UIC John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 2 *Journal of Computer & Information Law - Winter 2005*

Article 2

Winter 2005

Law and Order in Cyberspace: A Case Study of Cyberspace Governance in Hong Kong, 23 J. Marshall J. Computer & Info. L. 249 (2005)

Kam C. Wong

Georgiana Wong

LAW AND ORDER IN CYBERSPACE: A CASE STUDY OF CYBERSPACE GOVERNANCE IN HONG KONG

DR. KAM C. WONG† AND GEORGIANA WONG††

I. INTRODUCTION

Hong Kong, as an international finance center, has been enjoying great benefits generated by computer-mediated communication ("CMC") in the new Information Age, particularly so when networks are connected by the Internet. CMC is much faster, cheaper, and relatively effortless as compared to traditional communication channels, such as letter or facsimile. With a click of a mouse, people can share a large amount of information and process business transactions almost instantaneously. People are brought closer together in a virtual world that surpasses geographical distance, time zones, social inhibitions, and cultural barriers. For example, the Internet allows people to communicate with each other in real time, anonymously and anywhere in multifarious and interactive ways. Cyberspace has its own norms and culture that are very different from the real world. Social conventions must give way to computer etiquette that is known to be casual, informal and spontaneous.

---

† Associate Professor, Law and Criminal Justice, Department of Public Affairs, University of Wisconsin (Oshkosh). J.D. (Indiana), Ph.D. (SUNY-Albany, Criminal Justice). Managing Editor, Police Practice and Research: An International Journal. His publications appeared in British Journal of Criminology, Australian and New Zealand Journal of Criminology, Columbia Journal of Asian Law, International Journal of the Sociology of Law, Journal of Law and Society, Georgetown Journal of Law and Public Policy and others.

†† Georgiana Wong is a senior executive of an international computer firm with 20 years of experience in information technology. Her extensive knowledge in the IT business applications and the rapid growth of Internet usage has prompted her to pursue research studies in the area of computer crime and cyberspace governance. Georgiana holds a Master of Social Science in Law and Public Affairs and a Bachelor of Arts in English Literature from The Chinese University of Hong Kong as well as a Master of Science in Computing (University of Ulster) and Master of Business Administration (University of Macau). She is an independent researcher and has co-authored with Dr. Kam Wong several papers on cyberspace studies in PRC and Hong Kong.

With the rapid and advanced development in technology, Hong Kong's economy is increasingly and irreversibly relying, and made dependent upon CMC and the Internet to operate, because the Internet has become a catalyst of reform and development in other arenas including social, cultural, and public policy. The amount of financial information, government information, proprietary business data, and personal communications transmitted by and stored on computers is beyond imagination.[1] As Marjory Blumenthal, a perceptive scholar of the U.S. National Research Council observed, "[a]s the [21st century] begins, attention grows to the potential of the Internet as a public space, with implications not only for purposeful activity (business, education, and so on) but for personal activity, including social interaction and play."[2] The influence and implications of the Internet in Hong Kong go far beyond what had been originally contemplated and penetrate into layers of the society that we have yet to recognize. The Internet is still a history in the making.

The Information Age raises new criminality concerns as it aggregates traditional criminal problems. CMCs are vulnerable to attack by hackers and computers can be used to defraud people and businesses of millions of dollars. Tiny computer viruses have the capability to bring down multinational corporations.[3] In other words, computers connected to the Internet facilitate traditional criminality and bring new crimes of different types.

Similar to many developed societies, the phenomenal growth in the usage of CMC and the Internet in Hong Kong has been accompanied by an increase in computer-related crime since the late twentieth century.[4] The study of cyberspace governance in Hong Kong is still at its early stage. As yet, there are limited scholars or policy makers who have taken the challenge to conduct a comprehensive study on the subject. Academic publications on cyberspace governance in Hong Kong are rare. This paper is an attempt to fill in the research gap.

---

1. *See* Census and Statistics Department, *Hong Kong as an Information Society*, http://www.statisticalbookstore.gov.hk (accessed Apr. 30, 2005) (providing more survey statistics).

2. *See* Marjory S. Blumenthal, *Communications and Computers, Encyclopedia of Computer Science* 243-250 (Nature Publishing Group, 4th ed. 2000).

3. *See* David Icove, Karl Seger, & William VonStorch, *Computer Crime: A Crimefighter's Handbook* 5-15, 17-21 (O'Reilly & Associates, Inc. 1995) (for details on types of computer attacks and vulnerabilities); *see also* Kam C. Wong & Georgiana Wong, *Law and Order in Cyberspace: A Case Study of Cyberspace Governance and Internet Regulations in PRC, Proceeding Papers, Third Annual Conference of the Asian Association of Police Studies (AAPS)* (Hong Kong, 2002) (for similar work by the author) (copy of transcript on file with the author).

4. See Table 3 for Computer Crime Cases in Hong Kong reported from 1996 to 2003.

This project investigates into, and reports upon, computer-related crime and control in Hong Kong. Particularly, we will investigate the following questions in relation to cyberspace governance in the geographic region:

- Is there a computer crime problem in Hong Kong?
- What is the nature of the computer crime problem? – Prevalence, kind, distribution?
- What are the causations of the computer crime problem?
- Given our understanding of the computer crime problem, what actions have been taken by the Hong Kong government in addressing the issue?
- Are the control measures excessive or deficient?

This paper consists of seven sections. Section I, "Introduction," highlights the social implications of a new criminality created by the Internet. Section II, "Researching into Hong Kong Cyberspace Governance," informs the readers on research difficulties and data sources. Section III, "Information Technology Usage and Penetration in Hong Kong," describes, in statistical form, the trend of IT usage and Internet popularity in Hong Kong. Section IV, "Nature, Prevalence and Distribution of Computer Crime," provides an overview of the background, i.e. the nature, extent, and distribution, of computer crime in Hong Kong. Section V, "Cyberspace Governance in Hong Kong," explores and seeks to understand the policy, theory, legislative, law enforcement, and preventive measures through education. Section VI, "Regulating Cyberspace: Hyperbole or Ellipsis?," investigates the question on whether the Hong Kong government's regulation of the Internet is excessive or deficient. Section VII, "Conclusion," summarizes the report's key findings and suggests various recommendations to improve the cyberspace governance in Hong Kong.

II. RESEARCHING INTO HONG KONG CYBERSPACE GOVERNANCE

A. Research Difficulties

There are three major problems and issues with researching into cyberspace governance in Hong Kong: 1) defining computer crime; 2) fully understanding the extent of computer crime in Hong Kong's society; and 3) generating the needed empirical data. Failure in addressing these challenges will diminish our capability in generating a valuable contribution to effective measures in dealing with cyberspace's disorder.

First, although there is no commonly agreed definition of what computer crime entails, it is a worldwide issue that, with no exception, impacts relevant studies of the subject in Hong Kong. Computers connected to the Internet facilitate traditional criminality and bring new

and different types of crime. The term computer crime is generally referred to as three kinds of crime: 1) computer crime in the strict sense; 2) computer-related crime; and 3) computer abuse. A guru of computer security in the United States, Donn B. Parker has suggested a description of computer crime:

> Computer crime may involve computers not only actively but also passively when usable evidence of the acts resides in computer storage. The victims and potential victims of computer crime include all organizations and people who are affected by computer and data communication systems, including people about whom data is stored and processed in computers.[5]

According to Parker's definition, computer crime cases may involve computers in one or more of the following roles: 1) Object (such as destruction of computers or computer data or programs contained in a computer); 2) Subject (such as fraud cases where financial data being illegally changed); 3) Instrument (such as using the computer actively in search of passwords and credit card numbers, or passively in the course of a continuing financial embezzlement); and 4) Symbol (such as using nonexistent computers for intimidation or deception).[6]

In practice, it is never too easy, straightforward, or unproblematic to define computer crime.[7] For example, if a computer is stolen, it would not be classified as a computer crime; however, if knowledge of computer technology is used to commit a crime, such as an unauthorized electronic transfer of funds, it is readily considered a computer crime. Yet, both are stealing under the common law definition, that is, the "taking, carrying away, property of another, with intent to permanently deprive the owner thereof."[8] There are many varieties, in new and changing forms, of illegality emerging from computer crime such as theft or illegal interception of telecommunication services, child pornography on the Internet, information piracy, dissemination of offensive materials, online shopping theft, e-banking fraud, and electronic sales fraud.[9]

Second, Hong Kong faces a challenge in fully understanding the ex-

---

5. *See* Donn B. Parker, *Computer Crime, Encyclopedia of Computer Science* 349-353 (4th ed. Nature Publishing Group 2000).

6. *Id.* at 351.

7. Unless otherwise specified, the terms, 'computer crime,' 'computer-related crime,' 'computer abuse,' and 'Internet crime,' are used interchangeably throughout this paper.

8. *See* Parker, *supra* n. 3, at 349-353 (for problems and issues with defining computer crime); *see also* Ronald B. Standler, *Computer Crime*, http://www.rbs2.com/ccrime.htm (1999); *see also* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, http://www.eff.org/%7Ebarlow/ Declaration-Final.html (1996).

9. *See* Peter Grabosky, Lecture, *The Global and Regional Cyber Crime Problem, Proceedings of the Asia Cyber Crime Summit* (Hong Kong, Apr. 25, 2001) (for detailed descriptions on varieties of computer-related crime) (copy of transcript on file with the author).

tent of computer crime in its community.[10] It is well recognized in other countries that there are always dark figures in cyberspace crime, i.e. undiscovered and/or unreported crime cases. For example, the FBI's National Computer Crime Squad estimates that between eighty-five and ninety-seven percent of computer intrusions in U.S. are not even detected.[11] With sponsorship from the U.S. Department of Defense, Richard Power conducted a test to attack a total of 8,932 computer systems participating in the study. The management of only 390 systems detected the attack; among them only nineteen of the managers reported the attacks.[12] Hong Kong faces similar problems of dark figures in tracking statistics of computer crime. Attempting a cyber-crime typically requires sophisticated knowledge and a technical know-how of the invisible offender committing the illegal act in virtual space, causing unexpected damage and/or inconvenience to the victims. In most cases, the victims are not even aware of the impact to them, or perhaps, come to realize the loss after a prolonged period of time. Even if said victims are aware of the damage, they may not choose to report the case to the police. As with other crimes, many reasons exist for victims to not report computer misuse, but there are other specific considerations. Unless unavoidable, many corporations, especially those in service sectors such as finance and insurance industries, are reluctant to report a cyber-crime case due to a fear of jeopardizing their corporate image and credibility. Besides, many Hong Kong people in business sectors tend to believe that it is more effective, quicker, and less costly to settle a dispute outside the Court, if they think they can manage.

The rare treatment of computer crime as a distinct subject, coupled with the problem of dark figures described above, has created hurdles for us to understand the magnitude and significance of the problem. This leads to the third issue of our research problems—the need for empirical data and analysis. Today, the Hong Kong Police Force ("HKP") releases computer crime statistics to the public on the government security information ("InfoSec") website managed by the Office of the Government Chief Information Officer ("OGCIO").[13] Technology crime statistics since 2000 are available at the HKP Web site but not categorized in cyber-

10. *See* Kam C. Wong, Lecture, *Introduction: Asian Policing in the 21st Century, Proceeding Papers, Third Annual Conference of the Asian Association of Police Studies*, (Hong Kong July 29, 2002) (for an extensive discussion on the challenges in policing computer crime in Hong Kong) (copy of transcript on file with the author).

11. *See* Icove, *supra* n. 3, at 3.

12. *See* Icove, *supra* n. 3, at 3; *see also* Jiang Ping, *Jisuanji Fanzui Wenti Yanjiu* 105-107 (Commercial Press 2000) (providing research into computer crime problems).

13. *See* Hong Kong Special Administrative Region of The People's Republic of China, *InfoSec - Information Security & Prevention of Computer Related Crime*, http://www.infosec.gov.hk/engtext/ general/crc/statistics.htm (accessed Apr. 30, 2005).

crime details.[14] There is little visibility on the cases handled by the Customs and Excise Department.[15] Two things are certain—the available statistics do not present a total picture of computer crime in Hong Kong, and we are just looking at the tip of the iceberg. How many computer crimes are out there in totality? What are the crime categories and degrees of significance? How are computer crimes distributed in the social space, such as the age group and education level of the offenders? More importantly, what are the causes behind computer criminalities and what are the social impacts? Answers to these questions will very likely lead to a different set of computer crime measures adopted by the Hong Kong government. We'll address these questions in the later sections of this paper.

B. Data Sources

The data used in this article comes mainly from publications of the Census and Statistics Department, the Security Bureau, and the HKP of the Hong Kong Special Administrative Region ("HKSAR"). The HKSAR government information Web sites are open to the public.[16] The Security Bureau is one of the key players in the policy formation process of cyberspace governance in Hong Kong. In March 2000, the Security Bureau chaired an inter-departmental working group ("Working Group") "to examine existing legislation and related issues regarding computer crime"[17] in Hong Kong. Soon after, the Inter-departmental Working Group on Computer-Related Crime Report (September 2000) ("Report") was issued. In July 2001, the HKSAR government announced adoption of the suggestions recommended by the Working Group.[18] The Report is extremely instrumental for policy research in computer crime and it provides significant reference for studying the policy direction adopted by the HKSAR in cyberspace governance. Computer crime statistics are quoted primarily from the HKP Web sites on "Information Security & Prevention of Computer Related Crime."[19] Crime cases are cited from

14. *See* HKP, *Technology Crime Statistics in Hong Kong*, http://www.info.gov.hk/police/hkp-text/english/tcd/overview.htm (accessed Apr. 30, 2005).

15. *See* Customs and Excise Department, *Statistics*, http://www.customs.gov.hk/eng/statistics_e.html (visited 30 April 2005).

16. Hong Kong Special Administrative Region of The People's Republic of China, http://www.info.gov.hk (accessed Apr. 1, 2005) [hereinafter HKSAR].

17. *See* Legislative Council Brief, *Panel on Security, LegCo Brief on Inter-departmental Working Group on Computer Related Crime: Report and Recommendations* ¶ 2, http://www.legco.gov.hk/yr00-01/english/panels/se/papers/mis1059.pdf (Nov. 30, 2000) [hereinafter *LegCo*].

18. Hong Kong Government Press Release, *Government Initiatives to Combat Computer Crime*, http://www.info.gov.hk/gia/general/200107/16/0716105.htm (July 16, 2001).

19. *See* Hong Kong Special Administrative Region of The People's Republic of China, *General Information Corner*, http://www.infosec.gov.hk (last updated Jan. 2005).

HKP or local news media. Statutory Laws of Hong Kong are adopted from the Bilingual Laws Information Systems ("BLIS"), the database of the Laws of Hong Kong on Internet, serviced by the Department of Justice. Reference is also made to the proceeding papers of two distinct international conferences held in the territory: the First Asia Cyber Crime Summit[20] and the Third Annual Conference of the Asian Association of Police Studies.[21] These conferences were hosted by two of the prominent professional organizations in the field and contributed valuable insights directly relevant to this research.

III. INFORMATION TECHNOLOGY USAGE AND PENETRATION IN HONG KONG

In his 2001 Policy Address, the Chief Executive of HKSAR stated the urgent need for the community to rapidly transform from an industrial economy to a knowledge-based economy:

> Nevertheless, if we are to preserve our economic vitality, create greater prosperity, and maintain living standards, economic restructuring is the only way . . . . We are encouraging traditional industries to use technology and innovation to improve competitiveness . . . . The importance of electronic commerce is increasingly being recognized . . . we announced our revised 'Digital 21' IT strategy to promote the development of e-commerce under the theme 'connecting the world.'[22]

In his 2003 Policy Address, he re-emphasized the importance of "enhanc[ing] Hong Kong's information connectivity, [and] upgrad[ing] the necessary infrastructure . . ." to promote economic restructuring.[23] Undoubtedly, the deployment of Internet technology ("IT") is vital and instrumental for Hong Kong's economic development. Before we start our investigation into the computer crime situation in Hong Kong, let us first understand IT usage and the Internet penetration in the community, and with that understanding, the emergence of computer criminality as a social problem.

According to the Commissioner Tsang Yam-pui of the HKP, the upsurge of computer crime from thirty-four cases in 1998 to 358 cases in

---

20. The First Asia Cyber Crime Summit was hosted by the Center for Criminology of The University of Hong Kong on April 25-26, 2001 in Hong Kong.

21. The Third Annual Conference of the Asian Association of Police Studies ("AAPS") was held on July 29, 2002 in Hong Kong. The theme of this conference was Asian Policing in the 21st Century.

22. Chief Executive Tung Chee Hwa, Address, *The 2001 Policy Address: Building on Our Strengths; Investing in Our Future* (Hong Kong, Oct. 10, 2001) (available at ¶¶ 14 and 67-68 http://www.policyaddress.gov.hk/pa01/e8.htm).

23. Chief Executive Tung Chee Hwa, Address, *The 2003 Policy Address: Capitalising on Our Advantages; Revitalising Our Economy* (Hong Kong, Jan. 8, 2003) (available at http://www.info.gov.hk/gia/general/200301/08/0108141.htm, ¶¶ 14-17).

2000 "corresponds directly with the rapid growth in Internet usage."[24] Currently, there are about 200 Internet Service Providers ("ISP") . . . compared to fifty-six ISPs in 1995, with two and a half million Internet users in 2001 compared to 600,000 users recorded at the beginning of 1999.[25] Since 2000, there have been two major surveys on IT usage and penetration conducted by the Census and Statistics Department ("C&SD"), one amongst household members[26] and the other in business sector.[27] As indicated in Table 1 below, the household survey reported that 1,322,000 households had personal computers ("PC") at the time of the 2002 survey, representing sixty-two percent of the total households in Hong Kong, and that fifty-two percent of all households had their PCs connected to the Internet.

Table 1 below presents a yearly comparison of the IT usage and penetration between 2000 and 2002 amongst household members. It indicates an increased penetration of PCs and the Internet in the community with more persons aged ten or above who have used PC and Internet services. Fifty-four percent of all persons in the age group of ten or above had actually used a PC in the twelve months before the survey. Utilization of electronic business services is quite high in Hong Kong. These e-business services include Octopus card, Automatic Teller Machine ("ATM"), e-cash, Easy Pay System ("EPS"), Payment by Phone Service ("PPS"), online searching for information, and job searching, etc.[28] Forty-three percent of the persons within the age group of ten or above have knowledge of using Chinese input methods. The 2002 survey also reveals that the rates of using PC and Internet services are higher among younger persons, better-educated persons, and students. For ex-

24. Tsang Yam-pui, Address, *Foreword: Proceedings of the Cyber Crime Summit, Proceedings of the Asia Cyber Crime Summit* 6 (Hong Kong, 2001).

25. *Id.*; *see also Census and Statistics Department, Hong Kong as an Information Society* 40 (Hong Kong, 2002) (providing statistics on Internet Services) (C&SD reports available for download at http://www.statisticsbookstore.gov.hk) [hereinafter *C&SD*].

26. *See* C&SD, *Thematic Household Survey Report No. 10: Information Technology Usage and Penetration*, (Hong Kong, 2002) (on file with the author) (providing survey methodology and more statistical analysis). The Thematic Household Survey managed by the C&SD collects "information on IT usage and penetration in order to gain better understanding of the latest development of IT in the community." *Id.* The 2002 survey was conducted during May to July 2002. *Id.* Similar surveys were conducted during January to March 2000 and April to Jun 2001. *Id.*

27. *See* C&SD, *Report on 2002 Annual Survey on Information Technology Usage and Penetration in the Business Sector* (Hong Kong, 2002) (providing survey methodology). The 3rd Survey on Information Technology Usage and Penetration in the Business Sector was conducted by C&SD, during April to June 2002, under the auspices of the Commerce, Industry and Technology Bureau. *Id.* The objective was "to collect information relating to information (IT) usage and penetration in the business sector. The survey results would be useful for reference in the development of IT strategy in Hong Kong." *Id.*

28. *Id.* at 110-112.

ample, forty percent of the Internet users are aged ten to twenty-four and sixty percent of the users have attained an educational level of Secondary / Matriculation.

Table 1 - IT Usage and Penetration in Household (Years 2000 to 2002)

	Descriptions	2002	2001	2000
a.	Households with PC among all households in HK	62.1%	60.6%	49.7%
b.	Households with PC connected to Internet among (a)	84.6%	80.4%	73.3%
c.	Households with PC connected to Internet among all households in HK	52.5%	48.7%	36.4%
d.	Persons aged 10 or > using PC in 12-mths before survey within the age group	54.0%	50.3%	43.1%
e.	Persons aged 10 or > using Internet in 12-mths before survey within the age group	48.2%	43.3%	30.3%
f.	Persons aged 15 or > using e-business services for personal matters in 12-months before survey within the age group	92.6%	88.5%	84.9%
g.	Persons aged 15 or > using online purchasing services for personal matters in 12-months before survey within the age group	4.9%	5.6%	n/a
h.	Persons aged 10 or > with knowledge of using Chinese input methods within the age group	42.8%	39.9%	29.8%
i.	Persons aged 15 or above aware of Electronic Service Delivery scheme within the age group	39.7%	32.4%	28.7%

(Source: Census and Statistics Department)[29]

Table two below summarizes the key findings on IT usage and penetration in the business sector[30] between years 2000 and 2002. The survey reports fifty-five percent, forty-four percent, and twelve percent of all establishments for using PCs, having Internet connectivity, and having a

29. *See* C&SD, *Hong Kong as an Information Society* (Reports available for download at http://www.statisticalbookstore.gov.hk).

30. *See* ITBB, *LegCo Panel on Information Technology and Broadcasting: 2001 Surveys on IT Usage and Penetration in the Household and Business Sectors*, (Hong Kong, 2002) (for the 2002 survey, questionnaires were mailed to the 4,635 selected establishments of which 3,378 were successfully enumerated, representing an overall response rate of ninety-five percent. *See* C&SD Report. The response rate is consistent to that of the 2001 survey. "A total of 3,492 establishments selected in accordance with a scientifically designed sampling scheme were successfully enumerated in the survey, constituting a response rate of ninety-six percent. The fieldwork was carried out between April and June 2001 through mailed questionnaires followed by field officers' visits/telephone calls to verify the information and provide assistance in completing the questionnaires").

Web site respectively, indicating an upward trend in all three aspects. More establishments had Web sites in 2002 (twelve percent), compared to eleven percent in 2001 and seven and three tenths percent in 2000, providing information on the firm and products and services offered both for use by customers and staff. The survey indicates that about twenty-six percent of the establishments have used a Web site for online ordering, after sales services, and/or delivery of the firms' products and services. Only less than two percent of the firms use a Web site for the purpose of online payment transactions. It is also reported that PCs continue to be more popular in the financing, insurance, real estate and business services sector, representing seventy-eight percent compared to seventy-six percent in 2001. The same sector has the highest percentage (sixty-six percent) in using PCs that had Internet connectivity. The lowest percentage is found in the transport, storage and communications sector, thirty-one percent of the firms using PCs and twenty-seven percent having Internet connectivity.

Table 2 - IT Usage and Penetration in the Business Sector (Years 2000 to 2002)

	Descriptions	2002	2001	2000
a.	Establishments using PC	54.5%	49.7%	51.5%
b.	Establishment having Internet connection	44.2%	37.2%	37.3%
c.	Establishment having Web page/Web site	11.8%	10.7%	7.3%
d.	Establishment having acquired goods, services or info thru' electronic means	7.1%	6.2%	4.9%
e.	Establishment having received goods, services or info thru' electronic means	45.2%	40.0%	35.3%
f.	Establishment having sold goods, services or info thru' electronic means	1.5%	1.1%	0.3%
g.	Establishment having delivered goods, services or info thru' electronic means	12.1%	12.4%	8.1%

(Source: Census and Statistics Department)[31]

Results of the above two annual surveys inform us of several developmental trends, most of which are not unique to Hong Kong. However, some of the social phenomena that are quickly developing, under the strong influence of cyberspace etiquette, do raise a concern to the Hong Kong government with respect to maintaining social order. The following key areas are observed:

31. See C&SD, *Hong Kong as an Information Society* (Report available at http://www.statisticalbookstore.gov.hk).

1. Public awareness and usage of IT, including computers and the Internet, have significantly increased. Also, IT is quite commonly used in the business sector to enhance productivity and explore market opportunities. The increase in popularity has led to a proportional growth in motivation and opportunity for potential criminality committed in the virtual space.

2. The growing rate of PC users being younger, students, and better educated presents a new challenge to the government in strategic planning, such as youth education and crime prevention policy. An agenda of computer and information ethics is put forth in our daily life activities.

3. A safe environment in cyberspace is essential to enable the business sector to be confident in, willing to use, and benefit from, electronic means in processing business transactions. Electronic commerce is vital to Hong Kong both in terms of economic development and image building as an international business center and commercial hub in the Region.

In this section, we have discussed the importance of IT to economic development, the growth of IT usage, and the Internet's penetration in Hong Kong with data from the C&SD. We particularly note the concerns raised by such patterns of growth and spread to the local government, i.e., the propensity of social deviance, computer and information ethics, and the threats to electronic commerce. We now turn to focus on how the computer and Internet have been used for criminal purposes, both as tools and objects in Hong Kong.

IV. NATURE, PREVALENCE AND DISTRIBUTION OF COMPUTER CRIME

The wide spread of IT usage and Internet penetration has facilitated our economic growth, sped up social interaction, and changed our lifestyle in untold ways. Unavoidably, computers and the Internet have also introduced various kinds of computer-mediated criminality and network-related social deviance into Hong Kong. In this section, we will describe the nature, prevalence and distribution of computer crime in the community, as revealed by official data sources and news media, and as understood by the scholars and policy makers.

Computer crime in Hong Kong jumped drastically to 318 cases in 1999, a nine-fold increase from thirty-four cases recorded in 1998.[32] There was a sixteen percent increase to 368 cases in 2000, followed by a slight decrease to 235 cases in 2001.[33] In reporting the 2001 Crime Situation, the HKP accounted for the decrease in computer crime as a result

32. Yam-pui, *supra* n. 24. Also, see *supra* Table 3 for statistics on computer crime cases.

33. *See* Table 3 on Computer Crime Cases in Hong Kong reported from 1996 to 2003.

of the public's awareness of computer security and the deterrent effect of criminal convictions in four major cases.[34] Such an assertion was not supported by scientific research or empirical evidence. The drop might have been due to the burst of dot.com bubble and the slow-down of IT industry during the period. In 2002, the HKP recorded a total of 272 cases of computer crimes. In addition, the Newspaper Registration Section ("NRS")[35] received a total of ninety-nine public complaints of pornographic materials available on the Internet between July 2001 and June 2001.

A further analysis of the computer crime statistics reveals that over seventy-five % of the cases in 1999 and 2000 were 'hacking' cases.[36] In recent years, the number of hacking cases dropped while e-banking thefts and e-frauds increased. In 2001, sixty-five cases of electronic deceptions were recorded, including the use of stolen identity to obtain goods or services via the Internet. As e-banking became more prevalent in 2001, there were eight cases of e-banking theft recorded that involved a total loss of over HK$4.4 million.[37] The HKP stays very alert to the increasing trend of e-banking theft that may pose a significant threat to Hong Kong as a major international finance center.[38] Table 3 summarizes the computer crime cases between 1996 and 2003 according to the types of offenses currently categorized by the HKP.

Table 3 - Computer Crime Cases in Hong Kong by Various Offenses (1996-2003)

	Title of Offense*	2003	2002	2001	2000	1999	1998	1997	1996
	(Yearly Total)	**588**	**272**	**235**	**368**	**318**	**34**	**20**	**21**
a.	Unauthorized access to computer by telecommunication	47	26	33	53	238	13	7	4
b.	Access to computer with criminal or dishonest intent	356	138	81	222				
c.	Criminal damage (computer related)	16	16	27	15	4	3	3	4

34. *See* HKP, *2001 Crime Situation*, http://www.info.gov.hk/info/crime/01crime-e.htm (accessed Apr. 30, 2005).

35. Newspaper Registration Section ("NRS") is one of the enforcement agencies of the Control of Obscene and Indecent Articles Ordinance, Cap. 390. All the complaints received against Internet crime are in relation to the publication of obscene or indecent articles through the Internet.

36. *See* HKSAR, *Inter-departmental Working Group on Computer Related Crime September 2000* 14, http://www.infosec.gov.hk/docs/english/ComputerRelatedCrime_eng.pdf (accessed Apr. 30, 2005) (providing computer crime cases reported between 1996 and 2000).

37. *See* HKP, *supra* n. 34.

38. *Id.*

	Title of Offense*	2003	2002	2001	2000	1999	1998	1997	1996
	(Yearly Total)	**588**	**272**	**235**	**368**	**318**	**34**	**20**	**21**
d.	Obtaining property by deception (on-line shopping)	86	45	32	29	18	1	2	0
e.	Obtaining services by deception (computer related)	17	19	33	49	26	4	2	7
f.	Theft (e-banking related)	8	6	16					
g.	Other miscellaneous theft (computer related)		15						
h.	Others	58	7	13					
i.	Publication of obscene articles					32	13	6	6

(Sources: Security Bureau for years 1996 to 1999, and HKP for years 2000 to 2003)[39]

[* The column 'Title of offense' follows the descriptions provided by HKP in 2002 except row (i).]

Since 2000, the Hong Kong Computer Emergency Response Team Coordination Centre ("HKCERT"), Technology Crime Division of Commercial Crime Bureau of HKP, and Office of the Government Chief Information Officer ("OGCIO") conducted an annual survey of Hong Kong registered companies to ascertain their experience with computer crime. The survey investigated Hong Kong companies' experience with computer attacks, information security awareness, computer security technologies and strategy employed and information security expenses.[40] Survey data summarized in Table 4 below supplement the computer crime statistics released by the HKP in understanding the computer related crime situation in the business sector.

The survey showed that, over half of the respondents (56.2%) have installed servers and/or Web sites, of which 23.3% experienced computer attacks within the last twelve months (2003). Computer virus attack remains the most dominant mode of unauthorized computer attacks at 94.5%. This is followed by hacking (13.5%) and denial of service (5.6%). Unauthorized computer attacks had a greater impact on small companies than big ones; attacks on small companies resulted in a higher per-

39. *See* HKP, *Data Presented at Information Technology Service Department, Information Security & Prevention of Computer Related Crime: Statistics*, http://www.infosec.gov.hk/engtext/ main.htm (accessed Dec. 2, 2002) (providing figures between 2000 and 2002); *see also* Security Bureau, *Inter-departmental Working Group on Computer Related Crime* ¶ 1.2, http://www.hkispa.org.hk/pdf/ComputerRelatedCrime.pdf (Sept. 2000) (providing figures between 1996 and 1999).

40. *See* HKCERT, HKP, and OGCIO, *Information Security Survey*, http://www.hkpc.org/text/ eng/industry_survey/all_industries/doc/infosecsur.pdf (accessed Apr. 30, 2005).

centage of PCs being affected. Only about 12.2% of unauthorized attacks were traceable to local origin. The remaining 43.4% is still unaccounted for. Finally, 44.4% of the attacks were discovered to be originating from overseas.

According to this annual survey conducted by HKCERT, HKP and OGCIO, the total financial loss resulting from computer attack was about HK$1.22 million in 2003, HK$1.84 million in 2002, and HK$1.52 million in 2001. The decline in 2003 of computer-related financial loss is due to a drop in the reporting ratio by the respondents, as revealed by financial impact interviews.[41]

Table 4 – Information Security in the Business Sector (2000 – 2003)

	Descriptions	2003	2002	2001	2000
a.	Total no. of computer crime incidents	943	1,095	1,387	1,510
b.	Change in percentage as compared to previous year (+/-)	-13.9%	-21.1%	-8.1%	n/a
c.	Average no. of attacks per victimized company	2.4	3.4	3.5	2.6
d.	Change in percentage as compared to previous year (+/-)	-29.4%	-4%	+34.6%	n/a
e.	Total no. of PCs affected	4,098	5,460	5,366	4,733
f.	Change in percentage as compared to previous year (+/-)	-24.9%	+1.8%	+13.4%	n/a
g.	Average no. of PCs affected per incident	4.3	5	3.9	3.1
h.	Change in percentage as compared to previous year (+/-)	-14%	+28.2%	+25.8%	n/a
i.	Total financial loss estimated (HK$)	$1.22M	$1.84M	$1.52M	$1.38M
j.	Change in percentage as compared to previous year (+/-)	-33.5%	+20.5%	+10.8%	n/a
k.	Average financial loss per victimized company (HK$)	$3,116	$5,632	$3,888	$2,461
l.	Change in percentage as compared to previous year (+/-)	-44.7%	+44.9%	+58%	n/a

(Source: HKCERT, HKP, and OGCIO)[42]

The above statistics collected from the three respective surveys present a fair analysis on the current status of computer crime in Hong Kong even though they may not represent a complete picture of com-

41. *Id.*
42. *Id.*

puter crime, in terms of totality and impact, due to the dark figure problem discussed at the beginning of this paper. In the coming section, we will investigate the various aspects of cyberspace governance in Hong Kong.

In the previous two sections, we have observed that three major concerns have prompted the Hong Kong government to regulate cyberspace, i.e. the propensity for social deviance, computer and information ethics, and threats to electronic commerce. From government statistics, we have also seen a phenomenal growth in computer crime since the late twentieth century. In the coming section, we will share our investigations on various aspects regarding cyberspace governance in Hong Kong, including cyberspace policy, crime theory, existing legislation, law enforcement and crime prevention through education.

V. CYBERSPACE GOVERNANCE IN HONG KONG

A. Cyberspace Policy

Hong Kong is one of the key international financial centres in the Asia Pacific region. The Digital 21 Strategy promulgated in May 2001, under the theme 'Hong Kong: Connecting the World,' clearly stated five key result areas, one of which is to enhance Hong Kong's world-class e-business environment.[43] The government is concerned about the e-commerce environment being threatened by computer criminality. Accordingly, the Hong Kong Security Bureau established a strategy to enhance the government's capacity to deal with emerging computer crime; pledging "to strengthen present monitoring of and response to computer crime trends and developments."[44] Furthermore, the HKP was charged with the implementation of such a strategy to make Hong Kong one of the safest and most stable societies in the world.[45]

In the regard of cyberspace, the government recognizes a long-term need for the barriers between legislation on computer crime and that on physical crime to be demolished. "Our law should ideally be able to cater to the requirements of the information age without regard to whether an act is done via traditional means or in the cyber world . . . . [N]ew legislation or amendments to existing legislation should be drawn with an eye to the requirements of the information age. As far as possible, legislation should be technology- and medium-neutral. Given the constantly

43. *See* Hong Kong Information Technology and Broadcasting Bureau ("ITBB"), *Hong Kong Digital 21 IT Strategy*, http://www.info.gov.hk/digital21/eng/strategy2001/strategy_part04.html (accessed Apr. 30, 2005).

44. *See* Security Bureau, Address, *The 2001 Policy Address: Policy Objectives – Security Bureau: A Secure and Safe City* (Hong Kong, 2001) (available at 19 http://www.policyaddress.gov.hk/pa01/ pdf/safee.pdf).

45. *Id.*

evolving nature of the cyber world, we cannot afford to stand still in our effort to curb computer crime"[46]

Unlike China's central government, Hong Kong's government does not have a political concern in monitoring and regulating the flow of information on the Internet. Rather, the people of Hong Kong are eager to be able to enjoy the rights of free expression and privacy on the Internet in parallel to a concern about security, intellectual property, and fair competition in cyberspace. One topic that is relatively similar to the central government is the concern about computer ethics on the Internet, particularly on ethical education of the youngsters in cyber-crime prevention. In mainland China, it is very much emphasized to promote healthy, ethical and moral use of Internet.[47] The approach in Hong Kong is more decentralized and the numerous efforts of the various agencies need to be better coordinated in promoting the importance of security awareness and information ethics. Despite the fact that the context of information ethics may vary in these places, some U.S. officials do encourage youngsters to learn 'cyber-ethics.'[48] There is a U.S. Department of Justice ("DOJ") Web site dedicated to teaching young people the right ways to use the Internet[49] and educational programs, e.g. the Cybercitizen Partnership,[50] as well. It is encouraging to see that the Inter-departmental Working Group has recommended joint efforts of the private sector in public education of computer security awareness and information ethics.[51]

B. Computer Crime Theory

The current and emerging forms of computer-related illegality suggest that conventional legislation is inadequate to maintain law and or-

46. *See* Security Bureau, *Inter-departmental Working Group on Computer Related Crime* ¶¶ 14.3-14.5, http://www.hkispa.org.hk/pdf/ComputerRelatedCrime.pdf (Sept. 2000).

47. *See* Kam C. Wong & Georgiana Wong, Lecture, *Law and Order in Cyberspace: A Case Study of Cyberspace Governance and Internet Regulations in PRC, Proceeding Papers, Third Annual Conference of the Asian Association of Police Studies* (Hong Kong, 2002) (for a similar study of cyberspace governance in PRC) (copy of transcript on file with the author).

48. *See* Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice, *General Information*, http://cybercrime.gov/ (accessed Apr. 1, 2005).

49. *See* Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice, *General Information*, http://cybercrime.gov/ (accessed Apr. 1, 2005).

50. *See* Attorney General John Ashcroft, Speech, *First Annual Computer Privacy, Police & Security Institute* (May 22, 2001) (available at http://cybercrime.gov/AGCPPSI.htm).

51. See Hong Kong Security Bureau, *Inter-departmental Working Group on Computer Related Crime, September 2000*, http://www.infosec.gov.hk/docs/english/ComputerRelatedCrime_eng.pdf (accessed Apr. 30, 2005).

der in cyberspace. However, the basic principles of criminology apply to computer-related offenses, such as e-banking fraud or online shopping theft, similar to traditional criminality, such as bank robbery or shop lifting. Criminologists, e.g. Marcus Felson's 'routine activities theory,' established that crime follows from a motivation and an opportunity together in the absence of capable guardianship. Felson wrote, "predatory crime incidents depend on the physical convergence of these three elements: a likely offender, a suitable target, and the absence of capable guardians."[52]

The motivations of computer-related offenses are diverse, but none are new to those personal desires of traditional criminality, e.g. greed, power, lust, revenge, curiosity, adventure, etc.[53] One of the most dazzling dimensions is the challenge of mastering the complex technicality in committing a computer crime.[54] With the increased popularity in computer usage and Internet penetration, in personal life and business, there are increasing opportunities provided for computer criminals. The convergence of communication and computing technologies brings greater capacity to benefit our lives as well as greater vulnerability. It is interesting to note that, in the case of hacking incidents in Hong Kong, there is an indicative trend that offenders' motives are more for money rather than for fun or the satisfaction of testing their skills.[55] Notwithstanding the shift in motivation, the basic principles of criminology are essential to understanding the formation of computer crime control policy and the crime prevention approach adopted by Hong Kong's government.

C. Computer Crime Legislation

The Computer Crimes Ordinance in Hong Kong was enacted in 1993 through amending the Telecommunications Ordinance (Cap. 106), Crimes Ordinance (Cap. 200) and Theft Ordinance (Cap. 210), with some

52. Marcus Felson, *Crime and Everyday Life – Insight and Implications for Society* 30 (Pine Forge Press 1994); *see also* Ronald V. Clarke & Marcus Felson, *Routine Activity and Rational Choice, Advances in Criminological Theory* vol. *5*, 1-14 (Transaction Publishers 1993).

53. For crime as rational choice, *see The Reasoning Criminal* (D. Cornish & R. Clarke eds., New York: Springer-Verlag 1986). Criminals are rational, and they are motivated by money or status in committing crime. *Id.* For crime as "acts of force or fraud undertaken in pursuit of self interest," *see* Michael R. Gottfredson & Travis Hirschi, *General Theory of Crime* 15 (1990). Crimes are usually committed for short term gratification. *Id.* at 91.

54. Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (1992) (stating that original hackers were interested in mastering the technical aspects of the virtual world) (electronic version available at http://stuff.mit.edu/hacker/hacker.html).

55. *See* Michelle Chak, *Computer Criminals Logging on for Profit*, South China Morn. Post (Aug. 18, 2001).

new offenses created and the coverage of existing offenses extended.[56] Table five below summarizes these provisions and their maximum penalties.[57] The Inter-departmental Working Group once considered an option to capture all legislative changes regarding computer crime in one ordinance, but finally decided to leave the discretion to the law draftsman for an appropriate vehicle.[58]

Table 5 - Provisions of Computer Crimes Ordinance in Hong Kong

Law	Provisions	Maximum Penalty
Cap. 106, S.27A	Prohibiting unauthorized access to computer by telecommunication	Fine of $20,000
Cap. 200, S.59	Extending the meaning of property to include any program or data held in a computer or in computer storage medium	Not applicable
Cap. 200, S.59 & 60	Extending the meaning of criminal damage to property to misuse of a computer program or data	10 years' imprisonment
Cap. 200, S.85	Extending the meaning of making false entry in bank book to falsification of the books of account kept at any bank in electronic means	Life imprisonment
Cap. 200, S.161	Prohibiting access to computer criminal or dishonest intent	5 years' imprisonment
Cap. 210, S.11	Extending the meaning of burglary to include unlawfully causing a computer to function other than as it has been established and altering, erasing or adding any computer program data	14 years' imprisonment
Cap. 210, S.19	Extending the meaning of false accounting to include destroying, defacing, concealing or falsifying records kept by computer	10 years' imprisonment

(Source: Security Bureau)[59]

Given the trans-border nature of computer crime, the Working Group had completed a comparison study of our existing legislation with reference to the "Draft Convention on Cyber-Crime" of the Council of Eu-

56. See Hong Kong Security Bureau, *Inter-departmental Working Group on Computer Related Crime, September 2000* 5-9, http://www.infosec.gov.hk/docs/english/ComputerRelatedCrime_eng.pdf (accessed Apr. 30, 2005).

57. *Id.*

58. *Id.*

59. *Id.*

rope ("COE").[60] The COE has identified and published four major categories of offenses to be incorporated into the substantive criminal law of participating countries. The four categories are: 1) offenses against the confidentiality, integrity and availability of computer data and systems; 2) computer-related offenses; 3) content-related offenses; and 4) ancillary liability and sanctions. Table 6 below presents an analysis of computer-related offense provisions, based on the COE classification of offenses as defined in the Draft Convention.[61] Altogether, the Working Group has presented a framework with fifty-seven recommendations of legislative and administrative measures to improve the Hong Kong regime in tackling computer crime.[62]

Table 6 – Analysis of Computer-Related Offense Provisions in Hong Kong Based on the Council of Europe Classification of Offenses

	COE Classification of Offenses	Hong Kong Ordinance	
a.	Illegal access	Crimes Ordinance Cap.200	Cap.200, s161 (5 yrs max.)
b.	Illegal interception	Telecommunication Ord. Cap.106	Cap.106, s27A (fine of HK$20,000)
c.	Data interference	Crimes Ordinance Cap.200 (extending 'criminal damage to property' to include 'misuse of a computer') Theft Ordinance Cap.210 (extending 'burglary')	Cap.200: ss59,60,63 (10 yrs max. or life imprisonment if property intentionally destroyed so as to endanger life) Cap.210, s11 (14 yrs max. for burglary to include unlawful interference with computer)
d.	System interference		
e.	Misuse of devices		

60. *See* The Council of Europe, http://www.coe.int (accessed Apr. 1, 2005). COE is an international organization with 41 member states. It seeks to, inter alia, strengthen the rule of law throughout its member states by encouraging the adoption of common practices and standards.

61. *See* Gregor Urbas, Lecture, *Cyber-crime Legislation in the Asia-Pacific Region*, 58-85 (Hong Kong, 2001) (for a comparative analysis of cyber-crime legislation in the Asia Pacific jurisdictions from the Proceedings of the Asia Cyber Crime Summit) (copy of transcript on file with author); *see supra* n. 24, at Annex 12.

62. "Summary of Recommendations." *See* HKSAR, *Inter-departmental Working Group on Computer Related Crime* i – viii (Sept. 2000).

	COE Classification of Offenses	Hong Kong Ordinance	
f.	Computer-related forgery	Crimes Ordinance Cap.200	s85 (life imprisonment for falsification of bank computer records)
g.	Computer-related fraud	Theft Ordinance Cap.210	s19 (10 yrs max. for false accounting by falsifying computer records)
h.	Computer child pornography	Control of Obscene and Indecent Articles Ord.Cap.390	s21 (3 yrs max. and fine of HK$1 million)
i.	Copyright and related rights	See Copyright Ordinance Cap.39 Prevention of Copyright Piracy Ordinance Cap.544	
j.	Separate attempt, aiding etc. offenses	Theft Ordinance Cap.210	s56 (accessories) s159A (conspiracy) s159G (attempts)
k.	Corporate liability		

(Source: Gregor Urbas)

The Working Group report, regardless of some deficiencies in the study, has informed us that the existing legislation is inadequate to curb the new and emerging forms of computer crime that are characterized by their trans-border and evolutionary nature. The HKP plays a leading role in implementing the recommendations of the Working Group on computer crime.

D. Law Enforcement

The HKP has taken active steps in allocating resources in three areas of fighting computer crime: 1) policing computer crime in accordance to existing legislation; 2) developing professional and investigative computer forensics capability; and 3) promoting public awareness in computer security. The Technology Crime Division ("TCD") of the Commercial Crime Bureau ("CCB") was set up in June 2000 and supported by a computer forensics laboratory.[63] In July 2001, the HKP established the Computer Security Unit ("CSU") within the Crime Prevention Bureau ("CPB") to educate the public about the nature and extent of computer crime risks and to assist businesses to adopt measures to avoid from becoming victims of computer crime.[64]

63. *See* HKSAR, *Computer-aided Crime Faces Computer-aided Forensics*, HKSAR http://www.info.gov.hk/gia/general/200209/18/0918158.htm (Sept. 18, 2002).

64. Victor Yik-kee Lo, *Police Training for Cyber Transformation*, in *Bridging the GAP—A Global Alliance Perspective on Transnational Organised Crime* 95–99 (Roderic Broadhurst ed., 2002), (available at http://www.hku.hk/crime/Tocccontent.pdf).

E. Computer Crime Prevention through Education

Prevention is a proactive measure of any comprehensive effort in combating crime, particularly so for fighting cyber-crime. In view of the penetration of PCs and Internet usage at home and in business, public education plays a key role in raising security awareness and cultivating information ethics. According to the Inter-departmental Working Group on Computer Related Crime Report (September 2000), there were plenty of initiatives, such as exhibitions and seminars, driven by various government agencies and the private sector in promoting the importance of information security.[65] Unfortunately, these individual efforts need a closer coordination in yielding better results. The government departments, such as the Information Technology and Broadcasting Bureau ("ITBB"), Information Technology Services Department ("ITSD") and HKP, have their own publicity programs in the pipeline that do not appear to be well co-coordinated.[66] Relatively, quasi-governmental agencies are playing a more active role. Broadly speaking, the current efforts address three major groups of target audience: 1) the banking and finance industry; 2) the small and medium enterprises ("SME") of the business community; and 3) the mass public.

Among the private sector, the banking and finance industry demonstrates high self-initiative efforts in preventing computer crime, whereas the Hong Kong Monetary Authority ("HKMA") is taking a leadership role in working with banking members to formulate finance/banking guidelines and best practices for adoption.[67] Most of the larger organizations have engaged in-house staff in handling information security matters and awareness education. Taking reference from overseas, such as the U.S. and Singapore, the Hong Kong Monetary Authority ("HKMA") mainly studies the relevant finance/banking guidelines for possible adoption and shares with its members the best practices in conducting financial transactions over the Internet.[68] Besides publishing the guidelines for the industry members, the HKMA "has established contact with the industry Associations, Information Technology Services Department, the Technology Crime Division of the Police, and other relevant bodies with a view to promoting the general awareness of banking security, establishing a common incident reporting and response mechanism for the

65. *See* Hong Kong Security Bureau, *Inter-departmental Working Group on Computer Related Crime, September 2000*, http://www.infosec.gov.hk/docs/english/ComputerRelatedCrime_eng.pdf (accessed Apr. 30, 2005) (Chapter X Public Education and Annex 9 for a full description of the various efforts of individual agencies).

66. *Id.*

67. *See* Hong Kong Monetary Authority, *Electronic Banking and Technology Risk Management*, http://www.info.gov.hk/hkma/eng/bank/e-banking/e-banking_b.htm (accessed Apr. 30, 2005).

68. *Id.*

banking industry and enhancing public confidence in e-banking."[69]

Education and publicity campaigns for SME are primarily driven by the Hong Kong Productivity Council ("HKPC") enhancing their knowledge of information security. Together with the Consumer Council and the Office of Privacy Commission for Personal Data ("PCO"), an education leaflet 'Guide to Personal Data Privacy and Consumer Protection on the Internet' was published and distributed to SME.[70] The Hong Kong Computer Emergency Response Team Coordination Center ("HKCERT") of HKPC acts as an information center in sharing security information, such as news on virus and vulnerability on system software.[71] HKCERT also conducts surveys on the preparedness of SME for security set-up of their system infrastructure security, and provides consultancy to SME on system recovery and contingency planning.[72] Nevertheless, the preventive services provided are mostly a reactive or 'fire-fighting' mode.

The education programs and publicity events organized by the ITBB/ITSD and HKP mainly address the mass public, usually in large exhibitions or public seminars as reflected from the Event Calendar of the Information Security & Prevention of Computer Related Crime.[73] In coping with the increasing need for public awareness and education programs on computer security issues, the Crime Prevention Bureau ("CPB") of HKP established the Computer Security Unit ("CSU"), a specialized unit dedicated to providing services to the people of Hong Kong, advising on all aspects of computer security and facilitating public education on computer security awareness, in July 2001.[74]

The Inter-departmental Working Group report informs us that the government has made a conscious decision to engage the private sectors in taking a larger and more active role in respect of education and publicity based upon a philosophy that "every user has a responsibility to protect his own computer system and data . . . [and that] we cannot rely on the Government alone."[75] Regrettably, there is no visibility on the role

---

69. *Id.*

70. *See* Hong Kong Productivity Council, *Guide to Personal Data Privacy and Consumer Protection on the Internet* http://www.info.gov.hk/digital21/eng/ecommerce/guideline/privacy1_4.pdf (accessed Apr. 30, 2005).

71. *See* HKCERT Web site with security alert announcements posted at http://www.hkpc.org/text/eng/highlight/hkcert/langing.jsp.

72. For survey report, *see* HKCERT, HKP and OGCIO, *Information Security Survey* http://www.hkpc.org/text/eng/industry_survey/all_industries/doc/infosecsur.pdf; For HKCERT services, *see* HKCERT, http://www.hkpc.org/text/eng/highlight/hkcert/langing.jsp (accessed Apr. 30, 2005).

73. *See* HKSAR, *InfoSec Event Calendar*, http://www.infosec.gov.hk/engtext/general/newsevents/calendar.htm (accessed Apr. 30, 2005).

74. For HKP publicity and education efforts, *see* HKSAR, *Inter-departmental Working Group on Computer Related Crime* 106-107, (Sept. 2000).

75. *See supra* n. 24, at ¶ 11.7.

taken by the Education Department or universities even mentioned in the crucial policy paper. In our view, these organizations should have a prominent role in helping youngsters develop a proper legal understanding and cultivate ethical principles in using the Internet.

VI. REGULATING CYBERSPACE: HYPERBOLE OR ELLIPSIS

By now, we have a fair view of the computer crime situation in Hong Kong and the government attempts to impose constraints capable of achieving an environment conducive for the maintenance of law and order in society. Is the Hong Kong government doing too much, or too little in this controversial topic?

The policies and laws, under consideration and discussed so far, are/were designed to control the disorder of cyberspace. If it is natural for public administrators, or the police to have seen the dark side of computers and the Internet, then logically there needs to be more emphasis on governance. But many libertarians, e.g. John Berry Barlow and D. Boaz, take an opposing view that the government should take a 'hands-off' approach to preserve the liberty of the Internet.[76] Libertarians believe that the essence of cyberspace is liberty itself and the Internet should permit packets of information flowing freely without discrimination or interference by the government.[77] In the real world, many technologies that make the Internet possible were developed with government assistance or funding. "Internet history can be traced to a military research network established in 1968 called the Arpanet . . . [which] was sponsored by the Advanced Research Projects Agency ("ARPA") of the US Department of Defense ("DoD") . . . [which] was originally devoted to [the] support of data communications for defense research projects."[78] Also, many large corporations, such as AT&T, Cisco, Microsoft, and other commercial firms have played a role contributing to the infrastructure security of the Internet through research and development and private rewards.[79] The nature of the Internet is dynamic and

76. *See* John Barlow, *A Declaration of the Independence of Cyberspace*, http://www.eff.org/%7Ebarlow/Declaration-Final.html (Feb. 8, 1996).

77. *See* Richard A. Spinello, *Regulating Cyberspace: The Policies and Technologies of Control* 33-36 (Quorum Books 2002). "Hence, libertarians like Barlow and Boaz seem convinced that government regulations will be ineffectual, since the Internet will resist them. But they also believe that such regulations are inappropriate in the first place: To the extent those regulations succeed, they will only dissipate the creative energy of cyberspace." *Id.*

78. *See* Brandin and Lynch, *Internet* in *Encyclopedia of Computer Science* 915-927 (4th ed., Nature Publishing Group 2000) for historical development and applications of the Internet.

79. "Microsoft announces rewards for those that help catch cyber criminals Microsoft Teams With Worldwide Law Enforcement To Stop Internet Worm And Virus Distributors With US$5 Million Reward Fund Initiative SYDNEY, Australia, 6th November, 2003"

the essence can be changed. More importantly, there are other ways to regulate cyberspace as Internet governance is more than a matter of just imposing laws and subject to other constraints beside the legislation.

Larry Lessig argued that the Internet is far more 'regulable' than the libertarians realize or admit. In his book, Code and Other Laws of Cyberspace, Lessig has presented in detail the regulability of cyberspace depends on the code. "Some architectures of cyberspace are more regulable than others; some architectures enable better control than others."[80] The code, computer programs and protocols, written by programmers, determine the properties of the Net, the essence of which can easily be changed by human agents.[81] Hence, in cyberspace, the code is the law.[82] Just as in the physical world, regulations in cyberspace are also a function of the interaction of four constraints: laws, norms, the market, and architecture. Richard Spinello, a professor at Boston College specialized in computer ethics, added another dimension of 'ethical principles'[83] to Lessig's four modalities of regulation.[84] For instance, laws regulate human behavior by prohibiting certain activities and by imposing penalties for computer crime offenders. The supply and demand situation in the Internet market affects the ISPs' pricing policies and service packages. The Internet etiquette and social customs are norms that regulate the behavior of cyberspace users. The architecture in cyberspace is described as 'code' by Lessig. "The code embeds certain values or makes certain values impossible. In this sense, it too is regulation, just as the architectures of real-space codes are regulations."[85] The code writer emerges as the prime architect and regulator in cyberspace. Computer and information ethics aim to "integrate computing technology and human values in such a way that the technology advances and protects human values, rather than doing damage to them."[86] In summary, the regulation of cyberspace goes beyond the policy formation process of developing or imposing laws. We believe that self-regulation is

("The Anti-Virus Reward Program, will be initially funded with $5 million (U.S.), and aims to assist law enforcement agencies identify and bring to justice those who illegally release damaging worms, viruses and other types of malicious code on the Internet.").

80. Larry Lessig, *Code and Other Laws of Cyberspace* 20 (Basic Books 1999).

81. *Id.*

82. *Id.* at 3-8.

83. Spinello, *supra* n. 77, at 39-40. "My only quarrel with Lessig is that he does not pay adequate attention to ethical principles . . . . Lessig is mistaken when he lumps ethics together with the fleeting and impermanent norms of communities." *Id.*

84. Lessig, *supra* n. 80, at 86-90.

85. *Id.* at 89.

86. Simon Rogerson, *Computer and Information Ethics, The Concise Encyclopedia of the Ethics of New Technologies* 65-72 (Academic Press 2001).

the most optimal form of cyberspace governance.[87]

In reviewing the computer crime situation in Hong Kong, we do not agree with the extreme libertarian perspective that argues for a simplistic and idealistic 'hands-off' approach adopted by the government. We are inclined to defend more on the necessity of cyberspace control and Internet regulation. Concurring to the viewpoint of Lessig and Spinello, we think that, in addition to law, self-regulation in the dimensions of norms, the market, architecture, and ethics, can be powerful and flexible means of regulating cyberspace. But we are not totally convinced by Lessig's conclusion that "the code is the law," controlling or regulating more perfectly and completely than law. Self-regulation is one of the alternatives, but may not be the optimal form of regulation in cyberspace, depending on situations. Similar to the real world, there are situations where government intervention appears to be more effective in cyberspace to protect the interests of people, such as ensuring a safe electronic environment for e-banking and doing business, protecting children from vandalism and pornography, and protecting individual's intellectual property, etc. The growth in computer crime since the late 20th century in Hong Kong is a good illustration.

Since the economic crisis in 1997, Hong Kong's economy has rapidly deteriorated, particularly so in the last three years. One of the biggest challenges of the HKSAR government today is to facilitate a smooth economic restructuring that quickly relieves the people's hardship. IT development is a critical enabler for such a restructuring of which e-commerce and e-government are two major initiatives. The community cannot afford to have any social disorder, albeit in the physical world or cyber world. An unsafe Internet environment will discourage domestic or foreign investments, and consequently jeopardize the overall economy. In a domino effect, this will harm the economic restructuring, thus in turn lead to many adverse social impacts. The government, taking a 'hands-off' approach, or doing nothing to curb computer crime, will encourage or motivate more offenders along with the increasing opportunities brought by IT development and low cost. Government intervention is needed to establish legislation, creating deterrence to computer criminals and bringing back law and order in cyberspace. The HKP computer forensics laboratory is instrumental in bringing in the necessary technology, e.g. decryption, to crack the computer code for purposes of crime investigative and evidence tracking. Education is another typical example of government intervention needed to promote public awareness

87. Lessig, *supra* n. 80. "We live life in real space, subject to the effects of code. We live ordinary lives, subject to the effects of code." *Id.* Thus, we the people, as Internet citizens, have the obligation to provide our own code of conduct, socially, morally, and culturally, to be actualized by computer code, technically. That ultimately is the central thesis of Professor Lessig's insight.

on computer security and information ethics. This education role is of the utmost significance in helping young Internet surfers to cultivate information ethics as well as in preparing parents and teachers to provide capable guardianship in preventing computer crime.

Is the Hong Kong government introducing excessive measures or inadequate schemes in controlling computer crime or regulating cyberspace? While the topic is newly tabled on the government agenda, most observations are preliminary and judgment appears premature. The only complaint that we have is the untimely response of government agents and the lacking synergy in their efforts in tackling computer crime, a social issue that is trans-border, evolving and anonymous in nature. In comparison to other geographies in the region, Hong Kong started late in studying the topic and related legislation in an organized and professional manner.[88] For instance, the Inter-departmental Working Group report was only released in November 2000 for public consultation. The Computer Security Unit and the Computer Forensics Laboratory of HKP were set up in 2001. We see some progress after the Report, but as usual, things are not moving fast enough in terms of law drafting or policy implementation. In terms of computer crime prevention, an effort largely dependent on education, the government initiative or intervention appear to be inadequate, relying too much on the private sector.

VII. CONCLUSION

The Internet has fundamentally changed our way of life, both private and business, as well as our behavior in human interaction. The development trend of Internet applications and e-business is quite irreversible as we continue to enjoy the benefits derived therefrom. In parallel to the technological development, the Information Age also gives rise to new criminality as it aggregates old criminal problems. Computers connected to the Internet facilitate traditional criminality and bring new kinds of illegality. Given the trans-border and evolving nature of computer crime, it is an issue of international concern.

With the goals of restructuring the economy to one that is knowledge-based, and fostering a secure environment conducive to this economic growth, the Hong Kong government needs to be concerned about the propensity for social deviance in cyberspace, computer and information ethics, and threats to electronic commerce in formulating the control

88. Conference on Computer and Communications Security, *The Failure of Anti-Hacking Legislation: A Hong Kong Perspective*, http://delivery.acm.org/10.1145/240000/238189/p62-lau.pdf?key1=238189&key2=3850219011&coll=GUIDE&dl=vGUIDE&CFID=39270713&CFTOKEN=56849986 (accessed May 2, 2005) (The earliest academic study was completed by Rynson W. H. Lau, Kwok-Yan Lam, and Siu-Leung Cheung).

policies in computer crime. Inter-departmental efforts were organized to have a focused review on related legislation and administrative measures. The government adopted the proposed framework for improving the existing regime in July 2001. Thereafter, some actions have been observed, but the progress is relatively slow.

The Hong Kong government has been in a passive mode in addressing computer crime issues and the subsequent social impacts. The legislation is found inadequate and outdated in bringing a deterrence effect to computer criminals. The mass public, by and large, still lacks awareness in computer security or information ethics. Most initiatives in computer crime prevention are driven by the private sector, particularly the IT and banking/finance industries. Even so, the activities and solutions are so piecemeal that the efforts can hardly be significant or persistent. While both Internet and computer crime are evolving fast, the government policy is unable to keep with the pace.

Governance in cyberspace is a matter of managing the combinations of laws, norms, the market, the architecture (or code), and ethics in the cyber world. The Hong Kong government should adopt a comprehensive approach in the formation of the computer crime policy, managing these five dimensions in a balance. Undoubtedly, the government will continue her role in making legislation while the police force will enhance its capability in combating computer crimes. In seeking co-operations from the private sector, the government should take a stronger leading role, particularly in the area of public awareness and education in computer and information ethics. The free economy in the market will leave the consumers to opt for their choice of preference.

Cyber-crime is an emerging problem in Hong Kong. The Internet, by nature, is extra-territorial, recognizing no border. Fighting computer crime very often requires a joint effort from various regimes. The Hong Kong government should continue to keep in contact with international institutions and overseas regulators in sharing information, best practices, and legislation in cyberspace governance, as well as law enforcement in controlling cyber-crime. Finally, the study of cyberspace governance in Hong Kong is still at its infant stage. There is much to be discovered by scholars, researchers and professionals in the field.