Washington International Law Journal

Volume 14 | Number 2

4-1-2005

Computer Crime and Control in Hong Kong

Kam C. Wong

COMPUTER CRIME AND CONTROL IN HONG KONG

Dr. Kam C. Wong[†]

Abstract: This Article is a first attempt to study cyberspace governance and computer crime control in Hong Kong. It begins with a discussion of how computer crime was "discovered" as a cognizable object of control. Next, it explores the nature, prevalence and distribution of computer crime in Hong Kong before embarking on a comprehensive review and critical analysis of the Hong Kong government's cyberspace governance philosophy and computer crime control policy. The Article closes with a number of recommendations for improving Hong Kong cyberspace governance, which focus on developing a broad, overarching policy that both meets the public's goals and addresses private sector concerns.

I. INTRODUCTION

As an international finance center, Hong Kong enjoys many of the benefits of the new Information Age.[1] The Internet allows people to communicate with each other on demand, in real time, and anonymously, from anywhere in the world. The Internet is a much better way to do business and conduct commercial transactions. As one Hong Kong information technology ("IT") consultant put it:

> The promises held out by the Internet are at once compelling and confronting. The Internet promises to lower costs, streamline logistics, and shorten production cycles. The Internet holds out the promise of reaching new markets and new customers by eliminating the tyranny of distance. And the Internet promises to eliminate intermediaries. Those who move fast stand to gain a significant competitive advantage.[2]

[†] 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. The author is much indebted to Georgiana Wong, one of his former students at the Chinese University of Hong Kong, who assisted in this research in a most dedicated and efficient manner. The author also wishes to thank Elizabeth Tutmarc and the editorial staff of the *Pacific Rim Law & Policy Journal* for preparing this Article for publication.

[1] INTERNATIONAL TELECOMMUNICATION UNION, *Broadband as a Commodity: Hong Kong, China Internet Case Study* (May 2003), *available at* http://www.itu.int/ITUD/ict/cs/hongkong/material/CS_HKG.pdf (last visited Apr. 20, 2005).

[2] *See* Peter Lovelock, *Telecoms Infotechnology Forum: Hong Kong as an Internet Financial Hub* (1999), *available at* http://www.trp.hku.hk/tif/papers/1999/sept/9909posp.pdf (last visited Apr. 20, 2005).

The Hong Kong economy is increasingly and irreversibly relying upon computer-mediated communication.[3] Personal computer penetration grew from thirty-four percent in 1998 to fifty percent in 2000.[4] There were more than 190 Internet service providers ("ISPs") offering competitive prices and services. Consumers use the Internet to send e-mail, surf the cyberspace, conduct research, and shop. Businesses use the Internet for marketing and customer support. The Hong Kong Government ("HKG") uses the Internet to conduct business and deliver services.[5]

The Internet has also become a catalyst for Hong Kong economic reform, social development and political change.[6] The import, impact, influence, and implications of Internet use in Hong Kong go far beyond what has been contemplated. The history and legacy of computers in Hong Kong are still being written.[7]

Similar to the situation in many developed societies,[8] the phenomenal growth in information technology penetration and usage in Hong Kong has been accompanied by an increase in computer-related crime since the late twentieth century.[9] This has led to a call for critical review of cyberspace governance philosophy, law, and practices.[10]

---

[3] *See* Cyberspace Center of the Hong Kong University of Science and Technology, *Report on Internet Use by Hong Kong Industries* (May 1997), *at* http://www.cyber.ust.hk/survey/index.html (last visited Apr. 20, 2005).

[4] *APEC E-Commerce Readiness Assessment Guide—A Self Assessment of Hong Kong's Readiness for E-Commerce* (2000), *at* http://www.ogcio.gov.hk/eng/archive/pupr2000/eassess.htm (last visited Apr. 20, 2005).

[5] *Id.*

[6] For information on the distribution of Internet access in Hong Kong, *see* William Foster et al., *The Internet and South China (Taiwan, Hong Kong, Fujian, and Guangdong)* (Sept. 28, 1999), http://mosaic.unomaha.edu/schina.pdf (last visited Apr. 9, 2005).

[7] Hong Kong had no National Information Infrastructure Project to speak of before 1995, although Hong Kong Information Technology Federation and Hong Kong Generation Chamber of Commerce have championed its establishment. Hong Kong Monetary Authority ("HKMA"), *Financial Technology Infrastructure for Hong Kong* 31-2 (Dec. 1997) 31-32, *available at* http://www.info.gov.hk/hkma/eng/public/ftihk/ftihk.pdf (last visited Apr. 20, 2005). On December 6, 1996, the HKSAR Legislative Council (Legco) Panel on Information Policy was formed to discuss "Development of Information Highway and Internet in Hong Kong." *Id.* Correspondingly, the government established the Information Infrastructure Advisory Group ("IIAG") (under the Office of the Telecommunication Technology) on March 21, 1997. The charter of IIAG includes: "To advise on the development and regulation of the information technology in Hong Kong." *Id.*

[8] *See generally United Nations Manual on the Prevention and Control of Computer Related Crimes*, INTERNATIONAL REVIEW OF CRIMINAL POLICY 43-44 (Oct. 1992), *at* http://www.uncjin.org/Documents/irpc4344.pdf (last visited Apr. 20, 2005).

[9] Mike Carlson, *Firms Plagued by Computer Viruses*, SOUTH CHINA MORNING POST (SCMP), Dec. 7, 2000, at 5, *available at* LEXIS, News Library; Vivien Pik-Kwan Chan, *Tougher Law for Hacker*, SCMP, Jul. 2, 1998, at 9, *available at* LEXIS, News Library; Jo Bowman, *Security Warnings as Net Crime Soars*, SCMP, Feb. 22, 2001, at 5, *available at* LEXIS, News Library; *Credit Card Worries Curb Web Buying*, SCMP, July 27, 2000, at 5, *available at* LEXIS, News Library.

[10] Cook Beryl, *Expert Urges Change to Computer Law*, SCMP, Apr. 24, 1993.

The study of cyberspace governance in Hong Kong is still in its infancy.[11] As of yet, there are few scholars or policy makers who have taken on the challenge of conducting a defining, much less definitive, comprehensive study on the subject. Academic publications on cyberspace governance in Hong Kong are also rare.[12] This Article is an attempt to fill the research gap.

This project investigates computer-related crime and control in Hong Kong—its philosophy, policy, and practices. Specifically, this Article focuses on the following questions: Is there a computer crime problem and how was it discovered in Hong Kong? What are the nature, incidences, prevalence, distribution, and causation of computer crime? What are the cyberspace governance philosophy and computer crime control strategy in Hong Kong?

After this brief Introduction, Part II of this Article discusses various computer crime research problems. Part III investigates the emergence of computer crime and electronic privacy as a public concern and government problem since the mid-1990s. Part IV provides an overview of the nature, extent, and distribution of computer crimes in Hong Kong. Part V explores the HKG's approach to the control of computer crime and regulation of cyberspace. Part VI summarizes the key findings of this research, ending with recommendations for improving cyberspace governance in Hong Kong.

II. RESEARCHING HONG KONG CYBERSPACE GOVERNANCE

There are four major problems with cyberspace governance research in Hong Kong. First, there is a problem of defining computer crime.[13]

---

[11] The first comprehensive industrial study of computer crime was conducted by the HKMA as part of its Electronic Banking and Technology Risk Management mission. *See Security of Banking Transactions Over the Internet* (Nov. 25, 1997), *available at* http://www.info.gov.hk/hkma/eng/guide/guide_no/guide_1511xb.htm (last visited Apr. 20, 2005). The first comprehensive legal and policy study of computer crime and cyberspace governance in Hong Kong was INTER-DEPARTMENTAL WORKING GROUP ON COMPUTER RELATED CRIME, REPORT (Sept. 2000), *available at* http://www.info.gov.hk/archive/consult/2001/crime-e.pdf (last visited Apr. 20, 2005) [hereinafter HKSAR Computer Crime Report].

[12] The earliest academic study was Rynson W. H. Lau, Kwok-Yan Lam & Siu-Leung Cheung, *The Failure of Anti-Hacking Legislation: A Hong Kong Perspective*, Conference on Computer and Communications Security (1996), *available at* http://delivery.acm.org/10.1145/240000/238189/p62-lau.pdf?key1=238189&key2=3850219011&coll=GUIDE&dl=GUIDE&CFID=39270713&CFTOKEN=56849986 (last visited Apr. 20, 2005). A more recent professional paper on computer crime, legislation and control in Hong Kong is one by the Senior Assistant Director of Public Prosecution. The report relied entirely on newspaper accounts to support assertions in the paper. Richard Grant Turnbull, *Fraud and The New Technology—A Hong Kong Perspective*, 17th LawAsia Biennial Conference (Oct. 4-8, 2001), *available at* http://www.nzls.org.nz/conference/pdf%20files/TurnbullSa2.pdf (last visited Apr. 20, 2005).

[13] The problems with definitions have never been satisfactorily resolved, much less approached any

Second, there are difficulties in ascertaining the nature and extent of computer crime. Third, there are difficulties with valid and reliable computer crime data. Fourth, there is a lack of computer crime research in Hong Kong.[14]

A. *Problems Defining Computer Crime*

There is no commonly agreed upon definition of computer crime in Hong Kong.[15] Two issues are involved: defining "computer" and "computer crime."

What is the meaning of the term "computer"?[16] There are two concerns for legislation. Is the term "computer" defined specifically enough to give notice to criminal violators to fulfill deterrence and due process functions? Particularly, does the term "computer" include other systematic electronic applications of data features beyond the stand-alone computer set, i.e. monitor, keyboard, and central processing unit? For example, does the term include Wireless Application Protocol?[17] Second, is the term "computer" general enough to include any anticipated future computer technology-related crime?[18]

---

consensus. There are basically two approaches—legislative and academic: the former focuses on harm and the latter is oriented to causation. *See Research Needs for Computer Crime Introduction*, Computer Crime Research Center (2000-2001), *available at* http://www.crime-research.org/eng/library/Introduction.htm (last visited Apr. 20, 2005).

[14] Some of the earlier works include Matthew K.O. Lee, *Legal Control of Computer Crime in Hong Kong*, 3.2 INFORMATION MANAGEMENT & COMPUTER SECURITY 13-19 (1995), *available at* http://docserver.emeraldinsight.com/deliver/cw/mcb/09685227/v3n2/s3/p13.pdf?fmt=dirpdf&tt=1177&cl=82&ini=emerald&bini=&wis=emerald&ac=0&acs=291,3039,11035592,292939&expires=1109121988&checksum=EE9509F8B2D8C0D890512AD517F94B94&cookie=2115113088 (last visited Apr. 20, 2005); Lau et al, *supra* note 12; Bina Cunningham, *Cyber Crime—How Do We Fight It: A Hong Kong Perspective*, Denton Wide Sapte Publications (March 1, 2001), *available at* http://www.dentonwildesapte.com/assets/C/CyberCrime_HKPerspective_Mar01.pdf (last visited Apr. 20, 2005).

[15] In 1992 the Hong Kong Chamber of Commerce's Information Services Committee submitted a detailed response to the government's proposed Computer Crimes Bill, raising for the first time the issue of definition of computer crime. *See Report on Inter-Departmental Working Group on Computer Related Crime Response by the Hong Kong General Chamber of Commerce*, Comments of Hong Kong General Chamber of Commerce (Feb. 2001), *available at* http://www.hkcsi.org.hk/old/papers/report/computer_crime.htm (last visited Apr. 20, 2005).

[16] *See* HKSAR Computer Crime Report, *supra* note 11, at 10-20, specifically para. 3.7, *available at* http://www.hkispa.org.hk/pdf/ComputerRelatedCrime.pdf (last visited Apr. 20, 2005).

[17] *See id.*, para. 3.8.

[18] *See id* at 10-20, para. 3.7: "In a narrow sense, the term "computer" commonly conjures up the image of a stand-alone machine .... However, in a broader sense ... the term is increasingly taken to refer to a whole host of other items such as networked computer systems and many mobile electronic communication devices." *Id.* at 12, para. 3.7. The HKSAR Computer Crime Report intimated due notice concerns without explicit discussion. *See id.* at para. 3.8. The report completely ignored the need to discuss issues presented by the specificity of legislative definition and administrative of justice. *See generally* Marc Ribeiro, LIMITING ARBITRARY POWER: THE VAGUENESS DOCTRINE IN CANADIAN CONSTITUTIONAL LAW

After reviewing seventy-six sections in thirty-five Hong Kong ordinances,[19] the HKSAR Computer Crime Report recommends defining "computer" as an "information system,[20] as defined in the Electronic Transactions Ordinance (Ch. 553)."[21] The Electronic Transactions Ordinance does not define "computer," but uses "information system" to mean: "a system which . . .

> (a) processes information;
> (b) records information;
> (c) can be used to cause information to be recorded, stored or otherwise process [sic] in other information system (whatever situations); and
> (d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated)."[22]

But what is "computer crime"? The HKSAR Computer Crime Report (2000) acknowledges that: "The terms 'computer crime' and 'computer related crime' are rather amorphous . . . ."[23] These terms can refer to crimes directed at a computer (like hacking), crimes using computer as the medium (such as Internet gambling), and crimes where the computer plays a minimal role (e.g. online pornographic advertising).

The term "computer crime" generally refers to three kinds of crimes, namely, computer crime in the strict sense, computer-related crime, and computer abuse.[24] According to one computer crime expert, cybercrime cases may involve computers in any one or more of the following roles:

(University of British Columbia Press, 2004).

[19] HKSAR Computer Crime Report, *supra* note 11, at para. 3.10. For a list of ordinances reviewed, see Annex 3.

[20] *Id.* at para. 3.10.

[21] *Id.* at para. 3.9.

[22] Electronic Transactions Ordinance (Ch. 553) (H.K.).

[23] HKSAR Computer Crime Report, *supra* note 11, at para. 3.9.

[24] For a historical development of computer crime *see* Sam McQuade, *So-called 'Cybercrime': Its Nature and Manageability*, An Appendix Report Submitted for Inclusion in The President's Commission Final Report on Critical Infrastructure Protection (Aug. 1997), *available at* http://www.rit.edu/~scmgcj/CYBERCRIME%20-%20PCCIIP%20Appendix%20Report.htm (last visited Apr. 20, 2005). The author argues for a change of paradigm (see discussion of paradigm shifts in Thomas S. Kuhn, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (University of Chicago Press 1962)). McQuade prefers the use of the term "cybercrime" over computer crime, because digital technology allows crime to move away and beyond the narrow confines of computer crime to other emerging fields of vulnerabilities, such as alternation of digital photography and stealing of digital images.

1. Computer as object—such as destruction of computers or computer data or programs contained in a computer;
2. Computer as subject—such as fraud cases where financial data is being illegally changed;
3. Computer as 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;
4. Computer as symbol—such as using non-existent computers for intimidation or deception.[25]

A more conceptual definition of computer crime is supplied by Dennis Longley and Michael Shain: "[W]illful or negligent unauthorized activities that affect the availability, confidentiality and integrity of computer resources."[26] Availability of computer resources might be affected in cases of denial of services attacks, such as spam.[27] Confidentiality of computer resources might be compromised by means of unauthorized intrusion, such as hacking.[28] The integrity of computer data might be compromised when hackers try to steal, alter, contaminate or destroy existing databases.[29]

The difficulty with defining computer crime becomes apparent when applied. For example, if a computer is stolen to obtain the proprietary data or operational software, it is not classified as a computer crime. However, if

---

[25] *See* Donn B. Parker, *Computer Crime*, ENCYCLOPEDIA OF COMPUTER SCIENCE, at 349-53 (Nature Publishing Group, 4th ed. 2000). Unless otherwise specified, the terms "computer crime," "computer-related crime," "cybercrime," "computer abuse" and "Internet crime" are used interchangeably throughout this Article.

[26] W. CAELLI, D. LONGLEY & M. SHAIN, INFORMATION SECURITY HANDBOOK (1991). Another definition is supplied by University of South California Office of Information Security: "Computer Abuse: The willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation." UNIVERSITY OF SOUTHERN CALIFORNIA, OFFICE OF INFORMATION SECURITY, *Glossary*, *available at* http://www.usc.edu/org/infosec/resources/glossary_a.html (last visited Apr. 20, 2005). For a more technical discussion, *see* CERT COORDINATION CENTER, *Security of the Internet*, *available at* http://www.cert.org/encyc_article/tocencyc.html (last visited Apr. 20, 2005).

[27] *83% of U.S. E-Mail Is Spam*, SECURITY PIPELINE (May 25, 2004), *at* http://informationweek.securitypipeline.com/howto/21100194 (last visited Apr. 20, 2005). *See also* Frank Jargl et al., *Protecting Web Servers from Distributed Denial of Service Attacks*, 10th International World Wide Web Conference Refereed Papers, *at* http://www10.org/cdrom/papers/409/ (last visited Apr. 20, 2005).

[28] *Study: Israel, Hong Kong Hotbeds for Hacking Attacks*, SILICONVALLEY.COM, July 8, 2002, *at* http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3624610.htm (last visited Apr. 20, 2005).

[29] D. Ian Hopper, *"I LOVE YOU" Computer Bug Bites Hard, Spreads Fast*, CNN.COM, May 4, 2000, *at* http://archives.cnn.com/2000/TECH/computing/05/04/iloveyou.01 (last visited Apr. 20, 2005). The "I LOVE YOU" viruses substituted existing Web development (including ".js" and ".css" files) and multimedia files (JPEGs and MP3s) with a VisualBasic file with a similar name. It started with an attack in Hong Kong and moved west. *Id.*

knowledge of computer technology is used to access and download the data from the same computer, it is. Yet both crimes involve the theft of electronic data in common law terms, that is "taking, carrying away, property of another, if intent to permanently deprive the owner thereof."[30] Traditional computer crime concepts do not cover new and emerging criminality with the use of other digital technology, such as theft of software in a camera or illegal interception of telecommunication services.[31]

B. *Difficulties with Ascertaining the Nature and Extent of Computer Crime*

Hong Kong faces difficulties in ascertaining the nature, extent and distribution of computer crime. This has made preventing and controlling computer crime more problematic.[32] The main problem is in capturing "dark figures"[33]—undetected, unreported and/or unrecorded[34] instances of cybercrime.[35] For examples, the FBI's National Computer Crime Squad estimates that between eighty-five and ninety-seven percent of computer intrusions in the United States are not even detected,[36] much less reported.[37]

---

[30] For a law enforcement view on problems with defining computer crime, *see* Paul A. Curtis, *Cyber Crime: The Next Challenge An Overview of the Challenges Faced by Law Enforcement While Investigating Computer Crimes in the Year 2000 and Beyond* 5-6, *available at* http://www.cji.net/CJI/CenterInfo/lemc/papers/Cyber%20Crime%20Paper.pdf (last visited Apr. 20, 2005). For problems and issues of defining computer crime generally, *see* Ronald B. Standler, *Computer Crime*, *available at* http://www.rbs2.com/ccrime.htm (last visited Apr. 20, 2005).

[31] For a discussion on definitions problems with computers, *see* Legislative Needs *in Research Needs for Computer Crime Introduction*, *available at* http://www.crime-research.org/library/Introduction.htm (last visited Apr. 20, 2005).

[32] *See* M. E. Kabay, *Understanding Studies and Surveys of Computer Crime*, *at* http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.pdf (last visited Apr. 20, 2005) [hereinafter Kabay]. *See also* M. E. Kabay, *ICSA White Paper on Computer Crime Statistics*, *at* http://www.icsa.net/html/library/whitepapers/crime.pdf (last visited Apr. 20, 2005).

[33] The magnitude of "dark figures" of computer crime in Hong Kong is huge, and increasing. *See* HONG KONG COMPUTER EMERGENCY RESPONSE TEAM, INFORMATION SECURITY SURVEY OF 2003, *available at* http://www.hkcert.org/articles/sec2003_report.pdf (last visited Apr. 20, 2005). Only 0.3% of the respondents reported computer attacks to the police in both 2002 and 2003. *Id.* at 16. "Dark figures" are not the only problem in understanding the extent of computer crime. The modes of committing a "computer crime" are not the same everywhere. Computer hardware, software, and security structure all contribute to possible security breaches. Accounting for all these technical specifications will be difficult if not impossible when faced with millions of attacks a year. *Id.*

[34] *See* Kabay, *supra* note 32. *See also The Use, Misuse and Abuse of Statistics in Information Security Research*, Proceedings of the 2003 ASEM National Conference, St. Louis, Mo., *available at* http://www.attrition.org/archive/misc/use_misuse_abuse_stats_infosec_research.pdf (last visited Apr. 20, 2005) (two researchers reviewed the data and caution against its use due to methodology and validity problems).

[35] For a general discussion of detection and reporting problems, *see* Steven D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 HARV. J.L. & TECH. 699 (Spring 1998).

[36] *See* Kabay, *supra* note 32.

In a Congress-requested study, the Government Accounting Office found that the Department of Defense may have been the victim of as many as 250,000 intrusions in 1995.[38] Only one in 150 intrusions was detected and reported.[39] Department of Defense data also showed that it was able to penetrate the department's own security sixty-five percent of the time.[40]

Hong Kong faces similar dark figures of computer crime problems.[41] Computer viruses enter surreptitiously and are well hidden within computer architecture, waiting to be exploited at will or to explode at a designated time. In most cases, the owners or users are not aware of an ongoing attack, still less the scope and extent of the damages, until months or years afterward.[42]

Most computer crime victims choose not to report computer crimes.[43] Many corporations, especially those in financing and personal service sectors, are reluctant to report because reporting betrays trade secrets, reveals clients' confidences, draws attention to an insecure e-business platform, reflects poor internal control, and more generally undermines good will. In the United States, the 2004 annual CSI/FBI Computer Crime and Security Survey[44] uncovered the following reasons for non-reporting of computer crime: negative publicity (51%), fear that competitors would use the report to their advantage (35%), lack of awareness of reporting (18%), belief that civil remedies seemed better (20%).[45]

In Hong Kong, non-reporting of computer crime results from a number of factors: ignorance of crime or harm; uncertainty of detection, prosecution, or punishment; expensiveness of detection measures; fear of consequences such as damage to public image, revealing of weaknesses, and exposure to civil liabilities; difficulty in assessing loss of information, such

---

[37] *See id.*

[38] GENERAL ACCOUNTING OFFICE, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS, GAO/AIMD-96-84 (1996), *available at* http://www.gao.gov/archive/1996/ai96084.pdf (last visited Apr. 20, 2005).

[39] *Id.* at 3.

[40] *Id.* at 2.

[41] *See* Hilton Kwok Hung Chan, Comparative Study of Reported and Unreported Computer Crimes (2000) (Ph.D. dissertation, Hong Kong University of Science and Technology), *available at* http://lbxml.ust.hk/th_imgo/b672003.pdf (last visited Apr. 20, 2005).

[42] For example, the original Klez virus/worm program appeared on October 26, 2001. The virus was deposited in victim's computer and destroyed information in all files on the victim's computer on March 13 and September 13 of each following year. *See* Ronald B. Standler, *Examples of Malicious Computer Programs* (2002), *at* http://www.rbs2.com/cvirus.htm (last visited Apr. 20, 2005).

[43] Brian J. Peretti, *Computer Crime:Current Practices, Problems and Proposed Solutions*, *available at* http://www.etext.org/CuD/Papers/computer.crime (last visited Apr. 20, 2005).

[44] Lawrence A. Gordon et al., *2004 CSI/FBI Computer Crime and Security Survey*, *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf (last visited Apr. 20, 2005).

[45] *See id.*at Figure 21 and related text.

as customer data base or proprietary information; lack of motivation where data was not insured or insurable; and corporate executives' views of computer crime as internal business problems rather than external criminal matters. Finally, when computer crime is discovered, it might be too late to report. Many information technology and business professionals believe that the most cost-effective way to deal with computer crime is not through the criminal justice system, but through self-help.[46] As of now, the private sector has little confidence in the HKG's ability to deal with computer crime problems.[47]

C. *Problems with Accessibility to Data on Computer Research*

There is a need for valid and reliable data to support theoretically driven and empirically based computer crime and cyberspace governance research in Hong Kong. Computer crime data in Hong Kong is maintained and reported by a number of agencies, including the Information Technology Services Department, Hong Kong Police, and the Customs and Excise Department. There is, however, no uniform computer crime reporting system like that of the FBI/Uniform Crime Report in the United States. Questions related to Hong Kong's computer crime situation abound: what is the nature, extent, and distribution of computer crime in Hong Kong? More importantly, what are the causes, impacts and implications of computer crime? Effective cyberspace governance requires the development of a database that could help answer these questions.[48]

III. THE DISCOVERY OF CYBER RISKS, COMPUTER CRIME AND ELECTRONIC PRIVACY

Cyber risk is a psychological phenomenon. Computer crime is a virtual entity. Electronic privacy is a moral concept. All of these threats are not material or tangible. Thus, in order for them to be taken seriously, they have to gain public awareness in the sense of cognitive recognition and emotional resonance.

---

[46] For a professional's view on computer self-help, *see* David Loundry, *Internet Governance Through Self-Help Remedies*, COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY NEWSLETTER (Summer 1998), *available at* http://www.loundy.com/CPSR-Self-Help.html (last visited Apr. 20, 2005). For a theoretical treatment, *see* Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261 (2003).

[47] *See* Chan, *supra* note 41, at 123-24.

[48] The HKSAR Computer Crime Report, *supra* note 11, failed to address these issues, but nevertheless proceeded to offer solutions to rein in computer crimes.

Historically and culturally, China has had no conception of intellectual rights.[49] Historically, people were expected to cite past lessons to explain and justify contemporary actions. Culturally, sage writings were thought to contain the secrets of Chinese civilization. Generations of students were taught to recite the classical literature of old.[50] Not only is it not a crime to recite classical authorities without attribution, but it is a sign of intellectual prowess.[51]

Hong Kong was a barren island when ceded to England.[52] Many consider the Hong Kong people to be "survivors." Popularly, they are known for making fast money more than for following established principles, as people who work hard at getting things done rather than honoring the rights of others. To them, anything and everything in life is a "game" to be won at all costs.[53]

Given China's historical approach to intellectual property and contemporary Hong Kong society's attitude toward copyrights, it should come as no surprise that intellectual property rights and computer crime are not taken seriously in Hong Kong.[54] It takes time for the Hong Kong people to adopt new cultural values.

The "discovery" of computer crime and privacy resulted from the convergence of a number of factors, including post-1997 privacy concerns, government information technology security needs, private e-banking security considerations, foreign anti-privacy and anti-counterfeiting campaigns, domestic moral outrage with offshore Internet gambling, and public awareness of sensational computer crime news.[55]

---

[49] Peter Yu, *The Second Coming of Intellectual Property Rights in China* 11 *in* BENJAMIN N. CARDOZO SCHOOL OF LAW OCCASIONAL PAPERS IN INTELLECTUAL PROPERTY No. 11 (2002).

[50] *See generally* MICHAEL NYLAN, THE FIVE "CONFUCIAN" CLASSICS (2001), *available at* http://yalepress.yale.edu/YupBooks/pdf/0300081855.pdf?winOpen=true (last visited Apr. 20, 2005).

[51] *See* Peter Yu, *supra* note 49, at 16-17. *See generally* WILLIAM P. ALFORD, TO STEAL A BOOK IS AN ELEGANT OFFENSE: INTELLECTUAL PROPERTY LAW IN CHINESE CIVILIZATION (1995).

[52] FRANK WELSH, A HISTORY OF HONG KONG 133 (1993).

[53] *See* FUNG CHI PANG, SINGING AGAINST HONG KONG PEOPLE (1998). *See also* RICHARD HUGHES, BORROWED PLACE BORROWED TIME (1968). For a more detailed analysis of Hong Kong people's social psychology, see George Adams, *Games Hong Kong People Play—A Social Psychology of the Hong Kong Chinese*, *available at* http://www.ntscmp.com/games.htm (last visited Apr. 20, 2005).

[54] *See* Press Release, HKSAR, Survey on Public Awareness of Importance of Protecting Intellectual Property Rights 2002 (Dec. 3, 2002), *available at* http://www.info.gov.hk/gia/general/200212/03/1203100.htm (last visited Apr. 20, 2005).

[55] *Statement Concerning Police Action on Internet Providers* (Mar. 4, 1995), *available at* http://courses.cs.vt.edu/~cs3604/lib/Crime/hongkong.html (last visited Apr. 20, 2005).

A. *Post-1997 Privacy Concerns*

One of the driving forces behind ensuring the security of computer data and privacy safeguards on the Internet comes from a most unexpected source: pre- and post-1997 politics. In 1984, the Sino-British Joint Declaration paved the way for the return of Hong Kong to China on July 1, 1997.[56] The Joint Declaration provided that the rights and freedoms enjoyed by the Hong Kong people would last for fifty years, to be secured by a Basic Law.[57] Specifically, Article 3 of the Declaration provided in pertinent part:

> Rights and freedoms, including those of the person, of speech, of the press, of assembly, of association, of travel, of movement, of correspondence, of strike, of choice of occupation, of academic research and of religious belief will be ensured by law in the Hong Kong Special Administrative Region.[58]

The Basic Laws of Hong Kong of 1997[59] specifically provide for the guarantee of basic human rights. Article 30 provides that the "freedom and privacy of communications of Hong Kong residents shall be protected by law."[60]

The work of the Hong Kong Law Reform Commission on "Reform of the law relating to the protection of personal data"[61] ("1994 Report") was part of the process of institutionalizing privacy rights of individuals against interception and disclosure. In December 1996, the Law Reform Commission reviewed the electronic data interception, interference, and theft issues in "Report on Privacy: Regulating the Interception of Communications" ("1996 Report"),[62] observing: "[t]he rapid expansion of

---

[56] Sino-British Joint Declaration on the Question of Hong Kong, Dec. 19, 1984, P.R.C.-U.K.

[57] The drafting of Basic Law began in 1985 when the National People's Congress appointed the Basic Law Drafting Committee, composed of more than fifty mainland and Hong Kong members. *See* Eva Liu & S.Y. Yu, *Political Development in Hong Kong Since 1980s*, Research and Library Division, Legislative Council Secretariat (September 1996), at 3.

[58] The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (1990), *available at* http://www.info.gov.hk/basic_law/fulltext/index.htm (last visited Apr. 20, 2005) [hereinafter Basic Law].

[59] *Id. See also* YASH GHAI, HONG KONG'S NEW CONSTITUTIONAL ORDER: THE RESUMPTION OF CHINESE SOVEREIGNTY AND THE BASIC LAW (2d ed. 1999).

[60] Basic Law, *supra* note 58.

[61] LAW REFORM COMMISSION OF HONG KONG, REFORM OF THE LAW RELATING TO THE PROTECTION OF PERSONAL DATA (Aug. 1994), *available at* http://www.hkreform.gov.hk/reports/rdata-e.pdf (last visited Apr. 20, 2005).

[62] The 1996 Report's "Terms of References" were anchored to *Reform of the Law relating to the Protection of Personal Data*: "The issues raised at items (a) and (b) in the terms of reference were

the Internet, and the resultant increase in the amount of personal information available online, has made the public more concerned about the privacy of their communications. Service companies are likely to use privacy as a competitive weapon in winning customers."[63] More ominously, the 1996 Report warned of the coming privacy crisis: "The development of advanced communications networks is likely to be hindered unless service carriers can assure the public that there is adequate security for their communications."[64] While the 1996 Report mainly addressed government interception of electronic data and intrusion into computer domain, the warning applies equally to any kind of cyberspace interception and intrusion.

The review of the 1997 sovereignty change and law reform in Hong Kong makes it clear that the "discovery" of computer crime and privacy in Hong Kong was driven by many forces and made advances along a number of paths. The first step in discovering any computer-related crime problem is for it to be recognized cognitively and emotionally by the general public. The following sections describe the many ways in which computer crime and privacy has entered the Hong Kong people's psyche, ethos, and culture.

B. Private E-Banking Security Study

In the mid-1990s, the HKG became concerned about electronic security in business and government transactions. In 1997 the Hong Kong Monetary Authority ("HKMA"), the quasi-government banking watchdog, launched one of the first computer crime and information security studies in Hong Kong, called "Security of Banking Transactions over the Internet" ("1997 Study").[65] The study sought to identify the security risks associated with e-banking in Hong Kong. The HKMA has a statutory duty under the Seventh Schedule to the Banking Ordinance to require banks to maintain adequate accounting systems and adequate systems of control "to mitigate the risk of loss of confidentiality and the risk of unauthorized access to institutions' internal computer systems."[66] The major security risks identified by HKMA in the 1997 Study were false authentications,

---

addressed in the Law Reform Commission report on *Reform of the Law relating to the Protection of Personal Data* published in August 1994. Most of the recommendations of that report were adopted with the enactment of the Personal Data (Privacy) Ordinance (Ch. 486) (H.K.) on August 3, 1995. This Report deals mainly with item (d)." *See* LAW REFORM COMMISSION OF HONG KONG, *Introduction* to REPORT ON PRIVACY: REGULATING THE INTERCEPTION OF COMMUNICATIONS, *available at* http://www.hkreform.gov.hk/reports/rintercept-e.doc (last visited Apr. 20, 2005).

[63] *Id.* at para. 10(b).

[64] *Id.* at para. 10(d).

[65] *See Security of Banking Transactions over the Internet*, *supra* note 11.

[66] *Id.*

interception of information en route, and unauthorized access to databases. The HKMA concluded with this observation:

> The use of sophisticated cryptographic techniques, firewalls and other security tools can provide security that is comparable to that offered in physical transactions. However, similar to a physical transaction, the effectiveness of such measures would be largely dependent on their proper implementation and the establishment of a set of comprehensive policies and procedures that are rigorously enforced.[67]

The 1997 Study placed the issues of computer malfeasants and electronic transactional risks squarely on the table, first as a private e-business obstacle to overcome in launching e-banking, and later as a public information technology policy to be debated in developing Hong Kong's "Cyberport" project.[68] In hindsight, the importance of the 1997 Study goes far beyond merely highlighting e-banking risks in an electronic age. The Study helped to raise public consciousness of the emergence of computer crimes and privacy. In so doing, it set the agenda and defined the issues for future debate over the shape and contours of the HKG's cyberspace governance policy.

C. *Government IT Security Concerns*

In 1999, the HKG formally launched the Cyberport project as part of its overall economic development plan. The success of the Cyberport project ultimately depends on a safe and risk-free IT infrastructure environment. In the late 1990s, the HKG introduced ways to regulate cyberspace to make it safer. In June 2001, Cheung Siu-hin, the Deputy Secretary for Security of Hong Kong, announced the government's cyberspace governance philosophy and computer security strategy.[69] From

---

[67] *Id.*

[68] *See* CYBERPORT, *Project Scope*, *available at* http://www.cyberport.com.hk/article/cp_info_en/cpa_00002_en.html (last visited Apr. 20, 2005). "Cyberport is a symbol of Hong Kong's unwavering determination to develop as a leading Information Technology (IT) and digital city in the region. At an estimated cost of US$2 billion (HK$15.8 billion), this landmark project aims to create a creative and interactive environment that will be home to a strategic cluster of more than one hundred IT companies and over 10,000 IT professionals." *Id.*

[69] Cheung Siu-hing, *Information Security: Whose Responsibility?*, Address at the Internet Commerce Exposition and Conference (June 28, 2001), *available at* http://www.info.gov.hk/gia/general/200106/28/0628131.htm (last visited Apr. 20, 2005). The HKG acknowledged that regulations cannot be the only answer to information security. *Id.*

the beginning, the question has always been one of how to regulate the cyberspace, and not whether to regulate. As the Secretary put it, the issue is between having an Orwellian Big Brother "watching our every move" and having some basic rules for the information highway.[70] The Hong Kong government's approach has been to "treat regulation as the means to establish minimum ground rules to secure fair play."[71] HKG recognized that regulations cannot be the sole solution to cyberspace security. The best strategy is to educate the public about computer crime and promote self-help, for example by guarding against online identity theft and working with private-sector Internet service providers to reduce security risks.[72] The HKG media promotion and public education effort has been instrumental in making the public aware of computer crime and privacy problems and issues.

D. The Foreign Anti-Piracy Campaign

In the 1990s Hong Kong was known as the technological piracy capital of Asia.[73] A 1996 IIRA 301 Country Report described the piracy problem in vivid terms:

> CD-ROMs containing pirated computer software, both business applications and entertainment titles, are flooding the market in Hong Kong. Seizures of these pirate CD-ROMs skyrocketed from 5400 in 1994 to 176,872 in the first nine months of 1995, a 44-fold increase on a monthly basis. This contraband often takes the form of compilations .... For instance, the latest versions of Autodesk's AutoCAD Release 13 (retail price US $4,250), Novell's NetWare 4.1 (retail price $2,845) and Lotus's Smartsuite were packaged with over 100 other programs owned by different companies and sold openly in Hong Kong in October 1995 for HK $50 (US $6.50). Pirated versions of Microsoft's Windows 95 were on sale at the Golden Shopping

---

[70] *Id.*

[71] The Hong Kong government's position raises more questions than it resolves. First, what is meant by "minimum ground rules" is not ascertainable in the abstract, and certainly is a matter of degree. Second, the question of who defines "minimum" needs to be resolved. Ultimately, the debate is not about how much to rule (a technocratic calculus), but what is the end, means, object and people to be regulated (a jurisprudential, qua political, debate).

[72] *Id.*

[73] *See* E.A. Gargan, *Pirate's Bazaar Thrives in Hong Kong*, N.Y. TIMES (Feb. 27, 1995).

Arcade within a week of the operating system's launch on August 24, 1995.[74]

Hong Kong retail computer software piracy also took place in cyberspace. In August 1996, the Business Software Alliance ("BSA"), working closely with the Alliance Against CD-ROM Theft, closed down an Internet site called Sammy Game Center, which offered illegal CD-ROM products for sale and export to the United States, the Netherlands, Sweden and Canada, via the Internet.[75]

The economic impact of Hong Kong piracy and counterfeiting on the foreign intellectual property industry is great. The economic impact on Hong Kong is described in Table 1; the data demonstrates that losses from piracy and counterfeiting greatly increased from 1995 to 1998.

Table 1: Estimated Trade Losses (in Millions of U.S. Dollars) Due to Piracy & Levels of Piracy in Hong Kong: 1995-1998[76]

	1995		1996		1997		1998	
INDUSTRY	Loss	Level	Loss	Level	Loss	Level	Loss	Level
Motion pictures	10	4%	15	15%	20	20%	30	20%
Sound recordings and musical compositions	5	13%	18	20%	20	20%	30	60%
Computer programs: business applications	88.7	62%	89	65%	92.9	67%	69.2	59%
Computer programs: entertainment software	112.2	74%	115.7	73%	110.9	70%	112.3	72%
Books	2	N/A	2	N/A	2	N/A	2	N/A
TOTAL	217.9		239.7		245.8		243.5	

The foreign intellectual property commercial interests—film, music, theater, software, retailing, broadcasting and information technology industries—have adopted a two-prong strategy to prevent the spread of pirated software in Hong Kong. First, they conducted a public education program and awareness campaign to highlight the magnitude and seriousness of the piracy problem, as seen in the anti-piracy march in Hong

[74] IIPA SPECIAL 301 RECOMMENDATIONS (Feb. 20, 1996), *available at* http://www.iipa.com/rbc/1996/rbc_hong_kong_301_96.html (last visited Apr. 20, 2005).

[75] GRAYZONE DIGEST (Sept. 1996), *available at* http://www.grayzone.com/996.htm#hongkong (last visited Apr. 20, 2005).

[76] IIPA SPECIAL 301 RECOMMENDATIONS FOR THE YEAR 1999, *available at* http://www.iipa.com/rbc/1999/rbc_hong_kong_301_99.html (last visited Apr. 20, 2005).

Kong on March 17, 1999.[77] The message was as clear as it was dire: copyright piracy was causing serious losses to the Hong Kong economy and grave harm to Hong Kong's reputation as an international trading center. Piracy of intellectual property is a crime. Hong Kong people should not buy pirated goods. The public was urged to appeal to the HKG to take resolute measures to fight the crime of piracy.[78]

Second, commercial companies applied legal and economic pressure, by lobbying the U.S. Trade Representative ("USTR") to seek so-called Section 301 trade sanctions against Hong Kong to clamp down on piracy and counterfeiting. For example, in 1995 the International Intellectual Property Alliance ("IIPA"), acting on behalf of the industry, requested that Hong Kong be placed on Special 301 Mention status as a result of increased flow of pirated materials from China into Hong Kong.[79] In 1996 IIPA requested placing China on a Watch List to compel the HKG to devote more resources to copyright enforcement. In 1997 IIPA succeeded in convincing USTR Ambassador Charlene Barshefsky to place HKG on the 301 Watch List. In 1998, the USTR agreed with IIPA and kept HKG on the Watch List.[80]

IIPA public pressure and trade sanctions strategies worked in encouraging the HKG to pass more stringent laws against piracy. This included laws requiring the licensing of compact-disc copying machines and more aggressive enforcement actions against counterfeiters, such as raids.[81]

On December 16, 1998, Selina Chow, HKSAR Legislative Council ("LegCo") representative for the retail industry, made the following floor motion:

> [I]n view of the recent proliferation of pirated compact discs in

---

[77] Press Release, GrayZone Quarterly Digest, Hong Kong Anti-Piracy March (March 17, 1999), *available at* http://www.grayzone.com/hkmarch99.htm (last visited Apr. 20, 2005).

[78] Press Release, IFPI, Hong Kong Anti-Piracy Day a Major Success (March 17, 1999), *available at* http://www.grayzone.com/hk31799.htm (last visited Apr. 20, 2005).

[79] INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE, COPYRIGHT ENFORCEMENT UNDER THE TRIPS AGREEMENT, *available at* http://www.iipa.com/rbi/2004_Oct19_TRIPS.pdf (last visited Apr. 20, 2005). On January 1, 1996, the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") went into effect. In general terms, TRIPS requires an enforcement system that permits effective action against infringements, provides expeditious remedies that constitute a deterrent, is fair and equitable, is not unnecessarily complicated or costly, and does not entail any unreasonable time limits or unwarranted delays. TRIPS requires that member countries apply their criminal laws in cases of commercial piracy; it is not enough to merely have laws on the books if those laws are not used effectively. Failing that, USTR can impose trade sanctions. *Id.*

[80] IIPA HONG KONG COUNTRY REPORT 1999, *available at* http://www.iipa.com/rbc/1999/rbc_hong_kong_301_99.html (last visited Apr. 20, 2005).

[81] Legislative Council Agenda (Dec. 16, 1998), A 98/99 -20(1), *available at* www.legco.gov.hk/yr98-99/english/counmtg/agenda/ord1612.htm (last visited Apr. 20, 2005).

> various districts, this Council urges the Government to immediately review the existing policies and strengthen the co-ordination of various law enforcement authorities, so as to combat more effectively the manufacture, importation and sale of pirated video, music and software compact discs; furthermore, the Government should strengthen its publicity and education programmes with a view to making the public aware that the infringement of intellectual property rights is immoral; this Council also urges the Government to actively consider amending the relevant legislation in order to empower the law enforcement authorities to prosecute those engaged in the pirated recording of movies in cinemas and consider the imposition of fines on purchasers of pirated compact discs, thereby achieving deterrent effects.[82]

In February 1999, the HKG published a consultation paper entitled "Combating Intellectual Property Rights Infringement in the Hong Kong Special Administrative Region: Possible Additional Legal Tools."[83] The paper proposed a number of measures to fight piracy and counterfeiting, such as:

1. Including piracy and counterfeiting offences under the Organised and Serious Crimes Ordinance;
2. Amending the Copyright Ordinance and the Trade Descriptions Ordinance to provide for the confiscation of criminal proceeds from intellectual property infringement offences;
3. Introduction of mandatory or standard sentences for copyright and trade mark offences;
4. Closure orders against premises used repeatedly for piracy or counterfeiting activities;

---

[82] Hon. Selina Chow, "Combating pirated compact discs," Motion on the floor of the Legislative Council (Dec. 16, 1998) (English translation) *available at* http://www.legco.gov.hk/yr98-99/english/counmtg/agenda/ord1612.htm (last visited Apr. 20, 2005).

[83] *See* list of the HKG proposals at Jeannie Smith, *New Legislation To Shake Up Rights Scene*, IP PROFILE (2000), http://www.asialaw.com/directories/ipprofiles2000/hongkong/ (last visited Apr. 20, 2005). For a response from the software industry, see Hong Kong Software Industry Comments on June 1999 Trade and Industry Bureau Submission to The Legislative Council Panel on Trade and Industry, CB(1)1457/98-99(02) (June 3, 1999), *available at* www.legco.gov.hk/yr98-99/english/panels/ti/papers/ti07064g.htm (last visited Apr. 20, 2005).

5. Immediate closure orders for premises used for piracy or counterfeiting activities;
6. Banning unauthorized video recording in cinemas;
7. Banning video equipment in cinemas; and
8. Imposing consumer liability.[84]

As a result of the consultation process, the LegCo passed an amendment to the Organized and Serious Crimes Ordinance to include piracy and counterfeiting offenses.[85] On January 12, 2000, it also proposed criminalizing the possession of an infringing article other than for personal domestic use.

On June 22, 2000, the Internet Task Force of Hong Kong Customs conducted the first raid in Hong Kong against an Internet site selling pirated software, where Microsoft Windows 2000, Microsoft Project 2000 and Symantec pcAnywhere were sold at HK $20 per copy.[86] The foreign anti-piracy movement has had the net effect of persuading the Hong Kong public to respect intellectual property rights and moved the HKG to be more protective of them.

E. Moral Outrage and Economic Pressure Against Internet Gambling

Gambling is a favorite pastime in Hong Kong.[87] An HKG survey shows that in May 2001, 2.4% (120,000 people) of the Hong Kong population engaged in soccer gambling.[88] The annual turnover of soccer gambling amounted to HK $200 billion a year.[89]

The HKG's policy toward gambling has been to "restrict gambling opportunities to limited and authorized gambling outlets only."[90] This policy concedes that unregulated gambling would only contribute to

---

[84] Smith, *supra* note 83.

[85] Organized and Serious Crimes Ordinance (Amendment of Schedule 1) Order 1999 (H.K.). The Amendment allowed copyright piracy and trademark counterfeiting offenses to be included under Schedule 1 and empowered the Customs and Excise officers to take action against counterfeiters. *Id.*

[86] Hong Kong Customs First Crackdown on Online Sale of Pirate Software (Jun. 28, 2000), http://www.microsoft.com/hk/licenses/cases.htm (last visited Apr. 20, 2005).

[87] *See* Michelle Levander, *Log On Your Bets*, ASIA TIMES, Nov. 5, 2001 (first-person account of gambling in Hong Kong).

[88] HOME AFFAIRS BUREAU, PUBLIC CONSULTATION ON GAMBLING REVIEW: CONSULTATION REPORT (Mar. 22, 2002), *available at* http://www.hab.gov.hk/en/whats_new/gambling/public_consult.htm (last visited Apr. 20, 2005). The figure is underestimated because of respondents' unwillingness to admit to illegal gambling to government pollsters and the survey did not include people who bet through friends. *Id.*

[89] *Id.* at para. 3.6.

[90] *Id.* at para. 3.2.

unlimited gambling, underage gambling, gambling fraud, and a loss of revenue for charity.[91]

Offshore (Internet) gambling challenged the monopoly of the Hong Kong Jockey Club ("HKJC"), the only authorized gambling house in Hong Kong. With the discovery of the information highway, Internet gambling has become the betting avenue of choice. Hong Kong residents visiting gambling sites almost doubled between October and December of 1999—from twenty-two to forty-one percent of the population.[92]

The HKJC has asked the HKG to pass legislation outlawing offshore bookmaking.[93] In May 2002, LegCo amended the Gambling Ordinance[94] to include a ban on offshore gambling, with a maximum sentence of seven years in jail and HK $5 million in penalties for brokers, and nine months in prison and a HK $30,000 fine for gamblers. The legislative victory against offshore gambling was a result of two potent forces at work: one economic and the other moral.

Economically, the HKG and HKJC stood to lose billions every year if Internet gambling was not regulated. Morally, there was great public outcry against gambling.[95] Gambling was considered a vice that would destroy individuals,[96] ruin families,[97] corrupt youth,[98] and divide societies.[99] Yet in the Gambling Ordinance amendment, the HKG, HKJC, and religious and

---

[91] *Id.* at para 2.2.

[92] *Hong Kong Battle Against Internet Betting Continues*, THOROUGHBREDTIMES.COM, Dec. 11, 2004, *reprinted at* http://www.thoroughbredtimes.com/todaysnewsarchive/ttodaysnewsviewarchive.asp?ArchiveDate=12/11/2001#18189 (last visited Apr. 20, 2005).

[93] *Internet Gambling Leaves Hong Kong Out Of Pocket, Inside China*, SHANGHAI STAR, Mar. 15, 2003. HKJC estimates it was losing HK$50 billion (US$6.4 billion) a year to high-tech and illegal bookmakers. HKJC paid eleven percent of its income to the government as betting duties, a major source of income for the government. In Lunar New Year 2001, the HKJC collected eight percent less than in 2000. *Id.*

[94] Gambling Ordinance (Ch. 148) (H.K.).

[95] *See "Moral person" Hardworking in the Background*, The Society for Truth and Light, March 31, 2002, http://www.truth-light.org.hk/article_v1/jsp/a0000278.jsp (last visited Apr. 20, 2005).

[96] *See, e.g.*, Yee Ah, *Gambler story (1) Leaving the Police* and *Gambler story (2) A father who was transfixed with gambling*, The Society for Truth and Light, Jan. 31, 2000, http://www.truth-light.org.hk/article_v1/jsp/a0000129.jsp (last visited Apr. 20, 2005).

[97] *See* Chan Yin Ping, *Horrifying Tragic Gambling Cases*, The Society for Truth and Light, July 30, 2001, http://www.truth-light.org.hk/article_v1/jsp/a0000227.jsp (last visited Apr. 20, 2005) (Hong Kong newspapers reported fourteen cases of suicides or illegal activities by desperate gamblers between March and May 2001).

[98] Leung Lan Tien Wei, *Gambling Culture Spread, Poisoning of Youth*, H.K. ECONOMIC JOURNAL (July 13, 2000). *See also* Chung Kim Wah, *Do Not Underestimate the Negative Impact of Gambling Activities on Youth*, Society of Truth and Light, Jan. 31, 2000, http://www.truthlight.org.hk/article_v1/jsp/a0000127.jsp (last visited Apr. 20, 2005).

[99] *Summary Report on Research on Views About Legalization of Gambling*, The Society for Truth and Light, Sept. 19, 2003, http://www.truth-light.org.hk/article_v1/jsp/a0000400.jsp (last visited Apr. 20, 2005).

social services groups joined hands to condemn Internet gambling as being harmful to the youth, risky to gamblers, and beneficial to offshore brokers—the same kinds of shortcomings and risks as afflict all electronic transactions.

Overnight, cyber harm experienced in the form of Internet gambling became recognizable, tangible, material, consequential, and, more importantly, dangerous. Cyber criminality was no longer perceived as a distant commercial risk to be discussed in the abstract,[100] but something that is destructive of careers and families, harmful to youth, and corrupting of the community. The next step was to validate and reinforce the public perception of cyber ills and harms. For this, the public turned to media portrayals of a moral and legal crisis in the making.

F. Public Awareness of Computer Crime and Privacy

Three high-profile cases, one in 1995 and two in 1999, sensitized the Hong Kong public to law enforcement and piracy issues in the cyber era. On March 4, 1995, the Hong Kong Police and Telecommunications Authority conducted a raid to shut down seven ISPs for crimes involving computer hacking and providing a telecommunications service without a license.[101] The raids unexpectedly cut off the Internet access of thousands.[102] They raised a number of controversial and embarrassing issues, such as what they may indicate about the future of freedom of information in Hong Kong.[103] Another issue is Hong Kong's international free-trade image. Finally, it raised the question of whether the police or Telecommunications Authority are cognizant of, sensitive to, or otherwise concerned about these issues.[104]

The raids called into question the capacity and competency of the HKG to secure the cyberspace with minimal disruption to free speech and

---

[100] According to *2000 Opinion Survey Personal Data (Privacy) Ordinance: Attitudes and Implementation—Key Findings* (2002), commissioned by Hong Kong Privacy Commissioner's Office and conducted by the Social Sciences Research Centre of the University of Hong Kong, Hong Kong people were concerned with privacy when purchasing over the Internet: 84.3% are concerned with "money loss due to interception of credit card" and 72.2% are concerned with "misuse of personal data by third parties." *See id. at* www.pco.org.hk/english/publications/files/survey_e2.doc (last visited Apr. 20, 2005).

[101] Larry Campbell, *Police Blame Internet Raids on Expansion*, SCMP, Mar. 8, 1995, at 3, *available at* LEXIS, News Library.

[102] *Id.*

[103] *Internet Raids a Danger*, SCMP, Mar. 8, 1995, at 18, *available at* LEXIS, Nexis Library, SCMP File.

[104] Statement Concerning Police Action on Internet Providers, March 4, 1995, http://courses.cs.vt.edu/~cs3604/lib/Crime/hongkong.html (last visited Apr. 20, 2005).

trade.[105] The Hong Kong people were treated to a rude awakening—their much admired and feared Hong Kong Police could not effectively fight computer crime.

The case of *HKSAR v. Tsun Shui Lun* raised the issue of computer privacy versus the public's right to know.[106] It involved Tsu Shui Lun, a technical assistant to a radiologist at Queen Mary Hospital. Tsu used his computer access at the hospital to retrieve medical records of the Secretary for Justice and shared them with his wife, friends, and two local newspapers. He was arrested and prosecuted under Section 161(1)(C) of the Crime Ordinance for theft of computer data for personal benefits. Tsun defended himself on ground that he did not release the information for "personal gain," but "because the public have the right to know" that the HKG was lying about the medical condition of the Secretary of Justice.[107] The High Court decided against Tsun, observing that he had gained access to the records of the Secretary of Justice without authority and consent and with a view to dishonest gain for himself, contrary to Section 161(1)(c) of the Crimes Ordinance. His alleged desire to expose government corruption merely related to his motive.[108] The case generated a vigorous debate over the public's right to know, a government employee's ethical duty to keep a patient's secret, and the patient's right to privacy.[109] In a still-larger context, the case raised the broader issue of computer security.

The third case, *Apple Daily Ltd. v. The Commissioner of the Independent Commission Against Corruption*,[110] raised the issue of the government's power to search and seize computer data of the press. In November 1999, a leading anti-government newspaper, *Apple Daily*, was investigated by the Independent Commission Against Corruption ("ICAC").[111] It was alleged that the paper's journalists were bribing police

---

[105] *See* Michael W. Kim, *How Counties Handle Computer Crime?* Ethics and Law on Electronic Frontier (Fall 1997), *available at* http://www-swiss.ai.mit.edu/classes/6.805/student-papers/fall97-papers/kim-crime.html (last visited Apr. 20, 2005).

[106] HKSAR v. Tsun Shui Lun - [1999] HKCFI 77; HCMA000723/1998 (Jan. 15, 1999), *available at* http://898.typepad.com/ecommerce/2003/01/hksar_v_tsun_sh.html (last visited Apr. 20, 2005).

[107] *Id.*

[108] *Id.*

[109] *See* HKSAR LEGISLATIVE COUNCIL, "A Defence of 'Public Interest': A Paper Prepared for the LegCo Panel on Administration of Justice and Legal Services," LC Paper No. CB(2)1506/98-99(06), *available at* http://www.legco.gov.hk/yr9899/english/panels/ajls/papers/p1506e6.pdf (last visited Apr. 20, 2005).

[110] Civil Appeal No. 357 of 1999 (On Appeal From HCMP No. 7315 of 1999) (2000), *available at* http://legalref.judiciary.gov.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=13016&QS=%28apple%2Bdaily%29&TP=JU (last visited Apr. 20, 2005).

[111] *Id.*

officers to supply police information.[112] Later, two police communications officers and one reporter affiliated with *Apple Daily* were sent to jail for selling and purchasing police information. ICAC seized computers and databases of *Apple Daily* and searched them for evidence.[113] The newspaper appealed to the Court of Appeals,[114] but the appeal was unsuccessful.

The three high-profile cases reported here are important milestones in Hong Kong's long march in the journey of computer crime "discovery." Viewed individually and together as a series, they demonstrate how far Hong Kong has come in recognizing computer crime and privacy issues. The fact that the cases were able to precipitate a debate over privacy of patients (*HKSAR v. Tsun Shui Lun*), authority for search and seizure (*Apple Daily*), and competence in computer crime investigation (1995 raid on ISPs), is the clearest indication that concerns over computer crime invaded the public's hearts and minds. It is too early to tell whether Hong Kong would give in to thieves of intellectual property and intruders of privacy, but the battle lines have been drawn. The cyber criminals are coming.

G. *The Arrival of Computer Crimes*

In 1995, Hong Kong law enforcement officials began one of the first cybercrime investigations, and cracked a major credit-card fraud ring in Hong Kong and Shenzhen, seizing computer equipment and data.[115] Each fraudulent credit card account sold for US $250.[116] Then, in November 1996, a disgruntled computer technician brought down Reuters' trading net in Hong Kong.[117] On November 10, 1997, dragonserve.com was hacked in Hong Kong.[118] On February 9, 1998, SunSITE was also hacked.[119]

Major computer-related crimes cases started to appear in 1999 with some degree of frequency. The "Hong Kong Blondes" was a self-organized, anti-establishment group that used its information technology prowess to

---

[112] *Id.* at Introduction.

[113] *Id.*

[114] Civil Appeal No. 357 of 1999. The Court of Appeals ruled against the newspaper, finding that while the Prevention of Bribery Ordinance (Ch. 201) (H.K.) only allows for the power to enter and search, section 10C of the Independent Commission Against Corruption Ordinance (Ch. 204) (H.K.) authorized ICAC officers to seize anything "they believe to be or to contain evidence of any of the offences referred in section 10." *Id.*

[115] M. E. Kabay, The Information Security Year in Review: 1995, *available at* http://www2.norwich.edu/mkabay/iyir/1995.pdf (last visited Apr. 20, 2005).

[116] *Id.*

[117] *Timeline History of Computer Hacking*, http://www.francesfarmersrevenge.com/stuff/misc/hack/timeline.htm (last visited Apr. 20, 2005).

[118] *Id.*

[119] *Id.*

subvert communist China's dictatorial regime and disrupt international corporations' exploitative practices.[120] Starting in 1998, Hong Kong Blondes launched a series of attacks against the People's Liberation Army's ("PLA") computer systems, including attacks that resulted in denial of service and corruption of databases.[121] As time progressed, the group began to place cyber moles with the PLA to obtain access and install codes within the PLA computer mainframes to monitor its electromagnetic signals.[122] The Hong Kong Blondes even managed to obtain access codes with the help of these cyber moles.[123]

The Ministry of Public Security acknowledged the illegal attacks and unauthorized access on its Web site, reporting 72,000 cyber-attacks between January and September 2000 alone.[124] On May 20, 1999, the HKP successfully broke up an organized hacking syndicate, arresting three hackers, a middleman and six buyers of passwords.[125] This was the first organized hacking case investigated and prosecuted in Hong Kong.[126]

The Department of Public Prosecution in Hong Kong mounted a number of successful prosecutions in Hong Kong in 2001-02.[127] The challenge is now to devise effective measures to prevent the occurrence of computer crime and mitigate its damages. To do so effectively, we need to understand more about the nature, prevalence, distribution and causation of computer crimes. Part IV deals with this subject.

IV. THE NATURE, PREVALENCE, AND DISTRIBUTION OF COMPUTER CRIME

Computer crime has become more prevalent in Hong Kong in the past ten years, and this Part traces both the history and the recent developments in cybercrime offenses and investigations. Not only has the definition of computer crime expanded, but the number of cybercrimes committed has

---

[120] Anthony C. LoBaido, *The Beijing Hack Attack: Hong Kong-based Cyber Warriors Build Anti-China Techno Army*, WORLD NET DAILY, Dec. 16, 1999, *at* http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=17295 (last visited Apr. 9, 2005).

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Hong Kong Computer Hacking Syndicate Smashed* (June 1, 1999), *available at* http://lists.virus.org/isn-9906/msg00009.html (last visited Apr. 20, 2005).

[126] *Id.*

[127] Francis Lo Hing-Cheung, *Cyber Crime: The Challenges & Way Forward*, INT'L SOC'Y REFORM CRIM. L. (presented at the 16th International Conference: Technology and its Criminal Responsibility, Security and Criminal Justice, Charleston, S.C., Dec. 6-10, 2002), *available at* http://www.isrcl.org/Papers/Lo.pdf (last visited Apr. 20, 2005).

also increased, contributing to the mounting urgency with which the HKG has responded to cyberthreats.

A. *The Emergence of Computer Criminality*

In 1996, only twenty-one cases of computer crime were reported in Hong Kong. This increased to thirty-four cases in 1998, and 317 in 1999. The jump in the reporting of official computer crime during this time did not reflect a precipitous rise in computer crime as much as it showed growing public awareness and increased government attention in pursuing computer crime and control.[128]

Table 2: HKSAR Legislative Council: Reported Computer-Related Crimes: 1996-1999[129]

CRIME	1996	1997	1998	1999
Hacking	4	7	13	238
Publication of obscene articles	6	6	13	32
Criminal damage of data	4	3	3	4
Internet shopping fraud	0	2	1	18
Others	7	2	4	25
TOTAL	**21**	**20**	**34**	**317**

Table 2 lists computer-related crimes by type of crime as reported by the LegCo Panel on Security from 1996 to 1999. Table 3, infra, reports incidence of computer-related crime as reported by the Department of Justice from 1993 to 2000. There are two noticeable differences between these two sets of data. First, the LegCo data does not include fraud related to the private automatic branch exchange ("PABX") telephone system as a computer crime.[130] This could not have been an oversight, because later LegCo reports use the same tabulation as the Department of Justice reports. The more reasonable explanation is that the two institutions define computer-related crime differently. Second, the Department of Justice data reaches back to 1993 and the LegCo data starts with 1995. This disparity

[128] LEG. COUNCIL PANEL ON SEC., COMPUTER-RELATED CRIMES (March 2, 2000), at paras. 2 and 7-8, *available at* http://www.legco.gov.hk/yr99-00/english/panels/se/papers/b1187e04.pdf (last visited Apr. 20, 2005).

[129] *Id.* at 1-2.

[130] For a definition of PABX fraud, *see* The Information Security Glossary, *available at* http://www.yourwindow.to/information-security/gl_pabxpbx.htm (last visited Apr. 20, 2005). A PABX is a computerized system that manages an internal telephone extensions network. By manipulating the PABX system electronically, one can get calls billed to owner of the PABX. *Id.*

reveals that that there was a different understanding within the HKG as to when computer crime became a problem in Hong Kong. The Department of Justice began tracking computer crime two years earlier than did LegCo.

Both of these observations point to a larger truth: there was a lack of coordinated approach to and common perspective on the control of computer crime and regulation of cyberspace during this time. This is evidenced by the lack of inter-departmental exchange and the leadership void in this area. The Hong Kong LegCo, the Law Reform Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Exchange, the Hong Kong Security Bureau, the Hong Kong Police, and Hong Kong Customs and Excise all look at cyber risks and computer crime through their own prism—legal jurisdiction and organizational priority—and approach them in their own ways.[131]

Table 3: Department of Justice: Reported Computer Related Crimes: 1993-2000[132]

CRIME	1993	1994	1995	1996	1997	1998	1999	2000
Hacking	1	5	4	4	7	13	238	38
PABX Fraud	0	3	4	5	5	4	0	0
Publication Obscene Articles	0	0	1	6	6	13	32	0
Criminal Damage	0	1	2	4	3	3	4	1
Internet Shopping Fraud	0	0	0	0	2	1	18	4
Others	3	3	7	7	2	4	25	6
Total	**4**	**12**	**18**	**26**	**25**	**38**	**317**	**49**

1999 saw the highest incidence in reported computer-related crime in Hong Kong's history since the beginning of record-keeping in 1993.[133] Computer crime increased from four instances in 1993 to 317 in 1999,

[131] The case in point was the fumbled raid conducted by the HKP and OFTA on March 4, 1995, discussed in Statement Concerning Police Action on Internet Providers, *supra* note 104.

[132] Press Release, HKSAR, Speech by Director of Public Prosecutions (May 26, 2000), *available at* http://www.info.gov.hk/gia/general/200005/26/0526197.htm (last visited Apr. 20, 2005).

[133] *See* Table 3, *supra*.

representing a jump of 7825 percent.[134] Between 1998 and 1999, there was an increase of 734 percent.[135]

Senior Superintendent Raymond Lau Chi-keung of the HKP Commercial Crime Bureau observed that the computer crime rates increased as a result of the large increase in computer ownership and use.[136] Superintendent Raymond Lau also observed an increase in the sophistication and complexity of the computer crime cases.[137] Many crimes were committed by children under pressure to impress their peers.[138]

In 2001, there was a slight decrease of computer crime cases to 235.[139] The HKP attributed the decrease to public awareness and self-help, and successful law enforcement efforts of the HKP; the drop may also have been due to the bursting of the dot-com bubble and the slowdown of the information technology industry during the period.[140]

In 2002, the HKP recorded a total of 272 computer crime cases, an increase of thirty-seven cases.[141] In addition, the Newspapers Registration Section received a total of 3768 public complaints about pornographic materials on the Internet between July 2001 and December 2002.[142]

Further analysis of the computer crime statistics reveals that more than seventy-five percent of the reported crimes in 1999 and 2000 were computer hacking crimes.[143] The rest were pornography crimes (down from thirty-eight percent in 1998).[144] In recent years, the number of hacking cases dropped, while electronic banking thefts and electronic fraud increased. In 2001, sixty-five cases of electronic fraud, including use of a stolen identity to obtain goods or services via the Internet, were recorded.[145] There were also eight electronic banking thefts in 2001, and this has increased to 103 cases of e-fraud in 2003.[146] The LegCo was very much

---

[134] *Id.*

[135] *Id.*

[136] *See Offbeat Online: CCB Hindering IT Crime*, *available at* http://www.info.gov.hk/police/offbeat/695/014_e.htm (last visited Apr. 20, 2005).

[137] *Id.*

[138] *Cyber Crime Mushrooms in Hong Kong*, ASIA TIMES, Jan. 24, 2001, *available at* http://www.atimes.com/china/CA24Ad03.html (last visited Apr. 20, 2005).

[139] *See* Table 4, *infra*.

[140] Bruce Einhorn, *The Brutal Morning After for Asian Dot-Coms*, BUSINESS WEEK.COM (Apr. 24, 2000), http://yahoo.businessweek.com/bwdaily/dnflash/apr2000/nf00424d.htm (last visited Apr. 20, 2005).

[141] *See* Table 4, *infra*.

[142] *See* Public Complaints on Pornographic Materials received by Newspapers Registration Section Against Internet Jul 2001-Dec 2002, *available at* http://www.infosec.gov.hk/engtext/general/crc/statistics_6.htm (last visited Apr. 20, 2005).

[143] *See* Table 3, *supra*.

[144] *Id.*

[145] *See* Table 4, *infra*.

[146] *Id.*

concerned with the adverse impact of e-fraud on Hong Kong e-banking, e-commerce, and tourism industries.[147] In 2004, yet another kind of e-banking fraud afflicted Hong Kong: cybercriminals sent spam e-mails luring victims to access fraudulent websites and disclose sensitive information leading to the illegal transfer of money or disclosure of other assets.[148]

B. *The Patterns and Trends of Computer Crime*

Table 4 below summarizes the computer crime cases between 1996 and 2003 according to the types of offenses currently categorized by HKP. Computer crime in 2003 climbed to 588 cases, doubling that of 2002's 272 cases, and twenty-one times more than those reported in 1996.[149] In 1993, a majority of those computer crime cases (60.5%) involved illegal access to a computer with criminal or dishonest intent.[150] If all crimes of unauthorized access to computers were added together, the percentage would go up to 68.5%.[151] This is an increase of 158%, from 138 cases in 2002 to 356 cases in 2003.[152]

The second most prevalent computer crime appears to be "obtaining property and service by deception" via the Internet.[153] In 2003, there were 103 reported incidents of this crime, constituting 17.5% of all reported computer crime cases.[154] It is interesting to note that obtaining property by fraud has shown a steady growth pattern, from two cases in 1997 and 10% of all cases during that year, to twenty-nine cases and 7.9% of all cases in 2002, to eighty-six cases and 14.6% of all the cases in 2003; on the other hand, obtaining services by fraud has dropped, from thirty-three cases in 2002, and 7.12% of all reported computer crime cases, to seventeen cases in 2003, and 3% of all the cases.[155]

The third largest crime in 2003 was publication of obscene materials on the Internet.[156] At fifty-eight cases, this represented 9.9% of reported

---

[147] Press Release, HKSAR, LegCo to Debate Combating Crimes Relating to Automatic Teller Machine Cards and Credit Cards (Mar. 22, 2004), *available at* http://www.info.gov.hk/gia/general/200403/22/0322167.htm (last visited Apr. 20, 2005).

[148] Press Release, HKSAR, Deputy Government CIO Speaks on Information Security (July 7, 2004), *available at* http://www.info.gov.hk/gia/general/200407/07/0707174.htm (last visited Apr. 20, 2005).

[149] *See* Table 4, *infra*.

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *Id.*

crimes.[157] Thus, the three kinds of computer crime most prevalent in 2003 were unauthorized access, computer fraud, and publication of obscene material.[158]

Table 4: Computer Crime Cases in Hong Kong by Various Offenses (1996-2003)[159]

TITLE OF OFFENSE[160]	1996	1997	1998	1999	2000	2001	2002	2003
Annual total	21	20	34	318	368	235	272	588
Unauthorized access to a computer by telecommunication	4	7	13	238	53	33	26	47
Access to a computer with criminal or dishonest intent					222	81	138	356
Criminal damage (computer-related)	4	3	3	4	15	27	16	16
Obtaining property by fraud (online shopping)	0	2	1	18	29	32	45	86
Obtaining services by fraud (computer-related)	7	2	4	26	49	33	19	17
Theft (related to e-banking)						16	6	8
Other misc. theft (computer-related)							15	
Other						13	7	58
Publication of obscene articles	6	6	13	32				

While the crimes of unauthorized access and publication of obscene materials are self-explanatory, obtaining property and services by fraud is worthy of further explanation through an example. In December 2003, Hong Kong Monetary Authority issued an alert on fraudulent bank websites.[161] Since that time, numerous overseas fraudulent bank websites

[157] *Id.*

[158] *Id.*

[159] For figures between 2000 and 2003, see H.K. POLICE, INFORMATION SECURITY & PREVENTION OF COMPUTER RELATED CRIME: STATISTICS, *at* http://www.infosec.gov.hk/engtext/general/crc/statistics_4.htm (last visited Apr. 20, 2005). For figures between 1996 and 1999, see HKSAR Computer Crime Report, *supra* note 11, at para. 1.2.

[160] The column "Title of offense" matches the descriptions provided by HKP in 2002 for all rows except the last row.

[161] *See* Press Release, HKMA, Suspicious Fraudulent Website: www.dbshk.net (Dec. 24, 2003), *available at* http://www.info.gov.hk/hkma/eng/press/index.htm (last visited Apr. 20, 2005).

have been uncovered.[162] Victims included prominent and fake financial institutions in Hong Kong, Canada, and the United States, such as East Asia Credit,[163] Pacific Asian Bank,[164] and Paramount Bank.[165]

C. *Computer Crime and Corporations*

In 2003, Computer Emergency Response Team Coordination Centre, Technology Crime Division of Commercial Crime Bureau of Hong Kong Police Force, and Information Technology Services Department of Hong Kong Special Administrative Region conducted a survey of Hong Kong registered companies to ascertain their experience with computer crime.[166] The survey investigated Hong Kong companies' experience with computer attacks, information security awareness, computer security technologies and strategies employed, and expenditures on information security.[167] The survey showed that more than half of the respondents (56.2%) operated servers and/or websites, of which 23.3% experienced computer attacks in 2003.[168] Unauthorized computer attacks impact smaller companies more than big ones; attacks on small companies resulted in a higher percentage of PCs being affected.[169] The decline in 2003-2004 of computer-related financial loss was likely due to an increase in the rate of reporting by the victims.[170]

---

[162] *See* Press Release, HKMA, Suspicious Fraudulent Website: www.swisscreditbank.com (Dec. 31, 2003), *available at* http://ww.info.gov.hk/hkma/eng/press/2003/20031231e6.htm (last visited Feb.15, 2005); Press Release, HKMA, Fraudulent Website: www.barclays-eu.org (Jan. 5, 2005), *available at* http://www.info.gov.hk/hkma/eng/press/2005/20050105e3.htm (last visited Apr. 20, 2005).

[163] *See* Press Release, HKMA, Suspicious Fraudulent Website: "East Asia Credit" (Sept. 24, 2003), *available at* http://www.info.gov.hk/hkma/eng/press/index.htm (last visited Apr. 20, 2005).

[164] *See* Press Release, HKMA, Suspicious Fraudulent Website: www.pabbank.com (Oct. 31, 2003), *available at* http://www.info.gov.hk/hkma/eng/press/index.htm (last visited Apr. 20, 2005).

[165] *See* Press Release, HKMA, Suspicious Fraudulent Website: www.paramountbank (Oct. 31, 2003), *available at* http://www.info.gov.hk/hkma/eng/press/index.htm (last visited Apr. 20, 2005).

[166] The survey, completed between November and December 2003, is the fourth one conducted since 2000. For survey methodology and detailed findings, see H.K. COMPUTER EMERGENCY RESPONSE TEAM ET AL., INFORMATION SECURITY SURVEY 2003, *at* http://www.hkcert.org/articles/artindex.html?art0011.html (last visited Apr. 20, 2005).

[167] *Id.*

[168] *Id.* at 25.

[169] *Id.* at 13.

[170] *Id.* at 17.

Table 5: Information Security in the Business Sector (2000-2004)[171]

DESCRIPTIONS	2000	2001	2002	2003	2004
Total no. of computer crime incidents	1,510	1,387	1,095	943	865
Change in percentage as compared to previous year (+/-)	n/a	-8.1%	-21.1%	-13.9%	-8.3%
Average no. of attacks per victimized company	2.6	3.5	3.4	2.4	2.7
Change in percentage as compared to previous year (+/-)	n/a	+34.6%	-4%	-29.4%	+12.5%
Total no. of PCs affected	4,733	5,366	5,460	4,098	3,464
Change in percentage as compared to previous year (+/-)	n/a	+13.4%	+1.8%	-24.9%	-15.5%
Average no. of PCs affected per incident	3.1	3.9	5	4.3	3.9
Change in percentage as compared to previous year (+/-)	n/a	+25.8%	+28.2%	-14%	-9.3%
Total financial loss estimated (HK$)	$1.38M	$1.52M	$1.84M	$1.22M	$0.85M
Change in percentage as compared to previous year (+/-)	n/a	+10.8%	+20.5%	-33.5%	-30.1%
Average financial loss per victimized company (HK$)	$2,461	$3,888	$5,632	$3,116	$2,617
Change in percentage as compared to previous year (+/-)	n/a	+58%	+44.9%	-44.7%	-16%

The above statistical survey data makes possible comprehensive analysis of the current status of computer crime in Hong Kong. Between 2000 and 2002, four major concerns prompted the HKG to take aggressive actions to regulate cyberspace: an increase in computer-related deviance, increased number of breaches of computer ethics, violations of information privacy, and threats to electronic commerce.[172] Based on government statistics, there was also a phenomenal growth in computer crime since the late-20th century.[173] The following parts of this Article will inquire into various aspects of computer crime control and cyberspace governance policy and practice in Hong Kong.

[171] *Id.* at 28.
[172] *See* Table 4 and 5, *supra*, and related discussion in text.
[173] *Id.*

V. COMPUTER CRIME CONTROL AND CYBERSPACE GOVERNANCE IN HONG KONG

Because cybercrime has become an increasingly dangerous problem in Hong Kong, the Hong Kong government has implemented many policies—ranging from legislation to law enforcement—to combat the growing threat.

A. Views on Computer Crime Legislation

In providing for law and order in cyberspace, the HKG has pursued strategies that are broadly consistent with traditional Chinese values and its established governing philosophy. This means small government, positive non-interventionism, individual communitarianism and voluntarism, community empowerment and activism, and utilitarianism and pragmatism.[174] In 2000, Legislative Councilor Sin Chung Kai of Information Technology articulated four basic principles of cyberspace legislation in Hong Kong: First, apply current law to cyberspace.[175] Second, avoid undue legislation.[176] Third, support and promote a predictable, consistent and minimalist legislative regime.[177] Fourth, introduce laws only when necessary.[178]

Consistent with the above governing philosophy and legislative principles, the HKG recognizes a long-term need to reduce the "artificial" barrier between computer crime and street crime legislation. The thinking within the HKG, reflecting the community's point of view, is that a crime is a crime, no matter how it is perpetrated and where it occurred:

> 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

---

[174] *See generally* LAU SIU KAI, SOCIETY AND POLITICS IN HONG KONG (Chinese Univ. Press ed., 1982).

[175] *See* SIN CHUNG KAI, INFO. SYS. AUDIT & CONTROL ASS'N, LEGAL AND LEGISLATING ISSUE OF E-COMMERCE AND THEIR IMPACT ON INFORMATION SYSTEM AUDITORS 12 (2000), *at* http://www.isaca.org.hk/document/cisa_slide/ETO%20-%20Legal%20and%20Legistative/sld012.htm (last visited Apr. 20, 2005).

[176] *Id.*

[177] *Id.*

[178] *Id.*

> the constantly evolving nature of the cyber world, we cannot afford to stand still in our effort to curb computer crime.[179]

This view about the inseparability between street and virtual crime is based on the venerable Chinese understanding that crime is a challenge to heavenly order (*tianming*).[180] Specifically, crimes are disturbances (*luan*) of the heavenly order—embodied and personified in the Emperor's rule—to be suppressed at all costs.[181] Local officials who failed to maintain order within their jurisdiction are disciplined.[182] Emperors who experienced civil disorder are deemed to be unfit to rule and deprived of their legitimacy from heaven.[183]

B. Cyberspace Policy Affects the Public as Well as the Private Sector

Hong Kong is considered to have one of the most dynamic economies in the world. The Digital 21 Strategy entitled "Hong Kong: Connecting the World," promulgated in May 2001, has articulated five key objectives for improving Hong Kong's competitive advantages, including enhancing Hong Kong's world-class e-business environment.[184]

The HKG, realizing the importance and vulnerability of the information super-highway for global trade, has taken an active role in keeping it free and safe.[185] In the words of Peter Lovelock:

> Hence our position . . . : e-commerce in Hong Kong will continue to lag until the government becomes more involved in providing the necessary "soft" infrastructural development for commerce by cyberspace. By this we mean the legal framework for e-commerce, the regulatory framework for

---

[179] HKSAR Computer Crime Report, *supra* note 11, paras. 14.3-14.5.

[180] *See* Shih Ching, BOOK OF ODES, *available at* http://web.cn.edu/kwheeler/chinese_poetry_highheaven.html (last visited Apr. 11, 2005).

[181] KANG SHUHUA, CRIMINOLOGY 37 (1998). Crime and disorder as challenge to the Emperor's power is not unique to China. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISHMENT: THE BIRTH OF THE PRISON (Vintage Books ed., 1977) (reporting that in seventeenth-century France, punishment must not only had to be done but had to be seen to be done. It had to be inflicted upon the condemned and damned, in a slow, methodical, painful, and above all, spectacular way, to demonstrate the absolute power of the sovereign to inflict pain).

[182] *See generally* Shuhua, *supra* note 181.

[183] *See generally id.*

[184] GOV'T OF THE H.K. SPECIAL ADMINISTRATIVE REGION, 2001 DIGITAL 21 STRATEGY: CONNECTING THE WORLD (Price Waterhouse Coopers ed., 2001), *available at* http://www.info.gov.hk/digital21/eng/strategy2001/strategy_part04.html (last visited Apr. 20, 2005).

[185] *See* Lovelock, *supra* note 2.

> banking and securities trading, the security framework for merchants, consumers, and for copyright and data protection, and a new, more appropriate, emphasis upon education, training, research and development.[186]

Accordingly, the Hong Kong Security Bureau has established a strategy to enhance HKG's capacity to deal with emerging computer crimes, pledging "to strengthen present monitoring of and response to computer crime trends and developments."[187] The HKP was charged with the implementation of this strategy to make Hong Kong one of the safest and most stable, business-friendly societies in the world.[188]

The private sector and various business associations, not satisfied with the HKG's approach, have called for a more aggressive and assertive presence by the HKG.[189] For example, Hong Kong Coalition of Service Industries and Hong Kong General Chamber of Commerce have called for a more robust and focused information technology development plan, including: increasing information technology education and training, strengthening the protection of intellectual property rights, upgrading communications infrastructure in the Pearl River Delta region, conducting structural review of the regulatory framework for broadcasting and telecommunications, appointing an advocate to coordinate regulatory policies, and ensuring effective involvement across the information industries.[190]

C. *Cyberspace Policy in Action Has Made Some Gains, But Challenges Still Exist*

Unlike mainland China,[191] the HKG does not monitor and regulate the flow of information on the Internet. The right of free speech is firmly

---

[186] *Id.* at 6.

[187] HKSAR SECURITY BUREAU, THE 2001 POLICY ADDRESS: POLICY OBJECTIVES – SECURITY BUREAU: A SECURE AND SAFE CITY 15, *available at* http://www.policyaddress.gov.hk/pa01/pdf/safee.pdf (last visited Apr. 20, 2005).

[188] *Id.* at 15-17.

[189] *See* HONG KONG COALITION OF SERVICE INDUSTRIES AND HONG KONG GENERAL CHAMBER OF COMMERCE, RESPONSE TO THE DIGITAL 21 CONSULTATION DOCUMENT, Dec. 2003, http://www.chamber.org.hk/memberarea/chamber_view/policy_statement_template.asp?id=1174 (last visited Apr. 20, 2005).

[190] *Id.*

[191] Kam C. Wong & Georgiana Wong, *Law and Order in Cyberspace: A Case Study of Cyberspace Governance and Internet Regulations in China*, ASIAN POLICING IN THE 21ST CENTURY (PROCEEDINGS) (Hong Kong: AAPS, 2002).

secured by Article 27 of the Basic Law,[192] stating: "Hong Kong residents shall have freedom of speech, of the press and of publication . . . ."[193]

Hong Kong citizens have enjoyed unimpeded free expression and privacy rights on the Internet. Their yearning for freedom clashes with an emergent concern for the protection of intellectual property rights, computer security, and fair competition in cyberspace. It also challenges entrenched traditional Chinese values of proper moral education for the younger generation in the cyberspace age.

Just as in mainland China, the HKG has placed much effort in promoting the healthy, ethical, and moral use of the Internet.[194] The approach in Hong Kong, however, is more de-centralized and communalized. Education efforts have not been centrally coordinated and much depends on community voluntarism and individual self-help, such as having computer associations lead security awareness and information ethics efforts.[195]

The HKG has taken an aggressive leadership role in spearheading the teaching of computer ethics.[196] The Inter-departmental Working Group has recommended joint efforts of the public and private sectors in promoting public education in computer security awareness and information ethics.[197] Such a call to arms has resulted in many joint ventures. For example, in 2003 the HKP, the Education and Manpower Bureau, and the Television and Entertainment Licensing Authority, with the active participation of

---

[192] Basic Law, *supra* note 58.

[193] *Id.* art. 27.

[194] Wong & Wong, *supra* note 191.

[195] *See* COMMENTS ON "INTER-DEPARTMENTAL WORKING GROUP ON COMPUTER RELATED CRIME REPORT," HONG KONG COMPUTER SOCIETY (Feb. 10, 2001), http://www.hkcs.org.hk/legco_100201.doc (last visited Apr. 20, 2005).

[196] For HKG and related departments' efforts to educate the public on computer security and ethics, see *Publicity and Education Efforts*, HKSAR Computer Crime Report, *supra* note 11, at 106-16. Various departments involved with publicity and education efforts include the Hong Kong Police Force's Crime Prevention Bureau (Computer Crime Section), Information Technology and Broadcasting Bureau and Information Technology Services Department, Office of the Telecommunication Authority, Office of Privacy Commission for Personal Data, Commerce and Industrial Bureau/Intellectual Property Department, Hong Kong Productivity Council, Consumer Council, and the Fight Crime Committee. Conspicuously missing are the Hong Kong Monetary Authority and the Hong Kong Securities and Futures Commission. Both, while being quasi-public institutions, are sufficiently involved with implementation of public policy that their efforts in IT security education and training must be coordinated and integrated. For discussion of the HKMA role in information security, *see* Press Release, HKMA, Fraudulent Website (Nov. 30, 2004), *available at* http://www.info.gov.hk/gia/general/200411/30/1130236.htm (last visited Apr. 20, 2005). For discussion of the HKSFC role in information security, *see* Gu Xiaorong, *A Comparative Study of Security Systems of Shanghai, Shenzhen and Hong Kong*, *available at* http://www.rjmacau.com/english/rjm1996n3/security/ (last visited Apr. 20, 2005).

[197] HONG KONG ETHICS DEVELOPMENT CENTRE, LEVERAGING INFORMATION TECHNOLOGY—ETHICS PERSPECTIVES FOR MANAGERS FORUM 2001 (Mar. 5, 2002), http://www.icac.org.hk/hkedc/itconf/content/icaethic_williamgee.htm (last visited Apr. 20, 2005).

Information Systems Audit and Control Association, jointly organized a computer ethics promotion program for youth.[198]

The HKG also has taken a proactive approach to fighting computer crime. In this regard, ICAC has taken the lead by collaborating with thirteen local business associates to develop ethical guidelines for prevention of computer crime.[199] The guidelines include case illustrations extracted from the ICAC's investigation files, illustrating common patterns of computer crime in business organizations, and provide an ethical management model with practical tips of how to prevent workplace computer crime.[200] Likewise, the HKMA routinely sent security circulars and guidelines to alert bank management and operatives to structural security problems[201] or emerging security risks.[202]

D. Computer Crime Legislation Has Been Enacted

The Computer Crimes Ordinance in Hong Kong was enacted in 1993 through amending the Telecommunications Ordinance (Ch. 106),[203] Crimes Ordinance (Ch. 200),[204] and Theft Ordinance (Ch. 210),[205] creating new offenses and extending the coverage of existing offenses.

The pertinent Hong Kong laws governing computer-related crimes are summarized below in Table 6.[206] 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 Legislative Council.[207]

---

[198] *See* CYBER ETHICS FOR STUDENTS AND YOUTH, http://cesy.qed.hkedcity.net/ (last visited Apr. 20, 2005).

[199] *See* ETHICS@WORK—A GUIDE FOR BUSINESS MANAGERS IN THE USE OF IT, *available at* http://www.icac.org.hk/eng/0/1/10/17/12040/13856.html (last visited Apr. 20, 2005).

[200] *Id.*

[201] *See* HKMA, STRENGTHENING SECURITY CONTROLS FOR INTERNET BANKING SERVICES (June 23, 2004), *available at* http://www.info.gov.hk/hkma/eng/guide/index.htm (last visited Apr. 20, 2005).

[202] *See* HKMA, PRECAUTIONARY MEASURES AGAINST FAKE E-MAILS OR WEBSITES (Sept. 30, 2004), *available at* http://www.info.gov.hk/hkma/eng/guide/index.htm (last visited Apr. 20, 2005).

[203] Telecommunications Ordinance, Chapter 106, Laws of Hong Kong, Gazette Number: 36 of 2000.

[204] Crimes Ordinance, Chapter 200, Laws of Hong Kong.

[205] Theft Ordinance, Chapter 210, Laws of Hong Kong (June 30, 1997).

[206] For a detailed listing of the existing legislation, HKSAR Computer Crime Report, *supra* note 11, at 5-9.

[207] See *id.* at 88-92.

Table 6: Provisions of Hong Kong's Computer Crime Laws[208]

LAW	PROVISIONS	MAXIMUM PENALTY
Ch. 106, S.27A	Prohibiting unauthorized access to computer by telecommunication	Fine of HK $20,000
Ch. 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
Ch. 200, S.59 & 60	Extending the meaning of criminal damage to property to misuse of a computer program or data	Ten-year imprisonment
Ch. 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
Ch. 200, S.161	Prohibiting access to computer with criminal or dishonest intent	Five-year imprisonment
Ch. 210, S.11	Extending the meaning of burglary to include unlawfully causing a computer to function in a way other than for which it had been designed and altering, erasing or adding computer program data	Fourteen-year imprisonment
Ch. 210, S.19	Extending the meaning of false accounting to include destroying, defacing, concealing or falsifying records kept by computer	Ten-year imprisonment

Given the transborder nature of computer crime, the Working Group completed a comparison study of existing legislation with reference to the Draft Convention on Cyber-Crime of the Council of Europe ("COE").[209] The COE Draft Convention has identified four major categories of offenses and recommended they be incorporated into the substantive criminal law of participating countries. These categories included: offenses against the confidentiality, integrity and availability of computer data and systems; computer-related offenses; content-related offenses; and ancillary liability and sanctions.[210]

Table 7 presents an analysis of computer-related offense provisions, based on the COE classification of offenses as defined in the Draft

[208] *Id.*

[209] *See* COUNCIL OF EUROPE WEB SITE, http://www.coe.int/T/e/Com/about_coe/ (last visited Apr. 20, 2005). The Council of Europe is an international organization with forty-one member states. It seeks to, *inter alia*, strengthen the rule of law by encouraging the adoption of common practices and standards within its member states. *Id.*

[210] *See* EUROPEAN COMMITTEE ON CRIME PROBLEMS, DRAFT CONVENTION ON CYBER-CRIME AND EXPLANATORY MEMORANDUM RELATED THERETO (June 2001), *available at* http:// www.privacy international.org/issues/cybercrime/coe/cybercrime-final.html (last visited Apr. 20, 2005).

Convention.[211] 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.[212]

Table 7: Analysis of Computer-Related Offense Provisions in Hong Kong Based on the Council of Europe Classification of Offenses[213]

COE CLASSIFICATION OF OFFENSES	HONG KONG ORDINANCE	
	Name	Citation to Hong Kong law, max. sentence
Illegal access Illegal interception	Crimes Ordinance; Telecommunication Ordinance	Ch.200, Sec. 161 (5 yr. max.); Ch.106, Sec. 27A (fine of HK$20,000)
Data interference System interference Misuse of devices	Crimes Ordinance (extending "criminal damage to property" to include "misuse of a computer") Theft Ordinance (extending definition of "burglary")	Ch.200, Sec. 59, 60, 63 (10 yr. max. or life imprisonment if property intentionally destroyed so as to endanger life) Ch.210, Sec. 11 (14-year max. for burglary, including unlawful interference with computer)
Computer-related forgery	Crimes Ordinance	Ch. 200, Sec. 85 (life imprisonment for falsification of bank computer records)
Computer-related fraud	Theft Ordinance	Ch.210, Sec. 19 (10-year max. for false accounting by falsifying computer records)
Computer child pornography	Control of Obscene and Indecent Articles Ordinance	Ch.390, Sec. 21 (3-year max. and fine of HK$1 million)
Copyright and related rights	See Copyright Ordinance (Ch.39) Prevention of Copyright Piracy Ordinance (Ch.544)	
Separate attempt, aiding, etc. offenses	Theft Ordinance	Ch.210, Sec. 56 (accessories), Sec. 159A (conspiracy), Sec. 159G (attempts)

The HKSAR Computer Crime Report, while far from being perfect, is more than adequate to identify the challenges and issues of an emerging cybercrime problem in Hong Kong. For example, the report painstakingly

[211] *See* HKSAR Computer Crime Report, *supra* note 11, at Annex 12.
[212] *Id.* at i-viii.
[213] *Id.* at 6-8.

reviews existing legislation and probes relevant administrative measures, as it draws upon international experiences to find solutions to computer crime problems and issues.[214]

The HKSAR Computer Crime Report's legislative proposals were well-received,[215] but not without serious debate by the legal community,[216] business associations,[217] computer professionals,[218] and cyberspace academics.[219] The Criminal Law and Procedure Committee of the Hong Kong Law Society has raised a number of concerns.[220] For example, the Working Group has called for legislation to enhance the investigative power of law enforcement agencies, particularly recommending that officials should be "provided with the decryption tool or the decrypted text (including all the images and sounds) when necessary and justified."[221] In their submission the Hong Kong Law Society criticized this recommendation on privacy and other grounds. Specifically, it raised the following concerns:

1. Implications of the proposed legislation on the development of e-commerce;
2. Potential infringements of privacy;
3. Implications for the disclosure of encrypted information, which may include legally privileged information;
4. The right of individuals against self-incrimination;
5. The need for disclosure of keys when access to plain text would be sufficient; and

---

[214] *See* HKSAR Computer Crime Report, *supra* note 11, Annex 1, at 88.

[215] *See* Press Release, HKSAR, Government Initiatives to Combat Computer Crime (July 16, 2001), *available at* http://www.info.gov.hk/gia/general/200107/16/0716105.htm (last visited Apr. 20, 2005). *See also* LEGCO SECURITY PANEL, PAPERS ON COMPUTER RELATED CRIME, *at* http://www.legco.gov.hk/yr02-03/english/panels/se/papers/se_c.htm (last visited Apr. 20, 2005).

[216] SUBMISSIONS ON THE REPORT OF THE INTER-DEPARTMENTAL WORKING GROUP ON COMPUTER RELATED CRIME BY THE CRIMINAL LAW & PROCEDURE COMMITTEE OF THE LAW SOCIETY (Feb. 9, 2001), *at* http://www.hklawsoc.org.hk/pub/news/submissions/20010314b.doc (last visited Apr. 20, 2005) [hereinafter The Law Society].

[217] *See, e.g., Report on Inter-Departmental Working Group on Computer Related Crime Response by the Hong Kong General Chamber of Commerce* (Feb. 2001), *available at* http://www.chamber.org.hk/memberarea/chamber_view/policy_statement_template.asp?id=418 (last visited Apr. 20, 2005).

[218] Samuel Chanson, *Comments on Government's Report on Computer Related Crime*, *available at* http://isfs.org.hk/past_act/010217/sin.crime.pdf (last visited Apr. 20, 2005).

[219] Kam C. Wong, *Reflecting on Computer Crime in Hong Kong: A Critical Review of the Working Group on Computer-Related Crime Report of 2000*, *available at* http://www.asc41.com/www/2001/absgl019.htm (last visited Apr. 20, 2005).

[220] The Law Society, *supra* note 216.

[221] HKSAR Computer Crime Report (2000), *supra* note 11, at para. 5.14 (emphasis in original).

6. The need for the empowered agencies to be fully accountable to democratic institutions and subject to public scrutiny.[222]

Professor Samuel Chanson of the Department of Computer Science at Hong Kong University of Science and Technology found the HKSAR Computer Report to be "a step in the right direction."[223] However, he believed the report needed to balance the conflicting considerations of investigation, privacy, and costs to providers and the public.[224] Professor Chanson cautioned against placing too much emphasis on legal issues, such as the definition of computer crime, enforcement problems and investigative powers. According to him, it was just as important, if not more important, to put effort into prevention of computer crime.[225]

Finally, Information Security and Forensics Society made the following recommendations for improving the HKSAR Computer Report:

1. On Privacy: In order to develop Internet to its fullest potential, privacy is a major concern, especially while the data is in transit or on storage. Thus data flow should be protected by Personal Data Ordinance. Any future computer law should only be adopted after in-depth study of its impact on privacy.[226]
2. On fighting computer crime: The government should work with the IT community to fight computer crime, e.g., engaging the IT community in defining, identifying, preventing, detecting and investigating computer crime.[227] This includes seeking assistance and cooperation from ISPs and web hosting companies in investigating computer crimes, e.g., helping to preserve forensic evidence, maintaining security adopting standards and procedure to prevent computer crime.[228]
3. On setting best industrial standards: Police, academics and IT professionals should collaborate to create best industrial

[222] The Law Society, *supra* note 216, at 1.
[223] Chanson, *supra* note 218, at 4.
[224] *Id.* at 5.
[225] *Id.* at 7.
[226] *Id.* at 8.
[227] *Id.* at 10.
[228] *Id.* at 9.

standards on issues affecting computer security that will be admissible in court.[229]

4. On computer crime prevention: The government should promote computer security awareness to the public and small and medium-sized enterprises.[230]
5. On computer security experts: There is a gross shortage of computer security and forensic experts. The HKG should work with the university to develop computer security, investigation and forensic courses.[231]

The Hong Kong Internet Service Providers Association ("HKISPA") was very much encouraged by the HKG's attention to computer crime.[232] Overall, HKISPA supported the HKG's effort to improve cyberspace governance and considered many of its recommendations to be valuable. HKISPA, however, was opposed to some of the HKSAR Computer Report's recommendations. HKISPA considered disclosure of encryption code or text to be inherently dangerous and preferred stringent judicial oversight.[233] HKISPA suggested punishing unauthorized access to computer or data only when intent can be positively demonstrated.[234] HKISPA recommended new legislation against harmful acts of "intentional scanning and sending false data to a system."[235] Finally, HKISPA recommended that requests for ISPs' assistance should be reasonable and not cost prohibitive.[236]

E. Law Enforcement Has Made Great Strides in Confronting Computer Crime

The Hong Kong Police have taken active steps to deal with computer-related crimes, since as early as 1993, when legislation was first amended to address computer crime problems.[237] Three characteristics defined the nature of computer crime during this time. First, computer crimes were

---

[229] *Id.* at 10.

[230] *Id.*

[231] *Id.* at 11.

[232] *See* HONG KONG INTERNET SERVICE PROVIDERS ASSOCIATION, *Comment and Recommendation to the Inter-Departmental Working Group on Computer Related Crime Report* (Feb. 10, 2001), *available at* http://www.legco.gov.hk/yr00-01/english/panels/se/papers/b811e01.pdf (last visited Apr. 20, 2005).

[233] *See id.*

[234] *Id.*

[235] *Id.*

[236] *Id.*

[237] Victor Yik-kee Lo, *Tracing and Tracking Suspects Across Computer Networks* (2000), *available at* http://www.4law.co.il/365.pdf (last visited Apr. 20, 2005).

local crimes.[238] The criminal act, victim, and offender remained under HKP jurisdiction.[239] Second, computer crimes were conventional crimes (like fraud and theft) conducted with computers.[240] Third, computers were used an as instrumentality of a crime, e.g., storage of betting and payout information.[241] The computer was not an essential element of the crime itself, as is the case with spamming or hacking.

The HKP was ill-prepared to confront computer crimes in the early 1990s. Chief Superintendent Victor Lo, who was in charge of the Commercial Crime Bureau's computer crime division, reported many difficulties in investigating multi-jurisdictional computer crime, from tracing digital evidence to tracking cyber criminals, to concerns over the privacy rights of Internet users.[242]

Altogether, the criminal investigation structure, process, culture, staffing, training, experience, and expertise of the HKP were not suited for the effective investigation of computer crime during the early 1990s.[243] The HKP itself had few computers, much less computer expertise, information technology professionals, cyber investigators and forensic experts.[244] In 1993, the HKP established its first-ever Computer Crime section within the Commercial Crime Bureau, with seventeen officers.[245] One of the key challenges from the outset was the ability to recruit and train a cadre of officers with good computer knowledge and skills. The HKP's lack of basic computer technical knowledge and investigative skills came to the forefront when police were not able to bring cybercriminals successfully to justice. For example, a police raid on a hacker's premises in 1995 was bungled when the suspect managed to flip the fuse-box switch and turn off the computer system, destroying all the evidence necessary for his prosecution.[246]

Because of the lack of resources, competence, and size of the Computer Crime section, much of the work done during this period was related to computer security education and advice, typical of the work of the Crime Prevention Bureau. For example, the Computer Crime Section

---

[238] *Id.*

[239] *Id.*

[240] *Id.*

[241] *Id.*

[242] *Id.*

[243] E-mail from Patrick Lam, Superintendent, Technology Crime Department, Commercial Crime Bureau, HKP, to Kam C. Wong (Apr. 6, 2005) (on file with author).

[244] *See Offbeat Online: From the Era of the Typewriter to the Computer Age* (Feb. 10, 1999), *available at* http://www.info.gov.hk/police/offbeat/649/news2.html (last visited Apr. 20, 2005).

[245] *See Offbeat Online: Cyber Patrol* (Mar. 12, 1998), *available at* http://www.info.gov.hk/police/offbeat/626/news2.html (last visited Apr. 20, 2005).

[246] Victor Yik-kee Lo, *Police Training for Cyber Transformation*, *in* BRIDGING THE GAP—A GLOBAL ALLIANCE PERSPECTIVE ON TRANSNATIONAL ORGANISED CRIME 95–99 (2002).

published an accessible computer security manual,[247] held public computer security awareness and ethics seminars, and provided on-site visits to inform small business owners about the prevention of computer crime.[248]

At the turn of the millennium, HKP computer crime law enforcement resources were devoted mainly to three areas: policing computer crime, developing computer investigative skills and forensics capability, and promoting public awareness in computer security. In order to improve computer crime investigation and prosecution, the HKP set up the Technology Crime Division in the Commercial Crime Bureau in June 2000.[249] This division was supported by a computer forensics laboratory, and augmented by a Computer Crime Investigation Cadre (currently known as Technology Crime Initial Response Team) of eighty computer-proficient officers assigned to different regions to handle minor computer investigations and forensic examinations.[250] The Technology Crime Division was left to handle more serious and complex cases.[251] In July 2001, the HKP also established a Computer Security Unit within the Crime Prevention Bureau to educate the public about the nature and extent of computer crime risks and to assist businesses in adopting measures to avoid becoming victims of computer crime.

The HKP is not the only law enforcement agency with jurisdiction over computer crime. The Hong Kong Customs and Excise Department also acquired cyberspace jurisdiction on account of intellectual property right infringements, such as piracy of movies or duplication of copyrighted compact discs. Just like the HKP, customs officers suffered from a lack of interest in and knowledge about computer technology and related computer crime investigation techniques before the 1990s.[252] In response, the Customs and Excise Department established an all-volunteer Computer

---

[247] *See* HKP CRIME PREVENTION BUREAU, COMPUTER SECURITY FOR USERS OF SMALL COMPUTER SYSTEMS 3 (1997), *available at* http://www.info.gov.hk/police/hkp-home/english/tcd/sms.htm (last visited Apr. 20, 2005).

[248] *See Publicity and Education Efforts—Hong Kong Police*, *in* HKSAR Computer Crime Report, *supra* note 11, at 78.

[249] Press Release, Hong Kong Police Public Relations Bureau, Computer Forensics Laboratory Helps Detect Computer Crime (Sept. 10, 2002), *available at* http://www.info.gov.hk/gia/general/200209/10/0910298.htm (last visited Apr. 20, 2005).

[250] Press Release, Hong Kong Police Public Relations Bureau, Commercial Crime Bureau Hindering IT (Jan. 18, 2001), *available at* http://www.info.gov.hk/gia/genearl/200101/18/0118174.htm (last visited Apr. 20, 2005).

[251] *Offbeat Online: Computer Crime Section Takes on Cyber Criminals and Hackers*(Feb. 10, 1999), *available at* http://www.info.gov.hk/police/offbeat/649/news2.html (last visited Apr. 20, 2005).

[252] CUSTOMS AND EXCISE DEPARTMENT, *Custom News: Cyber Investigation Seminar* (June 2000), *available at* http://www.info.gov.hk/customs/eng/publications/new/issue10_e.html (last visited Apr. 20, 2005).

Forensic Special Interest Group to build up basic skills and keep abreast of development in computer crimes.[253] Of the seventy-five members in the Interest Group, twenty were specially trained to conduct computer crime investigation as members of a Computer Analysis and Response Team.[254]

In January 2000, the Customs and Excise Department established its first-ever Intellectual Property Investigation Bureau, with seven officers in charge of investigating intellectual property right infringement activities on the Internet.[255] Since the reorganization, the Hong Kong Customs & Excise Department has reported successful action on 8712 copyright infringement cases in 2004 as against 10,341 cases in 2003 (a decrease of 15.8%), with the values of seizures increasing to HK $273.4 millions, as against HK $229.5 millions in 2003 (or increase of 19.1%).[256] Data from the Department (through April 2004) shows that copyright infringement arrests constituted 12.16% of the Department's activities in 2004.[257]

Although much work has been done, there are three obstacles standing in the way of effective computer crime investigation and prosecution in Hong Kong. First, there is a need to overhaul the current computer legislation to give law enforcement agencies more power to investigate cross-border computer crime. Second, there needs to be international protocol or rules governing retrieval, preservation and authentication of computer forensic evidence that can be used in criminal proceedings across national boundaries. Third, there is a dire need to provide structured and relevant computer training to law enforcement officers, so that they can appreciate the concepts and theory of fighting computer crime.

F. Computer Crime Prevention Should Focus on Education

Prevention is a proactive way of combating crime, but individual prevention and education efforts need closer coordination to yield better results. In light of the deep penetration of computers and Internet usage at home and in business in Hong Kong, public education plays a key role in raising security awareness and cultivating information technology ethics.

---

[253] CUSTOMS AND EXCISE DEPARTMENT, *Custom News: Computer Forensic Laboratory* (Mar. 2001), *available at* http://www.info.gov.hk/customs/eng/publications/new/issue13_e.html (last visited Apr. 20, 2005).

[254] *Id.*

[255] HKSAR Computer Crime Report, *supra* note 11, at 78.

[256] *See* CUSTOMS AND EXCISE DEPARTMENT, STATISTICS ON CASES AND SEIZURES UNDER SELECTED ORDINANCES, *available at* http://www.info.gov.hk/customs/eng/statistics/s_case_e.html (last visited Apr. 20, 2005). The figures provided by the Customs and Excise Department do not draw a distinction between Internet related violations and copyright violations. *Id.*

[257] *Id.*

Numerous initiatives such as exhibitions and seminars by various HKG agencies and private-sector organizations promote the importance of information security. Unfortunately, numerous HKG departments each offer their own publicity programs, which sometimes overlap. The non-governmental organizations and quasi-government agencies are also playing a very active role in information security education.

Broadly speaking, the current education efforts tend to target three major groups: the banking and finance industry, the business community (particularly small and medium-sized enterprises), and the public. In the private sector, the banking and finance industry is the most active in providing for training and education on a continuing basis. Many of the larger commercial establishments have engaged in-house professional security staff to handle information-security breaches and risk-management training. The Hong Kong Monetary Authority has taken a leadership position in working with banking members to formulate finance/banking guidelines and best practices for adoption, but did little in the area of customer education programs.

The Hong Kong Productivity Council has primary responsibility for computer security education and publicity campaigns for the small and medium-sized businesses. For example, the council and the Office of Privacy Commission for Personal Data jointly published and distributed an education leaflet entitled, "Guide to Personal Data Privacy and Consumer Protection on the Internet."[258]

The Computer Emergency Response Team Coordination Centre of the Hong Kong Productivity Council acts as an information clearance center to share and exchange security information, such as news on viruses and vulnerability of system software. It also conducts surveys, provides advice and renders assistance to prepare small and medium-sized businesses against cyber attacks.[259]

The HKSAR Computer Crime Report states that the HKG has made a conscious decision to encourage the private sector to play a larger and more active role in computer security education and publicity.[260] This approach is based upon a philosophy that "every user has a responsibility to protect his own computer system and data . . . . We cannot rely on the Government alone."[261] Regrettably, the HKSAR Computer Crime Report did not discuss

[258] HONG KONG PRODUCTIVITY COUNCIL, A GUIDE TO PERSONAL DATA PRIVACY AND CONSUMER PROTECTION ON THE INTERNET (no date available), *available at* http://www.info.gov.hk/digital21/eng/ecommerce/guideline/privacy1_4.pdf (last visited Apr. 20, 2005).

[259] *Id.*

[260] HKSAR Computer Crime Report, *supra* note 11, at para. 11.1.

[261] *Id.* at 72.

the role of the Education Department or universities in preparing the Hong Kong community, industries or citizens in meeting computer security needs, either through education or research. These organizations should have a prominent role to play in helping youth become better cyber citizens, legally and morally.

VI. CONCLUSION

The HKG wants to build an information-rich and knowledge-based economy for the twenty-first century and beyond. In constructing the information super-highway, the HKG is concerned with deviance and disorder in cyberspace. Under the leadership of the Security Bureau, an Inter-departmental Working Group has been established to study the technology problems and legal issues in making the cyberspace safe. The HKSAR Computer Crime Report proposed a framework for improving the existing cyberspace security regiments by July 2001.

Consistent with traditional philosophy and contemporary policy, the HKG has adopted a passive, reactive, minimalist, and piecemeal approach in confronting computer crimes. The HKG also does not have an overarching philosophy, long-term vision, or integrated sets of policy compatible with Hong Kong's ethos, values, and interests to bring about law and order in cyberspace. The HKG has made much noise of consulting the public and deferring to the professionals in order to map a course for computer security development, but the public, by and large, is still not aware of the significance of computer security or the necessity of information ethics. The professionals are more solicitous of their own welfare and interests than that of the public.

The HKG should adopt a comprehensive approach in formulating and implementing a computer crime policy. Governance in cyberspace is a matter of successfully managing the combinations of laws, norms, the market, the computer architecture (or code), and ethics to achieve order. A comprehensive approach to fighting computer crime also calls for cooperation from all those who have a vested interest and can make a difference. In this regard, the HKG should take a stronger leading role in promoting public awareness and mobilizing public support for computer security.

Computer crime is an emerging problem in Hong Kong. Fighting computer crime often requires joint effort from various governing regimes and assistance from different legal jurisdictions. The HKG should continue to work with international institutions and overseas regulators in sharing

information, developing best practices, and adopting uniform legislation to facilitate cyberspace governance. Finally, the study of cyberspace governance in Hong Kong is still in its infancy; there is much to be discovered by scholars, researchers and professionals in the field. It is crucial for the HKG to act before computer crime reaches crisis proportions—a price too high for Hong Kong citizens to pay.