crime prevention strategies and programmes by supporting the inclusion of broad, multi-targeted measures to prevent cybercrime.</p>	

<i>Goal</i>	<i>Actions to Achieve Goal</i>	<i>Relevant initiatives and organizations that may cooperate</i>
<p>2. Increased exchange of information on information security and cybercrime at the regional and national levels.</p>	<p>2.1 Establish appropriate regional mechanisms to increase exchange of information on cybercrime and information security issues and activities between APEC and other regional cooperation secretariats.</p> <p>2.2 Establish national cybercrime and information security councils that include the participation of all stakeholders – the private sector, government authorities, telecommunications service providers, law enforcement officials, the judiciary, NGOs and others.</p> <p>2.3 Where appropriate, establish 24-hour points of contact between government and industry at the national level.</p>	<p>APEC ASEAN</p>
<p><i>II. Improved policy, legal and regulatory frameworks for promoting information security and addressing cybercrime.</i></p>		
<p>3. Policy, legal and regulatory frameworks at the national level that are consistent with existing or developing international legal instruments and that provide for proportionate and dissuasive sanctions, including deprivation of liberty.</p>	<p>3.1 Make “best practice” legislation and guidelines available, consistent with existing or developing international legal instruments such as the Council of Europe Convention on Cybercrime, the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.</p> <p>3.2 Provide technical assistance to governments to enable them to review and assess existing policies, laws and practices relating to cybercrime and information security.</p> <p>3.3 Maintain a detailed compendium of new and existing legislation in the Asia-Pacific region that impacts on information security.</p> <p>3.4 Encourage proactive, self-help approaches by the private sector, and enhance its willingness to assist in law enforcement investigations.</p>	<p>WIPO</p>

<i>Goal</i>	<i>Actions to Achieve Goal</i>	<i>Relevant initiatives and organizations that may cooperate</i>
<i>III. Establishment of regional mechanisms to improve cybersecurity.</i>		
4. Effective regional mechanisms for preventing cybercrime and improving protection against, detection of, and responses to, cybercrime.	4.1 Establish a regional standing group/ committee/network of experts to provide advice and give appropriate inputs, as well as act as a focal point or help desk for requests for assistance from developing countries, and establish a website in support of this activity. 4.2 Establish a Regional Information Security Centre. 4.3 Establish sub-regional CERTs covering several countries where necessary. 4.4 Establish a regional CERT Network. 4.5 Establish a regional mechanism for the exchange of information and experience. 4.6 In general, involve academia and establish private sector partnerships (in line with the UN Global Compact). Coordinate and consolidate initiatives to avoid duplication.	
<i>IV. Increased protection against cybercrime.</i>		
5. Secure information systems, networks and transactions in the public and private sectors.	5.1 Make information regarding IT security standards and international best practices relating to information security available to governments and the private sector. 5.2 Facilitate greater sharing of information and capacity-building relating to the APEC secretariat's work on IT security standards, in particular its work in best practices. 5.3 Share information on IT security professional certification and provide support for the development of the IT security professional workforce in less developed countries. 5.4 Identify and promote measures for encouraging and assisting companies and other legal entities to adopt minimum levels of systems and transaction security, including codes of conduct and other measures that assist the private sector to be more accountable for harm to governments, businesses and individuals.	APEC – e-security Task Group and the HRD steering group project ASEAN

<i>Goal</i>	<i>Actions to Achieve Goal</i>	<i>Relevant initiatives and organizations that may cooperate</i>
	5.5 Support governments in the establishment of national information security policies, procedures and practices that facilitate international assistance in combating cybercrime.	
6. Safe and secure environments for users, especially children and young persons.	6.1 Promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children, such as walled gardens.	ECPAT International
<i>V. Improved detection of, and responses to, cybercrime</i>		
7. Effective mechanisms for detection of, and responses to, cybercrime at the national and regional levels, including the creation of environments that are conducive to the reporting of cybercrime.	<p>7.1 Establish or strengthen Computer Emergency Response Teams (CERTs) where they do not exist, or where they require upgrading.</p> <p>7.2 Establish national hotlines for reporting cybercrime, in cooperation with the private sector and NGOs.</p> <p>7.3 Develop, disseminate and promote guidelines for consumer protection in the context of electronic commerce.</p>	OECD (Council Consumer Guidelines – December 1999)
8. Widespread adoption of, and compliance with, relevant codes of conduct and best practices at the national level.	<p>8.1 Develop, disseminate and promote relevant codes of conduct and best practices for users and suppliers of ICT, in support of the concept of “Ethics for the Information Society.”</p> <p>8.2 Promote self-regulation in the private sector.</p> <p>8.3 Ensure that codes of conduct and best practices are reflected in the criminal procedure laws of the country, where appropriate.</p>	ECPAT International INTERPOL

<i>Goal</i>	<i>Actions to Achieve Goal</i>	<i>Relevant initiatives and organizations that may cooperate</i>
<p>9. Increased capacity to conduct domestic electronic investigations and to assist with transnational investigations.</p>	<p>9.1 Increase focus on cybercrime issues in existing and proposed mutual assistance regimes, along the lines of the Council of Europe Convention on Cybercrime.</p> <p>9.2 Support the development of operational mechanisms and procedures for mutual assistance, for example, through the expansion of participation of less developed countries in existing cooperation frameworks such as the G-8 24/7 network.</p> <p>9.3 Provide technical assistance for the establishment of specialized units within government for addressing cybercrime and information security.</p> <p>9.4 Establish/strengthen/promote mechanisms for the exchange of information on cyber forensic tools, techniques and methodologies.</p>	<p>G-8 Network for 24/7 assistance</p> <p>International Organization on Computer Evidence</p>
	<p>9.5 Produce guidelines on cybercrime issues.</p> <p>9.6 Develop a webpage of cybercrime links (regional and national).</p> <p>9.7 Encourage acceptance of, and compliance with, international legal instruments such as the Convention on Transnational Organized Crime, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, the WIPO treaties relating to the protection of intellectual property rights and the Council of Europe Convention on Cybercrime.</p> <p>9.8 Encourage the development of low-cost systems for protection against, detection of, and responses to cybercrime, based on open-source solutions, including the development of technology that facilitates the surveillance of unlawful or harmful misuse of computers.</p>	<p>APEC (Electronic Authentication issues paper)</p>

Appendix B
Benchmarking: ICT Indicators

<i>Country</i>	<i>Daily Newspapers Per 1 000 People 1996</i>	<i>Radios Per 1 000 People 1996</i>	<i>Television Per 1 000 People 1997</i>	<i>Telephone Mainlines Per 1 000 People 1999</i>	<i>Mobile Telephones Per 1 000 People 1999</i>	<i>Personal Computers Per 1 000 People 1999</i>	<i>Internet Host Per 1 000 People 1999</i>
Argentina	123	677	289	213.8	109.72	59.9	3.08
Brazil	40	435	316	152.2	84.70	52.9	1.93
Hong Kong, SAR	800	695	412	559.6	551.02	360.2	66.40
Finland	455	1 385	534	557.2	678.10	507.8	117.25
Indonesia	23	155	134	29.1	9.83	13.4	0.18
Ireland	153	703	455	472.4	360.59	352.6	15.95
Korea	394	1 037	341	449.7	499.04	181.3	6.03
Malaysia	163	432	166	219.3	145.05	94.5	2.80
Philippines	82	159	109	37.9	36.97	19.5	0.23
Singapore	324	739	354	484.1	381.45	390.9	22.19
South Africa	30	316	125	126.9	101.06	54.1	4.21
Thailand	65	204	234	84.5	39.57	40.4	0.49

Source: World Development Report, 1999/2000.
World Competitiveness Yearbook, 2000.

Appendix C
Ranking Among Selected Nations

High	1	Finland	2	1	1	2	1	1	1	9
	2	Hong Kong	1	5	3	1	2	3	2	17
	3	Singapore	4	3	4	3	4	2	3	23
	4	Korea	3	2	5	5	3	5	5	28
	5	Ireland	6	4	2	5	5	4	4	30
Medium	6	Argentina	7	6	7	7	6	7	7	47
	7	Malaysia	5	8	9	6	8	6	8	50
	8	Brazil	10	7	6	8	9	8	9	57
	9	South Africa	11	9	11	9	7	9	6	60
Low	10	Thailand	9	10	8	10	10	10	10	67
	11	Philippines	8	11	12	11	11	11	11	75
	12	Indonesia	12	12	10	12	12	12	12	82

Source: NITC Estimates, 2000.

Appendix D
ICT Diffusion

ICT diffusion in selected Asian economies
(per thousand people)

<i>Economies</i>	<i>Telephone mainlines (1999)</i>	<i>Cellular phones (1999)</i>	<i>Personal computers (1999)</i>	<i>Internet users (2000)</i>
Developing Asia				
Bangladesh	3.4	1.2	1.0	0.2
China	85.8	34.2	120.0	13.4
India	26.6	1.9	3.3	4.5
Indonesia	29.1	10.6	9.1	1.8
Kazakhstan	108.2	3.0	n.a. ^a	4.2
Kyrgyzstan	76.2	0.6	n.a. ^a	2.1
Malaysia	203.0	137.0	68.7	68.8
Nepal	10.6	n.a. ^a	2.6	1.4
Pakistan	22.2	2.1	4.3	8.5
Philippines	39.5	36.6	16.9	6.2
Sri Lanka	36.4	12.2	5.6	3.4
Thailand	85.7	38.4	22.7	16.5
Vietnam	26.8	4.2	8.9	1.3
Industrial and newly industrializing economies				
Japan	494.0	449.4	289.6	213.8
Hong Kong, SAR	577.5	636.1	290.5	260.0
Singapore	482.0	418.8	527.2	419.1
Rep. of Korea	441.4	504.4	189.2	323.1
Taipei, China	545.2	522.4	180.7	288.4
United States ^b	681.8	311.5	510.5	537.2

Data sources: International Telecommunication Union (2000) and Nua Internet Surveys (2000).

^a n.a.: data not available.

^b Estimates for the United States were included in the table for purposes of comparison.

Human Development in the ASEAN Countries

<i>Country</i>	<i>Human development rank (2001)</i>	<i>Human development index (2001)</i>	<i>Life expectancy at birth (1999)</i>	<i>Adult literacy rate (1999)</i>	<i>GDP per capita USD (1999)</i>	<i>Technology achievement index (1999)</i>
Singapore	26	0.876	77.4	92.1	20 767	0.585
Malaysia	56	0.774	72.2	87.0	8 209	0.396
Thailand	66	0.757	69.9	95.3	6 132	0.337
Philippines	70	0.749	69.0	95.1	3 805	0.300
Vietnam	101	0.682	67.8	93.1	1 860	–
Indonesia	102	0.677	65.8	86.3	2 857	0.211
Myanmar	118	0.551	56.0	84.4	1 027	–
Cambodia	121	0.541	56.4	68.2	1 361	–
Lao PDR	131	0.476	53.1	47.3	1 471	–