CYBER-CRIME

The Challenge in Asia

Edited by

Roderic Broadhurst and Peter Grabosky

香港大學出版社

HONG KONG UNIVERSITY PRESS

Hong Kong University Press
14/F Hing Wai Centre
7 Tin Wan Praya Road
Aberdeen
Hong Kong

ISBN 962 209 735 9 (Hardback)
ISBN 962 209 724 3 (Paperback)

British Library Cataloguing-in-Publication Data

Secure On-line Ordering
http://www.hkupress.org

Printed and bound by Lammar Offset Printing Ltd., Hong Kong, China.

Hong Kong University Press is honoured that Xu Bing, whose art explores the complex themes of language across cultures, has written the Press's name in his Square Word Calligraphy. This signals our commitment to cross-cultural thinking and the distinctive nature of our English-language books published in China.

"At first glance, Square Word Calligraphy appears to be nothing more unusual than Chinese characters, but in fact it is a new way of rendering English words in the format of a square so they resemble Chinese characters. Chinese viewers expect to be able to read Square Word Calligraphy but cannot. Western viewers, however are surprised to find they can read it. Delight erupts when meaning is unexpectedly revealed."

— Britta Erickson, *The Art of Xu Bing*

Contents

Lists of Tables and Figures viii

Foreword xi
Justice K Bokhary, Hong Kong Court of Final Appeal

Acknowledgements xiii

Contributors xv

Abbreviations xxiii

1. Computer-Related Crime in Asia: Emergent Issues 1
Roderic Broadhurst and Peter Grabosky

2. The Global Cyber-Crime Problem: The Socio-Economic Impact 29
Peter Grabosky

3. Cyberspace Governance and Internet Regulation in China 57
Kam C Wong and Georgiana Wong

4. Cyber-Crime and E-Business in China: A Risk Perception Perspective 79
Ivan S K Chui

5. Governance in the Digital Age: Policing the Internet in Hong Kong 89
Laurie Yiu Chung Lau

6. Third Party 'Responsibilisation' Through Telecoms Policing 109
Keiji Uchimura

7. Cyber-Security: Country Report on Singapore 125
Clement Leong and Chan Keen Wai

8. Cyber-Crime in the 21st Century: Windows on Australian Law 141
Simon Bronitt and Miriam Gani

9. Cyber-Crime: Current Status and Countermeasures in Japan 169
Masao Tatsuzaki

10. Cyber-Crime in India: The Legal Approach 183
Pavan Duggal

11. Computer Crimes: What Everyone Should Know About Them 197
K H Pun, Venus L S Cheung, Lucas C K Hui, K P Chow, W W Tsang, H W Chan, C F Chong

12. Cyber-Crime Legislation in the Asia-Pacific Region 207
Gregor Urbas

13. Law Enforcement in Cyberspace: The Hong Kong Approach 243
Michael Jackson

14. International Cooperation in Combating Cyber-Crime in Asia: Existing Mechanisms and New Approaches 269
Jeffrey G Bullwinkel

15. The Council of Europe Convention on Cyber-Crime: A Response to the Challenge of the New Age 303
Peter Csonka

16. Human Security and Cyber-Security: Operationalising a Policy Framework 327
Julie Shannon and Nick Thomas

17. The Future of Cyber-Crime in Asia 347
Peter Grabosky and Roderic Broadhurst

Notes 361

References 403

Index 419

Contributors

Roderic Broadhurst is an Associate Professor, Department of Sociology, and Senior Fellow, Centre for Criminology, the University of Hong Kong. He is the current Chair of the Hong Kong Society of Criminology, Associate Fellow of the Australian Institute of Criminology and associate editor of the Australian and New Zealand Journal of Criminology. His research interests include violence, repeat offending, professional delinquency, organised crime and crime in developing countries. Recent work includes editor of *Bridging the GAP: A Global Alliance Perspective on Transnational Organised Crime,* Hong Kong Police (2003), and contributions to the journals *Forensic Science International* and *Criminal Behaviour and Mental Health.* He was co-convenor and proceedings editor of the First and Second Asia Cyber-Crime Summits held in April 2001 and November 2003 at the University of Hong Kong. (broadie@hkucc.hku.hk)

Peter Grabosky is a Professor in the Research School of Social Sciences, Australian National University, and a Fellow of the Academy of the Social Sciences in Australia. His general interests are in harnessing non-governmental resources in furtherance of public policy. His publications include *Cyber Criminals on Trial* (with Russell Smith and Gregor Urbas, 2004); *Electronic Theft* (with Russell Smith and Gillian Dempsey, 2001); and *Crime in the Digital Age* (with Russell Smith, 1998). He was previously Deputy Director of the Australian Institute of Criminology. Other appointments include Russell Sage Fellow in Law and Social Science at Yale Law School (1976–78), Visiting

Professor, Institute of Comparative Law in Japan, Chuo University (1993), Visiting Expert, the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (1995), and Visiting Professor, Chinese People's Public Security University (1996). He was Rapporteur for the Workshop on Crimes Related to the Computer Network at the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 2000. He is past president of the Australian and New Zealand Society of Criminology, and in 2000 was elected Deputy Secretary-General of the International Society of Criminology. (Peter.Grabosky@anu.edu.au)

Simon Bronitt is a Reader in Law and Director of the National Europe Centre at the Australian National University in Canberra. His scholarly interests lie in the field of criminal law and procedure, evidence, criminal justice and criminology. His research takes a broad interdisciplinary and comparative perspective, which is reflected in his recent book, Bronitt and McSherry, *Principles of Criminal Law* (Law Book Co, Sydney, 2001). He is a State Editor of the *Criminal Law Journal* and an Associate of the Australian Institute of Criminology.

Jeffrey G Bullwinkel graduated from Duke University with a Bachelor of Arts degree (cum laude) and received his law degree from New York University (cum laude). He is a member of the New York State Bar. He is presently Microsoft Corporation's Director of Corporate Affairs for the Far East Region, including Greater China, Japan, and Korea. Based in Hong Kong, he oversees a broad range of the company's activities in the region relating to the protection of intellectual property rights, as well as initiatives focused on building a safer and trustworthy computing environment. He also participates actively in industry associations devoted to increasing international protection of trademarks and copyright works, including the International Intellectual Property Association, the International Anti-Counterfeiting Coalition, the Quality Brands Protection Committee and the Business Software Alliance. In addition, he is an active member of the American Chamber of Commerce in Hong Kong. He has served as chairman of the Chamber's Intellectual Property Committee since January 2002 and was elected to the Board of Governors in December 2002. Prior to joining Microsoft, he was a federal prosecutor with the Office of International Affairs, Criminal Division, United States of America Department of Justice and, was responsible for matters relating to international criminal law enforcement, including negotiating bilateral treaties and multilateral conventions on international cooperation in criminal matters,

and providing advice on international law to the Office of the Attorney General.

Chan Keen Wai was formerly the Director of Infocomm Security at the **Infocomm Development Authority** (IDA) of Singapore. **Clement Leong** is a senior consultant at IDA. The IDA develops, promotes and regulates info-communications in Singapore, with the aim of establishing Singapore as one of the world's premier infocomm capitals. To nurture an internationally competitive infocomm industry, the IDA offers a comprehensive range of programmes and schemes for both local and international companies. For more information, visit www.ida.gov.sg.

Ivan S K Chiu obtained his BA (Hons) from Hong Kong Baptist University, and his MA and MPhil in Social Science from the Hong Kong University of Science and Technology. His main research interests are risk, reliability, safety and security in respect to science and information technology policy, cultural and the social psychology of online education. His publications (in Chinese) include, 'The Difficulty of Taking the Initiative in Online Teaching in Hong Kong' (2002) and 'The Difference of Risk Perception among the Educated Youth in Hong Kong and China: The Issue of Using Computers' (2002). He is also a manuscript reviewer for the *Journal of Risk Analysis*. (ivanchiusk@sinaman.com).

CISC (Centre for Information Security and Cryptography, Department of Computer Science & Information Systems, Faculty of Engineering, the University of Hong Kong) represents a coordinated effort to promote academic research and industrial collaboration with a mission of becoming a centre of excellence, in the University of Hong Kong and in the Asia-Pacific region. Research interests of CISC include computer security technology, cryptographic systems, network and Internet security, Public Key Infrastructure (PKI) systems, and most recently, the study of e-crime. **K H Pun, Venus L S Cheung, Lucas C K Hui, K P Chow, W W Tsang, H W Chan,** and **C F Chong** are colleagues of CISC.

Peter Csonka is currently a Senior Counsel at the International Monetary Fund's Legal Department, which he joined in December 2002. Born in Hungary and educated in France, he is a lawyer by training (LLM). In 1986–91 he was an Assistant Professor in criminal law at the Faculty of Law of Miskolc (Hungary) and conducted research at the University of Pau (France). He also practiced law as a Junior Prosecutor during this period. He then joined

the Council of Europe (Strasbourg, France), where he worked until December 2002 as Deputy Head of the Economic Criminal Law Division (Directorate General of Legal Affairs). He was in charge of legal drafting, policy and assessment-related issues in the area of economic criminal law, including cyber-crime and money laundering.

Pavan Duggal is an Advocate of the Supreme Court of India. He is the Founding President of Cyberlaw Asia, and has undertaken pioneering work in the field of convergence law. He is also President of Cyberlaw Asia, Asia's first organisation committed to the passing of dynamic cyber-laws in the Asian continent and President of Cyberlaws.Net, which is the Internet's unique online consultancy dedicated exclusively to cyber laws. He is a member of the Nominating Committee, Membership Advisory Committee and a member of the Membership Implementation Task Force of the Internet Corporation for Assigned Names and Numbers. He is a member of the WIPO Arbitration and Mediation Centre Panel of Neutrals and member of AFACT Legal Working Group of UN / CEFACT and a consultant with International Trade Centre, UNCTAD / WTO, Geneva. As a practicing advocate he has been a counsel in many path-breaking cyber law cases. He was the counsel for the complainant in the case that led to India's first cyber-crime conviction and he represented the plaintiff-company in India's and Asia's first 'Cyber Defamation' case. He was also counsel in the first Indian case for damages under India's Information Technology Act, 2000. He is the author *of Cyberlaw — The Indian Perspective.*

Miriam Gani is a Lecturer in the Faculty of Law at the Australian National University. She teaches criminal law and legal method and her principal research areas are cyber-crime, stalking, terrorism and statutory interpretation. She is currently participating, with several faculty colleagues, in a major project funded by the Australian Research Council. The project involves, in part, examining Australia's legislative response to terrorism.

Michael Jackson is a Lecturer in the Faculty of Law, the University of Hong Kong, where his teaching includes criminal law and cyber-crime. He writes mainly in the field of criminal law and is the author of *Criminal Law in Hong Kong* and a contributing author to *Archbold Hong Kong.* He was a member of the Criminal Law and Procedure Committee of the Law Society of Hong Kong from 1996–2003, and has practised criminal litigation both in New Zealand and in Hong Kong. (mjackson@hkucc.hku.hk)

Laurie Lau is a PhD candidate at the Cyberlaw Research Unit, Department of Law, University of Leeds. He was a Resident Graduate Scholar (2002–03) at the David C Lam Institute for East-West Studies, Hong Kong Baptist University. At present, he is a part-time lecturer in criminal justice studies at the University of Hong Kong. His research interests are: computer-related crimes, computer fraud, computer forensic evidence and cyber-policing issues. He has also presented conference papers in Europe and Asia. Currently he is a member of the executive committee of the Hong Kong Society of Criminology. (laurie.lau@alumni.cityu.edu.hk)

Julie Shannon is a doctoral student and an Assistant Lecturer in International Relations in the School of Political Science at the University of New South Wales. She holds an MA in International Relations from the University of New South Wales and a BA in Philosophy from the University of Sydney, and her interests include regional institutions and human security in East Asia. She has also provided research and programme management assistance for the Asia-Australia Institute's regional programmes and has recently been involved in programme preparation for the Research Institute for Asia and the Pacific training of East Timor's Environmental Protection Unit.

Masao Tatsuzaki is Assistant Director, Foreign Affairs Division, Security Bureau, National Police Agency, Japan. Previously he was Assistant Director, Security System Planning Office, Community Safety Bureau, National Police Agency (2001–03). He holds a Bachelor of Law from the University of Tokyo (1993) and LLM from Cornell Law School (1998). He is an Attorney at Law (New York), and has passed the Japan Bar examination.

Nicholas Thomas is a researcher at the Centre of Asian Studies, the University of Hong Kong. His main focus is the China-ASEAN project, which provides briefing reports on events in Southeast Asian countries to the Central Policy Unit of the Hong Kong SAR Government, and organises roundtables and meetings between Southeast Asian and Chinese scholars and policymakers. Prior to assuming this position, he worked as a Research Fellow at the Asia-Australia Institute, University of New South Wales. This involved academic research on East Asia as well as the design and management of 'Track Two' meetings between Australian and East Asian policy-makers. He has published articles, chapters and books on East Asian regionalism, human security, and Hong Kong politics. His most recent book is *Re-Orienting Australia-China Relations: 1972 To The Present*, Ashgate Publishing (UK), 2004.

Keiji Uchimura is a Professor in the Applied Technology Department, National Police Academy (Japan). He was previously Staff Officer of the First Criminal Investigation Division at Keishicho (Metropolitan Police Department) from 1997–98, and was Assistant Director in the Investigative Planning Division, Criminal Bureau, Keisatsucho (National Police Agency) from 1998–2001. From 2001–03 he completed an MSc in Criminology and Criminal Justice at Cardiff University in the UK while on secondment from Keisatsucho.

Gregor Urbas, PhD, is an academic lawyer based in Canberra, Australia. He was a researcher in the Sophisticated Crime and Regulation Program of the Australian Institute of Criminology and in the intellectual property legislation section of IP Australia, and is currently a Lecturer in the Law Faculty of the Australian National University teaching in criminal law, evidence and intellectual property. He is also a part-time Research Officer for the Law Council of Australia and has published on cyber-crime, intellectual property piracy, DNA evidence and criminal justice policy.

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

Kam C Wong is currently an Associate Professor of Law and Criminal Justice, University of Wisconsin (Oshkosh) and received his JD from Indiana and PhD (SUNY – Albany). He teaches police and homeland security related subjects. Previously, he was Director of the Chinese Law Program (1997–2002) in the Chinese University of Hong Kong. Professor Wong is currently involved with two research projects: *The Impact of USA PATRIOT ACT, on Society* and *Police Reform in Modern China.* His publications have appeared in many international criminal justice and law journals, including the *British Journal of Criminology, Georgetown Journal of Law and Public Policy, Columbia Journal of Asian Law, Australian Journal of Law and Society, International Journal of the Sociology of Law* and others. Professor Wong is an editor of *Police Practice and Research: An International Journal,* and an Advisory Board Member of the *International*

Journal of Comparative Criminology. He was the former vice-chair of the Hong Kong Society of Criminology and is an associate fellow of the Center for Criminology, the University of Hong Kong. He was President (2002–03) of the Asian Association of Police Studies and serves on the Advisory Board for the Yale in China Legal Program.

1

Computer-Related Crime in Asia: Emergent Issues

Roderic Broadhurst and Peter Grabosky

The rapid development of computer connectivity and the role of the Internet in the emergence of new e-commerce markets have increasingly attracted the attention of national governments and international agencies. Hyperbole aside, the astonishing reach of these tools has changed the way a large part of the world communicates and does business. It may be too early to evaluate claims that this medium ushers in an irresistible phase of a global 'information revolution' and, with it, a 'new economy'. However, we can be certain that with the erosion of traditional barriers to communication, our concepts of time and place have irrevocably changed and the process of 'globalisation' has accelerated.

The convergence of computing and communications and the exponential growth of digital technology have brought enormous benefits to modern society. Along with these new benefits, however, come greater risks. As never before, and at negligible cost to themselves, lone offenders can inflict catastrophic loss or damage on individuals, companies, and governments from the other side of the world. With these developments has come the awareness that 'information security' is no longer a matter for the technical and computer specialist, but for millions of people who now engage these new media every day for business, communications and leisure. The continued prosperity of industrial nations, and the economic development of the world's less affluent societies, seems likely to depend increasingly on electronic commerce. To the extent that public confidence in e-commerce is jeopardised by criminal activity, so too will economic well-being be threatened.

The new opportunities created in 'cyberspace' have also enhanced the capacity for criminal enterprises to operate more efficiently and effectively both domestically and across borders. In Asia and other parts of the world an evolving role for both individual offenders and criminal networks has emerged to exploit criminal opportunities in the e-commerce / new economy environment. The extremely rapid development of digital technologies and e-commerce in Asia, coupled with the expansion of the Internet and other forms of connectivity, has occurred at such a pace that law enforcement agencies in many jurisdictions have been unable to respond effectively. The traditional notion of information security with an emphasis on system and data protection no longer captures the scope of the risks and threats now unleashed by digital and wireless connectivity. In the chapters to follow the contributors address the wide range of problems and issues now faced in policing and regulating cyberspace and cyber-crime in Asia. The role of public and private law enforcement is crucial in curtailing criminal activity and ensuring the digital 'highways' are not lawless or hazardous but safe for all who wish to travel them. The term 'cyber-crime' is of course a misnomer, for what is described and discussed in the following pages includes computer-related crime: illegal behaviours with an obvious terrestrial dimension. As digital technology becomes more pervasive and interconnected, ordinary crime scenes are bound to contain some form of digital evidence.

■ Criminality and Computer Crime

With governments, industries, markets and consumers increasingly dependent on computer connectivity, they are prone to an array of threats. The most notable have been the widely publicised computer 'viruses', which have increased in both virulence and velocity since 2000. The beginning of 2004 saw the development of increasingly complex malicious code in the form of the 'MyDoom' or 'Norvag' worm. It apparently combined the effects of a worm, spreading rapidly across the Internet, with that of a distributed denial of service attack, where computing power is directed at a target system with a view to shutting it down. In other words, infected computers were remotely 'commandeered' and directed against the target computer. The implications of such activity for infrastructure protection are ominous (Semple 2004).

Many of these risks appear to mimic traditional criminal exploitation, albeit often executed with unprecedented ease, speed and impact across jurisdictions. Law enforcement has truly entered the digital age. The tasks of identifying cyber-criminals and bringing them to justice pose formidable

challenges to law enforcement agencies across the globe, and require a degree and timeliness of cooperation that has been until only recently regarded as difficult, if not impossible, to achieve.

As rational choice theories of criminal behaviour have gained increasing credence and the significance of pathological theories (defects of individual personality and socialisation) has declined, the perception has arisen of organised crime as essentially operating like any profit-seeking enterprise. Until the American scholar, E H Sutherland, coined the term 'white-collar' crime in 1939, the connection between business, politics and crime groups was a neglected part of criminological theory. He drew on the fundamental idea that criminal behaviour is learned through 'differential association'; that is, primary relationships that justify and support illegal conduct.

That criminal behaviour itself need not depend on social deviance is a fact that makes distinguishing good or bad behaviour from good or bad people one of the natural conundrums of policing. It also ensures that risk profiling, despite actuarial sophistication, is much more difficult than is often assumed. Thus while underlying motives are important at the individual level, at the macro level diverse criminal motives are in reality governed by opportunities — opportunities that are perceived to present low risk and high profit to the criminal or deviant enterprise.

The 'situational crime prevention' model is the criminological perspective most applicable to understanding crime and the control of opportunity-driven criminal groups or enterprises. Drawing on the work of 'situational crime prevention' criminologists such as Marcus Felson (1998) and Ron Clarke (1992; Newman & Clarke 2003), Grabosky argues that computer-related crime, like crime in general, may be explained by the conjunction of three factors: motivation, opportunity, and the absence of capable guardianship. Motives will vary depending on the nature of the crime in question, but include greed, lust, revenge, challenge and adventure.[1] Offenders tend to be generalists rather than specialists in choice of crime. Although offender profiling requires a flexible approach, there is increasing evidence of greater offender interest in financial rewards.

The convergence of these three factors in time and place — the motivated offender, a suitable target, and the absence of capable guardians — accounts for the amount of crime experienced. Crime prevention strategies based on this idea focus on strengthening the role of guardians (for example, neighbourhood watch, police telephone hotlines, CCTV) and reducing opportunity by target-hardening high-risk property (installing more effective anti-theft devices) and educating the public about the proper use of digital technology. A fourth factor, crucial to the success of a criminal act, is the extent

to which the motivated offender has access to the resources (both social and technical) that allow the act to take place. It is through a network of relationships that the various resources necessary to complete a criminal transaction are mustered; coupled with the opportunities provided by the absence of capable guardians, this is what gives criminal groups their sustenance.

■ Computer-Related Crime in Asia

Criminal opportunities are expanding globally with the rapid proliferation and penetration of digital technology.[2] A number of jurisdictions have reported substantial increases in computer-related crime following the passage of laws designed to control computer-related offences. Valeri (2001) suggests that the mixed trends in computer-related crime within the European Union reflect the partial success of longstanding regional efforts to address computer crime; this is also to an extent reflected by those jurisdictions in Asia with a longer 'history' of a formal legal response.

The relative novelty of computer crime has meant that most policing agencies have only recently developed specific measures for recording them. The advent of computer-related criminal laws and associated prosecutions and the establishment of computer emergency response teams (CERTs) and dedicated technology crime units within policing agencies, coupled with the development of crime-victim awareness and consumer advocacy, have prompted jurisdictions at the forefront of the digital revolution to begin recording the incidence of illegality in cyberspace. However, in many jurisdictions cyber-crimes, if reported, may not be differentiated from other commercial crime, fraud reports or criminal damage statistics or other categories. Thus the extent of computer-related crimes, even when reported, remains unclear.

Police statistics about reported crime often tell us more about the activities and priorities of police than they do about the extent of crime. This is because in many traditional crimes, victims do not report them to the authorities. This is undoubtedly also the case with computer crime. Replicated random surveys of crime victims in many jurisdictions over the past 30 years have shown there are various reasons why victims of crime do not report to police. These include, for example: the belief that police cannot (or will not) do anything; the offence was trivial or the victim felt the matter was better dealt with privately; reporting the case was too troublesome; or fear of reprisal or further trouble if they did report the incident (see for example Newman 1999; Alvazzi del Frate 1998).

Nevertheless, despite these limitations it is instructive to explore the available data from several Asian jurisdictions where some official records of reported computer crime are available.

We take as an example the work and capabilities of the Hong Kong Police, who have recognised the increased interdependence of global markets and have responded to the general risks to Hong Kong's commerce and financial services. The Hong Kong Police Commercial Crime Bureau's Technology Crime Division (TCD) was established in 2001 and its predecessor, the Computer Crime Section, was established in 1993. Headed by a senior superintendent with a team of 66 officers, TCD deals with computer crime investigations, computer forensic examinations, and support to force-wide investigation units both at scenes of crime and during their investigations. The TCD is divided into three sections: Operations, Forensic Investigations and Intelligence, and has a mission that broadly reflects the scope of public policing now required:

- Maintaining a professional investigation capability
- Broadening the investigation capability within the Force
- Developing accredited computer forensics
- Proposing changes in laws and policies
- Prevention and education
- Intelligence management, and liaison with industries and professionals
- Liaison with overseas law enforcement agencies and international law enforcement cooperation

In 2000, TCD conducted computer forensic examinations in 91 crime cases and in 2001 the number of examinations increased by 159 cases. The amount of computer data examined grew from 1100 gigabytes in 2000 to 4800 gigabytes in 2002 and in the first eight months of 2002, 128 cases and 3400 gigabytes of data were examined. In the same year a state-of-the-art Computer Forensics Laboratory was established, enabling each of its computer forensics examiners to handle, at any one time, three to four cases involving 'stand-alone' computers, or 600 gigabytes of data on any networked computer. (See Table 1.1.)

Cases reported under 'other' are mostly personal identification (ID) and password theft usually involving the fraudulent obtaining of access to Internet, phone and other services. While six cases of e-banking fraud were reported in 2002, all involved the 'misuse of passwords' and obtaining services without payment. Customer passwords, and not the bank system, were the actual target of offenders. Notably, Internet obscenity cases that totalled 32 cases in 1999 have since rapidly declined with only one case reported in 2001.

Table 1.1 Computer-related crimes reported in Hong Kong

Reported cases	*1995*	*1996*	*1997*	*1998*	*1999*	*2000*	*2001*	*2002*	*2003*
Hacking / cracking[a]	4	4	7	13	238	275	114	164	403
Criminal damage	2	4	3	3	4	15	27	16	16
Online deception	0	0	2	1	18	29	65	64	103
E-theft and other	8	13	8	17	57	49	29	30	66
All	14	21	20	34	317	368	235	274	588

Note: a. Unauthorised access or access to a computer with criminal or dishonest intent.

The general decline in cases reported in 2001 was thought to be due to the successful prosecution of hacking, obscenity and copyright breach offences and consumer and business security awareness. Another possibility for the rapid increase in reported computer crime in 2000 and 2001 was the widespread upgrading of computer networks and personal computers as a result of the 'millennium bug' fear and the consequent wider application of intrusion-tracking software and other security measures. Another less dramatic source of the drop in reported cases was the general reduction in the use of dial-up Internet connections and subsequent fewer cases of password and ID theft to gain free access. Although simple hacking cases have decreased, there are now increases in complex hacking, theft and criminal damage offences.

■ Other Asian Countries

Japan

In his chapter Masao Tatsuzaki of the National Police Agency of Japan describes the current status of cyber-crime in Japan, the law enforcement response, and the imperative of international cooperation. Cyber-crime is increasing in Japan, as elsewhere. Child pornography and Internet fraud are prominent, and fraud involving Internet auctions has risen sharply; government systems have been the target of attack, and viruses are common. To respond to these threats, the National Police Agency (NPA) established a Cyber Force: a mobile technical assistance unit that assists prefecture police in the course of their investigations. In 2000, 560 cases were reported, of which 87% were 'access' offences and 50% involved obscene materials. Keiji Uchimura's chapter outlines the Japanese approach to the interception and surveillance of Internet and other communications so necessary to combat the activities of Boryokudan and millennium sects such as the Aum Shinri

Kyo. He stresses the tensions between public police and the limitations of the 'Tachiainin' system (telecom enterprise technical staff) that mandates due process supervision of such interceptions.

Singapore

The chapter by Chan Keen Wai and Clement Leong from Singapore's Info-communications Development Authority of Singapore (IDA) outlines the Republic's efforts in both developing an information society and fostering information security. The emphasis in Singapore is that computer security and crime prevention is everybody's responsibility. In 2000 a special computer response group was created and merged with the Commercial Affairs Bureau of the Finance Department. In the first (financial) year of operation, 75 computer investigation cases were reported. In the same year 191 computer-related offences were recorded and, of these, 82% involved intrusion offences; most (64%) involved global roaming services.

Korea

The Korean Information and Security Agency (KISA) is the most active agency responsible for cyber-crime control in Korea and is a reflection of the nation's rapid acceptance of information technology. KISA has helped developed a comprehensive package of legislation and programmes designed to ensure a secure e-commerce environment hostile to cyber-criminals. Korea was one of the first countries to criminalise spamming and advocates a vigorous public education programme centred on a 'Prevention Day' on the 15th of every month. Of the 2000 incidents reported by KISA in 2001, 33% comprised 'spam' mail; 11% were virus or 'cracking' offences, 9.1% obscenity offences, and 43.5% were personal information and privacy intrusions. Korea's pioneering responses to the ubiquitous menace of 'spam' include efforts to both criminalize this conduct and to stress the critical role of consumer awareness. However, 'spammers' from outside Korea's borders still operate with relative impunity. KISA estimated that on average 41 'spam' mails were received per person per day in Korea in July 2003 and unless spamming was addressed this was likely to flood email systems to extinction. KISA notes that many 'relay servers' were sourced from schools and that improving information security in that sector along with requiring ISPs to register bulk mailers may stem the flood of unsolicited commercial email. According to a KISA survey

56% of 'spam' involved sexually explicit material, 19% other illegal products, 14% was fraud style emails, and 11% other forms of advertising (Broadhurst 2004).

China

The Information Security Supervision Bureau of the Ministry of Public Security of PR China estimates that in 2002 there were approximately 48.8 million Internet users, nearly 30 million computers and 150 000 websites in China. Just fewer than 5000 computer crimes were reported in 2001, up from about 2900 in 2000 and around 400 in 1999. By mid-2002 the bureau had reported just over 3000 cases. It estimated that by year's end it would handle 350 cases of system intrusion and over 800 cases of damage to computer systems.[3] The number of cases identified by the bureau was thus seen to be growing at an overwhelming rate, although many cases went unreported or unnoticed. Most offenders were younger people (aged 18–30) with most attacks mounted from Net or cyber-cafés with offenders hiding their identities by connecting through a http or Sock proxy, by fake IP addresses or by employing cryptography or steganography. Consequently, stronger measures have been taken in the registration and monitoring of cyber-cafés, with many being closed or reorganised.

At present, the bureau labours without specific laws and with no explicit definition of computer evidence or procedures to retrieve evidence. Although current regulations (Regulation of Security and Protection of Computer Information Systems of the People's Republic of China 1994; Management Regulation of Security and Protection of Computer Information Networks Connected with the Internet 1997; and the Criminal law of PR China 1997) relating to cyber-crime are complex, they lack the detail to enable successful enforcement, while emergency response and case reporting measures have yet to be fully developed. Being implemented are basic policies that seek to place prevention as the priority, along with the protection of crucial computer systems while strengthening education and propaganda about information and computer security. More needs to be done to develop the local information security industry and to improve the level of cooperation with foreign police in the pursuit of cross-border cases.

Thailand

Although no specific computer crime statistics are available for Thailand, the Royal Thai Police have set up an Internet Hotline.[4] In its first eight months, 3640 incidents were reported. Over half related to pornographic websites (39% Thai and 23% foreign languages) and a further 15.5% related to pornographic products or prostitution. About 10% related to intellectual property piracy or other illegal products, 3.5% to gambling sites and 7.5% to national security. Several new laws are being worked on (Electronic Transaction, Signatures and Fund Transfer Laws, Computer Crime, Data Protection and National Information Infrastructure Laws) by the newly restructured (November 2002) Ministry of Science and Technology. The *Electronics Transaction Act* B.E. 2544, which provides electronic transactions and signatures, came into effect in April 2002, and the computer-crime law now in draft follows the framework of the Council of Europe's Cyber-crime Convention. ThaiCERT was established in April 2001 and at present the Royal Thai Police, the Special Investigations department of the Ministry of Justice and the National Electronic Computer Technology Centre are responsible for dealing with all aspects of cyber-crime in Thailand.[5]

Indonesia

Indonesia, one of the largest countries in the region, has an Internet service that is estimated to serve about 7.5 million users via 170 ISPs. Internet banking began in 1998–99, and the most prevalent cyber-crime is the misuse of payment cards. Website defacing of the major banks and government departments have been reported, as well as cases of cyber-squatting and typo-pirating. At present there is no legal framework, although draft cyber-crime, electronic and personal data protection laws are being drawn up. A significant lack of relevant human resources among law enforcement and IT professionals is acknowledged.[6]

Philippines

Since the infamous Trojan type 'I love you' virus was launched from the Philippines in May 2000, the passage of the *Electronic Commerce Act* in June 2000 penalised hacking or cracking and piracy offences. Since the passage of the new law, there have been ten cases of hacking as well as cases involving

cyberspace defamation, pornography, gambling, and the sale of firearms and drugs. The National Bureau of Investigation (Anti-Fraud and Computer Crimes Division) along with the Intellectual Property Office, the National Telecommunication Commission and the Department of Trade and Industry, has overall responsibility for addressing computer-related crime. A comprehensive cyber law is under study with proposals to criminalise intentional unauthorised access, computer sabotage, domain squatting, spamming, and the illegal distribution of copyright products. The Philippines National Police have limited capacity and generally lack technical capability, trained investigators and developed domestic and regional cooperation mechanisms.[7] Weak banking laws make the Philippines an ideal 'staging' post of money laundering via wire or electronic transfer.

The position of Uzebekistan, Kazakhstan and Mongolia is considerably less developed than the countries reported above, although all are in the process of developing both laws and infrastructure to enable e-commerce. Vietnam, Laos, Cambodia, Myanmar and North Korea have yet to enter the digital age, although the North Korean government may be developing an information warfare capability.

■ Transnational Policing and Cyber-Crime

Cyber-crime is often transnational crime, and efforts to address it therefore need to adopt a transnational approach. The focus here is on the development of international and multilateral efforts aimed at addressing increasing threats posed by various computer-related crimes and the associated investigative, evidentiary, legal and procedural problems. A simple but effective response is the need for expedited (e-mail) requests for mutual legal assistance (MLA); a number of nations are moving towards compulsory disclosure of cryptographic keys subject to judicial oversight (Grenville-Cross 2003).

The transnational nature of cyber-crime reflects the process of globalisation, which has intensified over the past two decades. By globalisation, we mean the general shift of economic forces towards multinational and interdependent markets coupled with a decline in the capabilities of individual states to assert independent jurisdiction over such markets. The pace of this process, characterised by the expansion and transnational flow of capital coupled with 'real-time' communications, undermines the power of states to control (or protect) both markets and populations from external forces. The revolution in information and communication technology (ICT), particularly digital technology, has

accelerated the impact of transnational capital flows and production such that traditional concepts of time, distance and place have fundamentally changed. The emergence of e-commerce, as well as the social dimension of the Internet and associated 'cyber-crimes', is a striking example of the challenges to the independent capability of nation-states to regulate social and economic order within their territories. As significant has been the shift in the form of economic management, because by the 1990s most of the largest economies in the world were transnational corporations and not nation-states. Braithwaite (2000) argues that the influence of transnational corporations and the numerous hybrid private-public international regulators (for example the Basle Commission on Banking Supervision) serve to reduce the dominance of the regulatory role of states.

Radical versions of globalisation go further and suggest that the nation-state system of international relations no longer provides an effective methodology for regulating either domestic or transnational activity, especially international trade. In either version of globalisation, so-called 'sub-state' actors, such as large commercial institutions, play a crucial role in the emergence of what Sheptycki (2000) terms a transnational-state-system. In this system, new configurations of actors and power emerge and transnational organisations (both licit and illicit) will flourish due to the diminishing sway of the state (Lizee 2000: 165). The roles of multinational agencies such as Interpol and the United Nations have never been more essential. Yet within Asia (and globally) the results fall far short of creating a seamless web of bilateral or multilateral agreements and enforcement that would ensure a hostile environment for cyber-criminals. The compatibility of criminal activity with these global changes is illustrated by the expansion and convergence of the profitable business of smuggling of humans, narcotics or other illicit commodities with the development of communication infrastructure and trade.

Given the context just described, what may eventuate in the absence of the rule of law in transnational environments is 'governance without governments' (Rosenau 1992). While there now exist international conventions and treaties expressly designed to inhibit serious criminal networks or offenders operating across borders, the reach of these instruments is limited by the speed and scale of domestic ratification and consequential enabling laws. Nevertheless, they provide a moral climate hostile to some forms of transnational crime and seek to harmonise laws and evidentiary processes that enable cross-border investigations to take place as well as other cooperative undertakings.

The UN Convention Against Transnational Organised Crime (the TOC Convention) was introduced in December 2000 in Palermo, Italy.[8] The TOC

Convention significantly extends the reach of the 1988 Vienna Convention Against Illicit Traffic in Narcotics and Psychotropic Substances. The TOC Convention establishes several offence categories: participation in an organised criminal group, money laundering, corruption and obstruction of justice as well as protocols in respect to trafficking in women and children, illicit manufacturing and trafficking in firearms, and smuggling of migrants. Serious crime is defined broadly (conduct attracting punishment of four or more years' imprisonment). The basis of the framework is one that yields such flexibility in the definitions of both organised and transnational crime that it may serve as a generic legislative model across diverse common law and continental systems. In addition, the TOC Convention expressly refers (Art. 29 (2)) to methods for combating the misuse of computers and telecommunications networks. Provisions for training and materials, especially assistance for developing countries, place obligations on capable states.

As well as the innovations provided by the TOC convention, the Council of Europe's Convention on Cyber-crime, discussed in Peter Csonka's chapter, was completed in November 2001. It specifies a variety of computer-related offences.[9] The convention is designed to deal with the special problems of cyber-crime and the inevitable transnational character of many of the offences involved. Upon ratification, the convention will provide law enforcement agencies with the basis for investigating and preserving vital evidence in the cross-border dimension so characteristic of those forms of crime that exploit new information and communication technology. In dealing with ICT crime, law enforcement is at a disadvantage because of the remarkable speed in which cyber-crimes unfold against the typically 'low-speed cooperation' offered by traditional forms of mutual legal assistance. Although requests for law enforcement assistance are now routinely undertaken on an officer-to-officer basis via encrypted e-mail, this novelty should be available to judicial officers in the future. It is now conceivable that 'letters rogatory' and associated instruments may in the near future arrive by secure encrypted e-mail, as already do many of the communications between law firms.

These developments are mirrored by the increasing transnational activities of corporate and private security. Indeed, given the role of (self-) regulatory[10] approaches by corporations, especially multinational enterprises, the role for transnational private policing is already significant and widespread (Johnston 2000). For example, private security is the major provider in the payment card industry, intellectual property investigations and airline security. The sheer volume of potential global cyber-crime activity compels police partnerships with banks, telecommunication providers and corporations.

Partnerships also raise real issues of shared intelligence in environments of trust. Thus the mobilisation of so-called 'private police' and non-government organisations in partnership with public police are essential if cyber-crime is to be contained. Crime exploits the 'gaps' in the sovereign state system of international relations and, unless it is recognised that in communities of 'shared fate', coordinated forms of regulatory endeavour (free, for example, from unduly strict or pedantic definitions of 'dual criminality') may be the only means to curtail cyber-crime and its inevitable cross-border dimension. To fail to recognise that we share a 'common fate', that problems belong to others and not ourselves alone, undermines the very basis of mutual legal assistance — reciprocity.

Regional Coordination and Cooperation

As noted by Jeff Bullwinkel in his chapter, although cyber-crime has drawn increasing attention at both national and international levels in Europe and North America,[11] rather less is known about the nature and extent of the problem in the Asian region. Gregor Urbas provides a comprehensive overview of the current status of Asian jurisdictions in the development of domestic laws to address computer-related crime and the protection of intellectual property. Bullwinkel provides a detailed review of the international effort to manage the impacts of cyber-crime.

Regional efforts have begun, notably through ASEAN and the APEC forum. Such developments have yet to evolve into fully institutionalised forms of cross-border legal cooperation or significantly influence the response of states within the region.[12] However, the 'Interpol Asia and South Pacific Working Party on IT' is active, and nine countries within the Asia-Pacific region participate in the Cyber Crime Technology Information Network System formed by the National Police Agency of Japan.[13] There are now significant regional forums for police and other law enforcement officials and there is routine exchange of consular police liaison officers.

In recent papers, both Keiichi Aiziwa (2001) and Yasuhiro Tanabe (2004) of the United Nations Asia and Far East Institute for Crime and the Treatment of Offenders (UNAFEI), have argued that existing MLA Treaties including extradition are inadequate. Key problems relate to dual criminality, reciprocity, and the non-political nature of the predicate offence in order for formal cooperation to take place — states must mutually agree that the conduct is outlawed. The Council of Europe approach is innovative because it requires requested states to assist regardless of dual criminality. The treaty places

emphasis on preserving evidence and reducing procedural delay while promoting the role of 24/7 agents (24-hour, 7 days a week contact or liaison). Michael Jackson outlines the approach and scope of Hong Kong's arrangements for facilitating mutual legal assistance, extradition and evidence collection (see also Luk 2001; Blanchflower 2003).[14]

The various measures now operating within the European Union, notably the Council of Europe Convention, the establishment of EUROPOL and a European Judicial Network, provide examples of greater law harmonisation and fewer opportunities for transnational criminals to exploit jurisdictional and legal loopholes between nations.[15] European initiatives in international crime provide sound examples of the way forward in regional cooperation, but may not serve as a model for the development of countermeasures in the vastly different socio-cultural and economic circumstances found in Asia (Khoo 2003). Nonetheless, it is abundantly clear that cyber-crime, and not just the traditional concerns about narcotics and piracy, is a matter of significant concern. Thus 'international law enforcement' has shifted from a peripheral to a central role within otherwise domestically focused law enforcement agencies. In addition, the lines between the policing function and national security appear less distinct, and considerable overlap now routinely occurs between the agencies countering threats such as cyber-crime, low-intensity warfare and terrorism. Thus, importance is attached to intra-agency cooperation within jurisdictions and the need to improve and maintain these to enhance MLA at the regional and international levels.

While ASEAN[16] has provided a limited pan-Asian approach, it does form a basis for developing a wider regional forum for considering matters of MLA. Its approach, even given the developing nature of the region, mirrors the methodology of the European Union. The sheer cultural and economic diversity of Asia makes the process of multilateralism fraught with difficulty (Khoo 2003). Yet understanding the different capacities and perspectives of how each state could contribute was an essential first step. The endorsement in October 2000[17] of the action plan of the ASEAN and China Cooperative Operations in Response to Dangerous Drugs (ACCORD) in partnership with the United Nations Drug Control Program (UNDCP) illustrate within our own region the quickening of MLA responses to transnational crime such as cyber-crime. ASEAN has conducted four ministerial meetings on problems of transnational crime (Manila 1997, Yangon 1999, Singapore 2001, Bangkok 2003). These meetings oversee the work of the Annual Senior Officials Meeting on Transnational Crime and consider the deliberations of ASEANAPOL meetings of the ASEAN National Chiefs of Police and their cooperative efforts to combat transnational crime.

Julie Shannon and Nick Thomas provide an overview of the role of 'human security' models in dealing with complex threats posed by cyber-crime. They suggest that over-reliance on the state, especially the public police, to address cyber-security issues would expose both markets and society to frequent low level, but costly, risks. Consequently the role of public-private police partnerships in the market-place and the emergence of civil society on the Internet, combined with public awareness, may be the only viable means to contain cyber-crime among ordinary users.

Internet Security and the Public

Internet connectivity is now estimated to reach over 50% of the populations of the most developed nations in the Asian region and an increasingly significant number of people in the less developed nations have on-line access.[18] China, for example, in 2003 had nearly 50 million Internet users, and about 30 million computers regularly connect to the Internet. Internet penetration was reported to reach 19% of households in cities such as Beijing, Shanghai, Guangzhou and Shenzhen. Chinese households were connected for an average of 9.6 days a month and web surfing accounted for 61% of activities online, followed by e-mail (19%) and Internet messaging (10%).[19] This was low compared to the 45–48% connected to the Internet estimated for cities like Hong Kong and Singapore and the high rates of participation reported for Japan, Taiwan, and Korea. However by the end of 2002, in the People's Republic of China (PR China) about 57 million or 5–6% of households had access to the Web (about 33 million computers online) and by the year 2006 it is expected that 200 million (15% of the population) or 25% of households will be connected (Neilsons / Netrating 2002).[20] In short, China will become one of the largest populations of computer and Internet users[21] when compared to the most developed countries such as the United States (166 million with Internet access), United Kingdom (29 million), Japan (51 million) and Germany (32 million). The striking challenge that this rapid uptake in connectivity poses for e-governance is addressed later in the chapter by Wong and Wong. In China, the growth of M-commerce and WAP (wireless applications) access to the Internet is also likely to grow faster and pose similar risks to commerce.[22] Mobile phone users are now estimated to number 198 million and may reach the astonishing figure of 500 million mobile / land phones by 2006.

Among the Asian tiger economies / 'little dragons' (Hong Kong, Singapore, Taiwan and Korea) and Japan, Internet access has already reached between

40 and 60% or more of households. Many of those households and business have also adopted broadband access. Both the speed and utility of connectivity have been enhanced by developments in data compression, while telephone line connectivity may present less of a barrier to data transmission. This is especially the case with the large data files needed to transmit digital images (movies, books and music). In contrast to such astonishing developments are the Asian Central Republics and ASEAN's least developed economies: in Laos, Cambodia, Mynamar and Vietnam, Internet access is less than 1–2% of the population. The gap between the digital 'haves' and 'have nots' could not be greater.

E-commerce customers and businesses are most concerned about threats to the integrity of financial transactions as well as violations of privacy. Ivan Chiu's research on the attitudes of Chinese users and their concerns about privacy and risk provide an example of the universality of this issue. Risk of card fraud, the ability to track purchases and delivery, and legitimacy of online merchants were more important than convenience, lack of sales support and the personal touch (Lisker 2001; Valeri 2001). The UK National Consumer Council reported that many consumers cited concerns about releasing credit card details as the major reason for considering e-commerce risky. Internet shopping was regarded as the most unsafe of all methods (survey undertaken in August 2000, cited by Valeri 2001). Based on research reported by a payment card enterprise, Lisker (2001) showed that fraud involving Internet services has tended to cluster around 'adult' or pornographic content sites,[23] online services, and direct marketing activities. He also notes a significant trend towards the use of online payment methods and it was forecast that 52% of all payment card transactions would be conducted remotely by 2005.[24]

The exponential growth of computer usage and Internet connectivity is expected to continue unabated, but it is also evident that this increased connectivity will be highly structured and unevenly distributed. The gap between wealthy and poor, the computer literate and illiterate, will also significantly widen, both within and across nations.[25] Access constitutes an important indicator of both national and individual potential for growth. It attracts attempts, enlightened or otherwise, at governance of this new arena for markets and social relations. The fundamental issue of how to regulate and police this new arena, 'cyberspace', is the basic focus of the chapters that follow. The contributors cover the international or multilateral implications of cross-national cooperation through to the role of the private and public sectors in information technology security, and the forensic issues involved in the investigation of computer-related crime.

Responding to Computer-Related Crime

The expansion of computer connectivity and the associated risks to data privacy, new modes of criminal opportunity, and other nuisances present special difficulties to law enforcement agencies. Moreover, the increasing take-up and connectivity (via TV) of digital technology means that cyber-crime is becoming a core business rather than a specialised function of law enforcement. Most significantly, attacks are instantaneous and often remote, disregarding national sovereignty.

However, digital technology also affords new opportunities for individual citizens to communicate efficiently with police. An example is the Internet Fraud Complaint Center, which operates in the United States and receives online information from members of the public relating to questionable online activity. Personnel at the centre evaluate these communications and refer them to the appropriate agency or jurisdiction. At the international level, Interpol has stressed financial and high-technology crime — two of Interpol's top five priorities (along with drugs, terrorism, people smuggling and organised crime).

The threat of cyber-crime and the capacity to respond to it will vary dramatically across nations. Nearly half of Interpol's member countries lack the infrastructure for online communication (Noble 2003). The UK response to this challenge was to establish a National High-Tech Crime Unit and along with the G8 network (with its 17 members) for 24/7 or round-the-clock liaison in cyber-crime matters. There remains, however, a need for enhanced mutual legal assistance, for speedier processes for extradition, for consistent evidential standards, and for improved liaison between police and industry.

The scope of criminal activities, and associated law enforcement and their social consequences, are expanded upon in the next chapter by Peter Grabosky. A typology of computer-related crime comprises the following: conventional crimes in which computers are instrumental to the offence, such as child pornography and intellectual property theft; attacks on computer networks; and conventional criminal cases in which evidence exists in digital form.

The kinds of criminality encompass the following (by no means exhaustive) list:

- Interference with lawful use of a computer: cyber-vandalism and terrorism; denial of service; insertion of viruses, worms and other malicious code
- Dissemination of offensive materials: pornography / child pornography; online gaming / betting; racist content; treasonous or sacreligious content
- Threatening communications: extortion; cyber-stalking

- Forgery / counterfeiting: ID theft; IP offences; software, CD, DVD piracy; copyright breaches etc
- Fraud: payment card fraud and e-funds transfer fraud; theft of Internet and telephone services; auction house and catalogue fraud; consumer fraud and direct sales (e.g. virtual 'snake oils'); on-line securities fraud
- Other: Illegal interception of communications; commercial / corporate espionage; communications in furtherance of criminal conspiracies; electronic money laundering

The offences are diverse, but many are traditional crimes executed with new technology. Thus the appropriate response is guided by new technological disciplines. Lucas Hui and colleagues in their chapter present an example of cooperation between police and universities when they discuss a new forensic tool developed jointly by the Hong Kong Police and the Center for Information Security and Cryptography at the University of Hong Kong. The Digital Evidence Search Kit, or DESK, enables investigators to search for patterns in both Chinese and English, as well as to identify codified or deleted files. The technology permits inspection of the suspect's machine from a connected computer, while locking the suspect's machine to preserve file integrity. They stress the vulnerability of computers, especially via e-mail services, and note that system security is closely related to the capabilities of system administrators and auditors.[26]

Forensic computing and evidence preservation protocols are essential to effective investigation and prosecution, especially given the trans-border nature of evidence collection (Chan 2001; Pollitt 2003).[27] In most cases it is unlikely that a computer expert will be available at the crime scene and the risks of contaminating the evidence are high. Consequently, as with other types of crime, the emphasis is on following the traditional chain-of-evidence rules and ensuring that command and control assigns the relevant expertise promptly to the task at hand. Frequently this will require drawing on expertise in the private sector or academia.

■ Criminal Networks and IT Crime

Striking illustrations of the practicality of social network theories (Castells 1996) in understanding the impact of global communications on criminality are the behaviour of computer viruses. The way in which computer viruses (for example the 'I Love You' bug and the 'Code Red' worm) may spread, within days, to virtually every computer network and terminal around the world

shows how connections facilitate behaviour. Little imagination is required to extend the ideas behind these dramatic phenomena to the actual and potential networks of social relations that enable illicit commodities to move across borders and to be distributed to consumers. Organised crime 'is a social phenomenon, a network of relationships based on reciprocal benefits that extends to the heart of society and of institutional and economic life'. Nor is it simply a problem of the criminal law but one of 'civil law, economic regulation, industrial management, and fiscal policy' (Jamieson 2001: 386).

There is growing evidence to show that digital technologies have greatly enhanced the effectiveness of forgery and counterfeiting, especially of ID documents, payment cards and bank and securities instruments. IP and other copyright infringements have now become lucrative targets for organised criminals, while smuggling (humans, endangered species, narcotics, precursors, disc stampers, and arms) and traditional customs avoidance are assisted by the application of encrypted communications and the use of sophisticated forged documentation.

Apart from the use of digital technology to improve forgeries and instruments of deception, organised crime groups appear to have used IT to assist in online gaming (and gaming scams), pornographic sites and advance fee and other deception offers via e-mail or websites. The major area of risk is forged payment cards and related ID theft to obtain goods including via online transactions. The Hong Kong Police Organised Crime and Triad Bureau report few cases of systematic triad involvement in online fraud; traditional activities of protection, debt collection and vice are still dominant. Nevertheless, China's 'opening up' policy and its rapid development as a market economy have allowed foreign criminal groups to establish relationships with local groups and to invest directly or indirectly in licit or illicit business. This infiltration of foreign syndicates has helped to enhance the size and reach that serious criminal groups have in many cities and towns across China. Local criminals have shifted activities, once typically based on 'black markets' and commodity theft, into lucrative intellectual property offences, trafficking, vice and gaming. The most insidious aspects have been the criminal investment in factories (both licit and illicit) including state-owned enterprises through the corruption of officials. Chinese police, once reluctant to develop arrangements with their counterparts, now actively seek the cooperation and assistance of overseas colleagues and support arrangements for shared intelligence and capacity-building (Zheng 2003).

Although there is little novelty in the criminality involved, its scale and scope make contemporary cyber-crime of a different kind from crimes of the

past. In future, organised crime may be expected to recruit IT specialists, intimidate corporate insiders to obtain access to IT systems, and use anonymisers and encryption in furtherance of cyber-crime. Such a global problem demands a global solution. In addition, the nature of telecommunications has changed: there are no more monopolies, geographically confined. Now a single communication can pass through many providers in different countries with different legal systems. Remote attacks are now possible. Whether they are the work of a 14-year-old, a terrorist, a foreign intelligence service or an organised criminal may not be immediately apparent; all must be investigated.

Digital footprints are fragile or ephemeral, so swift action is often required. This becomes very difficult when an attack transits multiple jurisdictions with different regimes for preserving evidence. Traditional methods of law enforcement are therefore no longer adequate. A slow formal process risks losing evidence, and multiple countries may be implicated. Following and preserving a chain of evidence is a great challenge. Even 'local' crimes may have an international dimension, and assistance may be required from all countries through which an attack has been routed. Examples include the case of Mafiaboy, whose distributed denial of service attacks in February 2000 was a watershed event: the seriousness of the threat and the vulnerability of e-commerce became apparent. The investigation of Mafiaboy was a textbook example of close cooperation between the FBI and the Royal Canadian Mounted Police; only rapid and close collaboration between the two police services could have achieved such a result.

Among the challenges faced by investigators is the enormous increase in storage capacity in today's computers, and the challenge to effective and efficient searches that this entails. Almost every case will soon require computer forensics, and evidence will be located in multiple places. The challenge faced by investigators will be one of *information management* (Pollitt 2003).

The Role of Public and Private Security

Digital technologies have greatly facilitated the commission of such traditional offences as intellectual property theft, piracy, counterfeiting and forgery.[28] Generic problems of forgery and counterfeiting were the focus of Interpol's efforts illustrated by a recently established Universal Classification System for Counterfeit Payment Cards secure website. This secure site provides up-to-date information on trends and techniques with respect to the

forgery of payment cards and fraud. Apart from illustrating how Interpol's unique clearing house function[29] can be adapted to meet new problems it shows that, with fiscal and technical support from the payment card industry, the law enforcement community can be better trained and equipped. This cooperation strengthens police capacity to respond to the theft of payment cards and other computer-related crimes that reduce the integrity of the market and limit the social benefits of Internet communications. It takes little imagination but considerable endeavour[30] to see that a rapid application of this model to many global and transnational crimes would help fulfil repeated recommendations for more practical support for cross-national cooperation in law enforcement.

As well as serving as an example of how international agencies can assist with essential tasks, such as secure shared intelligence, this example also clarifies the role of private non-state actors in the prevention of crime. Private investigation has grown significantly in recent years, and there is now much closer cooperation between the private IT security sector and law enforcement. Cooperation is paramount but there is still a degree of mutual suspicion and uncertainty about what form this cooperation should take. These matters are discussed with emphasis on the way individuals and private industry can contribute to their own security, since commercial and computer crime is generally an area of weak policing.

The active cooperation of the private sector is essential in assisting police investigations. Given corporate victims' reluctance to report cyber-crime attacks, Len Hynds (2003), Director of the UK National High Tech Crime Unit, has proposed a new initiative: confidentiality contracts between police and victim. Such contracts can serve to harness intelligence that would otherwise be lost because of non-reporting. He also observed that police should begin to appreciate the mindset of corporate executives and that the police may have a role in collecting and sharing business intelligence.

The FBI has also stressed that critical infrastructure protection is a current priority in the United States. This is particularly challenging, given that most elements of critical infrastructure such as power generation, telecommunications, transport, and institutions of the financial system are owned by the private sector. The need for cooperation between law enforcement and the private sector is obvious. To help bridge the public–private gap, the FBI has introduced its Infraguard Program with over 4000 members (Iden 2003).

Reinforcing the essential need for industry self-help, Li (2001) cited recent survey data from the United States that shows 70% of organisations experienced unauthorised use of their computers but, of these, only 44%

reported the intrusion to the police. Among the most frequently cited reasons for not reporting intrusions was the fear of negative publicity and / or giving a competitor an advantage. He also stressed the neglected observation that a significant threat arises within the victim organisation from employees and other insiders and this risk may be higher than the more widely publicised attacks by outsiders.

Effective control of cyber-crime, however, requires more than cooperation among institutions of public and private security. The role of the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation cannot be understated. No less an entity than Microsoft has now committed itself to reducing the vulnerability of its products (Charney 2003).

■ Copyright and the Internet

The problems of protecting various forms of intellectual property (IP), specifically music, motion pictures, games and computer software, are heightened in the Internet environment. Significantly, as digitised versions of these products become available, Internet access is rapidly becoming the preferred means for obtaining them. Consequently, the illegal or unauthorised access to relevant Internet sites is perceived as both a motive and source of increased risk to IP holders. Given that IP piracy has traditionally been widespread within the Asian region, it had been thought that only an unlikely radical change in community attitudes could impact on the volume of 'illegal' sales. While community sentiment, at least in Hong Kong, has shifted away from pirated products, this was assisted by a multi-level enforcement approach that incorporated vigorous and sustained investigation and prosecution with the full cooperation of the relevant industries. The inclusion of copyright offences as part of Hong Kong's Organised Crime Ordinance provided better legal prescription and aided customs agents in cooperation with private sector counterparts to substantially improve IP protection Tsang (2001).

In Hong Kong and other jurisdictions, however, non-actionable cases were typically linked to overseas or cross-border events. Although IP piracy is often touted as a problem restricted to wealthy multinational corporations and not a significant local or Asian issue, it is apparent that IP piracy can also be fatal to indigenous IP holders, as Malaysian, Thai, Mandarin and Cantonese artists have lamented. Typically in Hong Kong and other jurisdictions, government willingness to address legal loopholes, including extradition, and provide police with resources is still a critical factor since the deterrent value of

punishment and the associated publicity is a crucial part of any multi-level approach.[31]

Poon (2003) observed how digital technologies facilitate IP and copyright infringements. He noted that there were many websites in Hong Kong for downloading pirated content. In response to this challenge, Hong Kong Customs has a forensic special interest group, a computer analysis and response team, an anti-Internet piracy team, and a computer forensics support team with its own lab. The three most pressing problems they face are limits of territorial jurisdiction, impediments to the acceptance of digital evidence, and the fact that many offenders commit their offences from overseas. Poon concluded that to meet these challenges will require active dialogue with industry, improved forensic skills, and better technical means for the collection, preservation and presentation of digital evidence.

Copyright, however, is primarily a private right and the IP holder or industry has the responsibility to be active and vigilant in the protection of such rights.[32] As many commentators note, piracy is sustained by public demand and the need for education and raising respect for IP are also important factors. Given the relatively low investment required to set up activities such as optical disk piracy, even rigid inspection and raids may merely force them underground and / or displace activities to weaker jurisdictions. More resources may not be enough because of public demand encouraged by low prices. Efforts by governments[33] and consumers to encourage better pricing of legitimate products and fund public education are seen as positive measures.

China has suffered heavily from piracy despite a strong policy to crush illegal operators. Although 115 underground optical disk manufacturers had been closed before 2001, the problem continued as offenders had actively countered government schemes that encouraged reporting of illegal operations. The ready supply of unemployed workers provided IP 'pirates' with an ample sales force and distributive network, and modifications to the criminal law were necessary to criminalise this conduct.[34] He also noted that considerable quantities of pirated good were imported from neighbouring countries. The pressure on IP pirates in Hong Kong had led to the displacement of factory-style operations to China and, unless the financiers are targeted, the underground industry is destined to continue.[35] Malaysian police, who have also been concerned with targeting the financial sources of piracy production,[36] have observed a similar displacement effect. Nevertheless, it is apparent that targeting optical disk 'stampers' and the introduction of mandatory laser recorded codes would be the most helpful strategically.

Industry is responding with impressive resort to additional remedies, as a recent successful civil action in PR China on behalf of the motion picture industry illustrates. The Motion Picture Association (MPA) achieved resolution of two civil actions in relation to DVD piracy in the Beijing Second Intermediate People's Court, and six cases in the People's Courts of Shanghai, in 2003. The terms of the settlements included: ceasing further replication and destroying all copies; making formal apologies; the payment of penalties averaging US$10 000 per case; and an agreement to pay increased penalties if unauthorised replication recurs.[37]

The Role of Law and Comity Between States

Many nations and regional bodies such as the Council of Europe have addressed these issues and laws exist that criminalise unauthorised access and unlawful use of computers, but such laws are neither universal nor uniform.[38] In India, the recently passed *Information Technology Act 2000* is instructive, and provides a variation on the approach adopted by the Europeans. The Act aims to facilitate e-commerce governance, and specifically recognises electronic evidence and signatures. The Act creates two levels of cyber-crime: infringements and offences. Infringements (eight types are specified) focus on improper use of computers and impose no fines or criminal punishment, although compensation can be ordered via non-judicial civil compensation mechanisms. Offences, however, include hacking, destruction of data, unauthorised access, misrepresentation / fraud, and the publication of offensive material and are dealt with through normal criminal proceedings. The law creates special prosecutors and courts to deal with special offences and requires police, prosecutors and judges to be technologically literate.[39]

Law enforcement agencies are now compelled to respond to cyber-crime through technological adaptation (retooling) and legal innovation. Consensus is the best strategy, for the suppression of computer-related crime entails a mixture of law enforcement, technological and market-based solutions. We argue, however, that a strict enforcement agenda is usually not feasible because of the limited capacity of the state. It is also feared that over-regulation could stifle commercial and technological development. Those sceptical of a heavily interventionist approach also argue that the marketplace may at times be able to provide more efficient solutions to the problems of computer-related crime than the state. Even if they were increased, police resources could never be enough. Without political will, public support (especially awareness of the potential threat) and the cooperation of industry in the context of a global

response, policing is unlikely to bring timely relief. Given pressures on government to reduce public expenditure, the challenge is to enhance policing capacity, especially between nations. As one practitioner observed:

> The most important need in the battle against cyber-crime is to develop close cooperation and personal relationships among law enforcement agencies and technical experts around the world ... A custom-made liaison mechanism is needed ... a mechanism by which countries can investigate offences and obtain evidence quickly and efficiently, or at least not lose important evidence in cross-border law-enforcement.[40]

An underlying concern among many observers is the effect of 'crime displacement', that is, as some jurisdictions effectively enforce laws, criminal activities will shift to jurisdictions of low capability — the vulnerable 'weakest link'. Comity thus can only be assured if wealthy states and affected industries are prepared to extend aid to those states or agencies less capable. If a single theme emerges as dominant, then the role of mutual legal assistance in developing universal or global measures to suppress computer-related crime is perhaps the most evident.

The capacities of the state are nevertheless limited, and constructive ways of mobilising private industry to help are necessary. The nature of the public–private interface must be flexible and responsive to the changing environment. Effective cooperation ultimately relies on shared objectives and the benevolence of all parties. A frequently cited need is for the education and training of law enforcement personnel, including prosecutors and judges. Considerable deficits characterise the technical and computing capacities of police and others, and it is often difficult to retain trained agents. A critical factor is the need to cultivate multidisciplinary approaches that require a broader educational preparation than previously necessary. Education, that all-purpose solution for technical and social ills, however, had not been developed or effectively targeted in respect to 'high-tech' crime, and long-term shortages in the relevant skills might have been foreseen. Support for specialised education within law enforcement agencies, and more generally in the public higher education system, is urgently required. This is one ready avenue by which the private and state sector might effectively contribute to long-term solutions to the numerous problems arising from the criminal exploitation of Internet and information technology.

Conclusion

With properly funded international law enforcement agencies, established mechanisms for common threat assessments and joint intelligence, more comprehensive forms of mutual legal assistance might be effectively activated. Many commentators express concern about the failure to address the 'weakest links' in the supposedly seamless security chain necessary to prevent and reduce serious criminal groups. Short and long-term policing assistance, sensitively deployed via regional security coordination, can give enormous help to vulnerable developing countries, countries in transition and those traumatised by conflict.[41] To help train, specialise and equip the law enforcers of these at-risk states will benefit them, their communities and all of us. The remarkable effects on morale that are produced by sound leadership, adequate equipment, best practices and practical training should not be underestimated. Some law enforcement agencies in the Asian region are critically short of specialised personnel in the forensic sciences, ICT, law, accounting and investigations, crime prevention and intelligence analysis. In addition, basic training is often rudimentary and leadership (command and control) training limited or military in nature. Endless lists of shortages in materiel are evident, from the most basic items such as radios and vehicles, mortuaries and armouries to the more advanced such as comparison microscopes or advanced electronics and decryption.

A number of policy and programme initiatives are suggested, from increasing regional-level coordination and cross-jurisdictional exchanges in personnel, intelligence and training to the creation of joint task forces and other operational collaborations. Many of these are already taking place and need to be expanded as rapidly as possible while continuing to evolve common methods among stronger and wider law enforcement networks. The technically advanced, highly capable policing agencies must provide more direct and strategically relevant assistance to hard-pressed neighbours; they must be triggered not by particular cases but by the mutual benefits of long-term collaboration. They must focus this 'police aid' on the priorities of the evolving regional and international security entities and by systematically undertaking the essential preparatory work in the field.

Despite the muscular image of police, much of modern policing revolves around the intelligent management of information. Police are now 'knowledge' rather than 'craft' workers and this is increasingly so as the full impact of the 'information age' is realised. High-order research and analytical skills and communication skills are increasingly needed along with traditional skills and discipline. Shortages in specialities such as forensic computing, law and

accounting, as well as statistical evaluations and communications, are now widely encountered. Training and retaining agents will be a major challenge, and reliance on in-house or short-term training will no longer serve the need for professionalism and continuous learning. There are an estimated 5 million police officers in Asia; around 5% of these are graduates but many are barely literate. If we are to address the myriad problems faced by modern policing and invest in prevention and intelligence, then due recognition must be given to investment in knowledge and the research that feeds it.

In conclusion, controlling crime involving digital technology and computer networks will require a variety of new networks: networks between police and other agencies within government, networks between police and private institutions, and networks of police across national borders. Over the past five years, considerable progress has been made within and between nations to develop the capacity of police to respond to cyber-crime. But the pace of technological change will continue unabated, and the adaptability of cyber-criminals will continue to pose challenges for law enforcement. The extent of transnational law enforcement cooperation achieved thus far, laudable though it may be, can only be regarded as a beginning.

Notes

Chapter 1

1. Victor Lo (Hong Kong Police) noted at the First Asia Cybercrime Summit (April 2001) that about 75% of cases in Hong Kong involved hacking and that this was about showing off and testing IT security rather than the pursuit of criminal enterprise. He and other discussants felt this would change as the opportunities presented by computer-related crime attracted innovative criminals.
2. For example, Hong Kong has an estimated 3.2 million residents on-line and is served by 56 ISPs. European Union computer-related crime trends also show that reported attacks on computer systems grew from approximately 1400 incidents in 1997 to just under 2500 cases in 1999. Similar increases have been observed for counterfeiting offences but computer fraud declined from 3000 cases in 1998 to 2250 cases in 1999, while computer assisted telephone service theft declined from over 7000 in 1997 to 4200 cases in 1999 — a trend also noted for recent Hong Kong data on computer crimes (Valeri 2001).
3. Figures cited from a 'Country Report' provided for the UN ESCAP Asia Pacific Conference on Cybercrime and Information Security, Seoul, 11–13, November 2002.
4. See www.police.go.th/crimewebpost/report/sum.php and summary country report by Surangkana Kaewjumnog, National Science Technology Development Agency, Asia Pacific Conference on Cybercrime and Information Security, Seoul, 11–13, November 2002. In 2001 there were about 3.5 million users and over 10 500 websites in Thailand and the number of users was expected to double by the close of 2002.
5. The new computer crime law is anticipated to take effect in late 2004 (personal

communication Ms. Surangkana Wayuparb, National Electronics and Computer Technology Centre, Ministry of Science and Technology) but as noted by Police Colonel Naras Savestanan (personal communication) the extent to which general police, as distinct from the small specialist unit already established, were equipped to handle computer-related crime remained a very significant challenge.

6. Comments by A M Natsir Amal, Ministry of Communication and Information, Republic of Indonesia, Asia Pacific Conference on Cybercrime and Information Security, Seoul, 11–13 November 2002.
7. Comments by Armi Jane R Borje, Commissioner, Philippines, National Telecommunications Commission at the Asia Pacific Conference on Cybercrime and Information Security, Seoul, 11–13, November 2002.
8. The TOC Convention came into force in September, 2003 (141 States and 16 parties have signed): see www.undcp.org/crime_cicp_signatures_ convention. html. The protocols in respect to trafficking in humans, smuggling in migrants and the illicit manufacture and trafficking in firearms have thus far attracted respectively 105, 101 and 31 state signatories.
9. As of July 2004 the Cybercrime Convention come into force after the minimum 5 ratifications (three of whom are by Council of Europe member states). As at 27 July 2002, 37 states have signed the Convention (including non-Council member states: Canada, South Africa and Japan). The 'First Additional Protocol to the Convention on Cybercrime on the criminalisation of acts of a racist or xenophobic nature committed through computer systems' has been signed by 22 states and awaits the necessary ratification: see http://conventions.coe.int/treaty/EN/projets/cybercrime27.htm; visited 9 August 2004.
10. The term 'regulatory' means in this context a contractual basis for rules of conduct and performance in contrast to 'mental intent' criminal laws and the associated higher thresholds of proof and reliance on custodial sanctions.
11. See for example the US Department of Justice (2000), 'Executive Order 13 133 Working Group on Unlawful Conduct on the Internet' — www.usdoj.gov:80/criminal/cybercrime/append.htm; European Council's treaty on cyber-crime (Csonka this volume and Csonka 1996) and the United Nations Secretary–General's 'Conclusions of the study on effective measures to prevent and control high-technology and computer-related crime'. For related analysis of the work of the European Union and the OECD see Valeri (2001).
12. UNAFEI, however, has activated training and related programmes. Further attention is likely and a number of states (for example, Singapore) and NGOs (for example, the Asian Development Bank and the Asian Crime Prevention Foundation) have promoted forums to raise awareness and improve cross-border cooperation on this issue.
13. Hong Kong is Vice-Chair of the UN group and participates in the NPA network: personal communication, Mr Victor Lo, Hong Kong Police
14. The Hong Kong Department of Justice established a dedicated mutual legal assistance unit in 1998. Five MLAT are in force and a further ten are under

consideration, although assistance to non-treaty jurisdictions can be offered subject to appropriate reciprocity. Hong Kong has 12 extradition agreements of which nine are in force and can cover computer offences. As noted by many commentators, formal channels are usually too slow to be effective and the authentication of evidence collected in other jurisdictions remains a problem.

15. For a cooler assessment of the European Union's efforts against organised crime: see Den Boer (2001). Despite the 1997 *Action Plan to Combat Organised Crime* (OJ 97/C 251/1) adopted by the Ministers for Justice and Home Affairs during the Dutch Presidency, differences between the policing institutions remain considerable. However, increased transparency and knowledge about one another's systems and recognition of the problem has led to re-organisation, improved resources and greater centralisation designed to improve cooperation amongst member states.
16. ASEAN comprises the following ten nations: Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, Myanmar and Vietnam: its meetings, coupled with the overlap among the 21 nations of the APEC forum, may yet hold out prospects for the development of a suitable mechanism for law enforcement coordination in the Asia Pacific region despite the primary focus on trade. In addition, Interpol regional meetings are held annually. The most recent, the 17th Asian Regional Conference, was held in Colombo in February 2002 and focused on terrorism.
17. The ACCORD followed the formalisation of the ad hoc meeting of the Special Senior Officials Meeting on Transnational Crime in Yangon (October 2000). Note also the increasing institutionalisation of cross-border cooperation on migration via the ASEAN Plan of Action on Immigration Matters.
18. China's largest portal Sina.com claims to be the world's fifth largest holder of e-mail accounts, with the 25 million-odd accounts, out of and estimated 570 million worldwide, ranking it the largest server of non-English e-mailers.
19. China now has about 50 million Internet users, ten backbone networks and 3 600 ISPs / ICPs. Although estimates of the numbers of Internet subscribers are difficult to verify, estimates placed the number around 33 million at the end of 2002 (MFC Internet Update 2002: www.mfcinsight.com, December). China's Internet population growth has been hampered by insufficient bandwidth and relatively expensive by-the-minute charges but this is expected to diminish as wireless applications and compression technologies become available.
20. PRC users are currently reported to spend an average 11 hours online a week: 40% on 'cultural activities': news, sports, movies and TV, IT, finance and literature and 60% on email and shopping. Nearly a third (32%) of users purchased goods / services online (source: PRC Ministry of Information Industry Vice-Minister Zhang Chunjiang: China Network Civilization Project Organizing Committee).
21. According to a CNNIC survey in 2001, 31.9% of the then 26.5 million net users purchased goods online in the previous year. Most Internet users are aged 20–30

years, and their payment ability is limited. Moreover, most surveyed Internet users were unsure if B2C would develop in the next two years. The CNNI report also noted that about two thirds of China's users, about 8 million people, are willing to try online shopping.

22. The PRC has launched a secure online financial services / e-commerce infrastructure run by the China Financial Certification Authority (CFCA). The CFCA issued more than 100 000 digital certificates in 2002 to corporate banking customers and Chinese stock traders.
23. Beijing's municipal Education Commission discovered through its survey that 20% of the city's secondary students primarily search out porn when surfing.
24. Philippe Bertrand (Visa Fraud Control, Asia-Pacific) reported that 400 cases of credit card fraud were noted in 2000 by Visa but difficulties of prosecution meant that only a fraction of cases went to court (cited in Broadhurst 2001).
25. Chinese Internet user profiles are similar to those found elsewhere in that professional, younger and urban populations are predominant. Many (30%) users have post-college level education, and half (49%) work in white-collar jobs. They typically use the Net to send and receive e-mail, chat, and seek information about health, community and education, and when shopping they normally buy theatre tickets, travel tickets, DVDs and VCDs. The Chinese Academy of Social Science's Social Development Research Center reported that China's Internet users average 27 years in age, 65% began surfing in 1999, 61% are male, 43% are students, 16% are managers, and 11% are science, education, culture or health workers.
26. Hui recommends developing hacking tools as a means to learn about them and staging 'laboratory' cyber attacks to help train investigators. Simple techniques such as creating document registries based on 'flags' (via # hash functions) help monitor intrusions and hacking.
27. The importance of the preservation of evidence and its connection with the need for harmonised procedures and laws is also necessary; see the guide from the USA National Institute of Justice designed to assist law enforcement and others who are responsible for protecting an electronic crime scene. 'Electronic Crime Scene Investigation: A Guide for First Responders' (NCJ 187736) at http://www.ncjrs.org/txtfiles1/nij/187736.txt.
28. Broadhurst (2001) reported Robert Yule's (IFPI) observation that there were an estimated 1.9 billion pirated units in circulation (DVD / CD, Internet and cassettes) worldwide. The introduction of recordable CDs / DVDs also facilitated the downloading of an estimated 25 million music files from the Internet. He also noted growing evidence that organised crime had moved into the production and distribution of pirated CDs.
29. Other examples include interpol's directory on art theft.
30. It took ten years to develop the Interpol credit card fraud classification scheme.
31. For the past three years, a specialised IP court in Thailand heard 3000 cases in which 98% of the accused pleaded guilty due to the emphasis placed on plea-

bargaining by the court in securing convictions. The Thai approach was to avoid tough penalties because higher penalties could encourage corruption of police (Mr Weerawit Weeraworawit Intellectual Property Department, Thailand cited in Broadhurst 2001)

32. Copyright holders, usually through industry bodies now directly invest in crime prevention and prosecutions. For example, Michael Ellis of the Motion Picture Association reported that they have helped in the past few years investigate and assist in some 4000 prosecutions of copyright violations in the Asian region.
33. Notably the Thai and Malaysia governments have actively encouraged IP industries especially in music products to reduce prices and co-operate more actively in promoting awareness of the costs of piracy on state and private revenue.
34. Internet piracy is not apparently clearly covered by PRC laws for distributed pirated works — although the view was expressed that a judicial interpretation has been issued for civil law breaches on the Internet.
35. The introduction of cyber-codes or unique identifiers for optical discs had been helpful in tracking factory sources but they also have been copied.
36. The Royal Malaysia Police (Mr Mohd Nawawi Ismail) noted that the *Copyright Act 1987* was ineffective and the recently passed *Optical Disk Act 2000* has yet to be fully assessed as operations had only been initiated from March 2001.
37. Personal communication Mr Mark Day and see: The Motion Picture Association Announces Expeditious Resolution of Two Landmark Civil Action Proceedings Concerning DVD Piracy in China (Encino, CA / Hong Kong) and, Motion Picture Association Announces the Successful Resolution of Six Civil Action Proceedings Concerning DVD Piracy in Shanghai (Encino, CA / Hong Kong).
38. Approximately 30 nations have passed specific laws criminalising computer-related crime. However, a large number have such laws in development or in process. Details of the relevant laws applicable for jurisdictions in the Asian region are reported by Urbas in this volume.
39. Summary drawn from remarks made by Mr R Sri Kumar, IPS, Inspector General of Police. India at the Asia Cybercrime Summit, April 2001, Hong Kong.
40. Comments of Victor Lo: Roundtable: Regional Law Enforcement Co-operation, Asia Cybercrime Summit, April 2001, Hong Kong.
41. There is an important role for professional associations and business corporations to play in fostering business ethics and contributing financial and other resources to public police, notably in the field of training. Many examples of effective partnerships between public police and private security occur; however, the form of assistance is often limited by commercial self-interest. The payment card industry's crucial contribution to Interpol's Universal Classification System for Counterfeit Payment Cards and their routine support in operational, training and computer support for public agencies is a good example.

Index

Access, *see* illegal access
access codes, 254
Act on International Judicial Mutual Assistance in Criminal Matters (Republic of Korea), 392n4
Act on Mutual Assistance in Criminal Matters (Thailand), 392n4
Adult Site Against Child Pornography, 99
Aiziwa, Keiichi, 13
Allan v UK (2003), 382n78
ancillary liability, 227, 265, 270–1, 312
'Anna Kournikova' virus, 37
Annual Senior Officials Meeting on Transnational Crime, 14
ASEAN, 13, 14, 287–9, 340
ASEAN and China Cooperative Operations in Response to Dangerous Drugs (ACCORD), 14
Asia Cyber Crime Summits, xi, 357
Asia Pacific Computer Emergency Response Teams (APCERT) Forum, 131
Asia-Pacific Economic Cooperation Forum (APEC), 13, 177, 277, 293–5, 302
Asia/Pacific Group on Money Laundering (APG), 292
Asia-Pacific region, 31, 337
  cyber-crime legislation in, 216–27
Asia-South Pacific Working Party on Information Technology Crime, 292
asset confiscation, handbook on, 393n18
Association of South East Asian Nations, *see* ASEAN
asymmetric warfare, 330–1
Aum Shinri Kyo (cult), 6, 110–1
Australia, 335
  cyber-crime legislation, 146–54
  offence provisions in, 216–8, 231

Basic Law [of the Hong Kong Special Administrative Region] (PRC), 247, 253
biometric security devices, 49, 355
Birth and Deaths Registration Ordinance (Cap. 174), 260
Boden case, Vitek, 335, 336
bookmaking, online, *see* gambling, online
Bowden (2000), 262
Broadhurst, Roderic, xv

Bronitt, Simon, xvi, 354
Budapest Convention, *see* Convention on Cyber-crime
'buffer attack', 199
Bullwinkel, Jeffrey G, xvi–xvii, 13, 348, 349, 351
Burma, *see* Myanmar
Business-Government Task Force on Critical Infrastructure (Australia), 335
Business Registration Ordinance (Cap. 310), 246
Business Software Alliance, 229

Cambodia, 10, 16, 347
case studies, 350
  in cyber-security, 330–44
censorship, 76, 339
Central Bureau of Investigation (India), 227
Centre for Information Security and Cryptography (CISC), xvii
Centre for International Crime Prevention (CICP) (UN), 383–4
certification authorities, 128
Chan, H W, xvii
Chan Keen Wai, xvii, 7
Chernobyl virus, 342, 344
Cheung, Venus L S, xvii
child pornography, 6, 33, 49, 317–8, 340
  laws relating to, 221, 227, 244, 260–2
China Internet Network Information Centre (CNNIC), survey, 83
China, People's Republic of, 19, 102, 330, 333
  cyber-attacks by, 334
  cyber-crime in, 8, 61–4
  governance of cyberspace, 57, 64–78
  information technology, development, 58, 64
  Internet
    control of, 77, 218–9, 340
    development, 58–61
    government concerns, 59–61
    users, 31, 80, 363n18, 364n24
    offence provisions, 218–9, 232
    penalties, 341
    piracy, 23
  virus damage to, 342
  websites, 80
Chinese characters, encoding, 385n2–3
Chinese Communist Party (CCP)
  Internet access a threat to, 64–5, 76–7
Chinese, *see* Hong Kong Chinese
Chiu, Ivan S K, xvii, 16, 351
Chong, C F, xvii
Chow, K P, xvii
circumvention, of technological protection measures, 240
Civil Procedure Law (PRC), 392n4
Clarke, Ron, 3
'Code Red' worm, 18
Cohen, Stanley, 118
comity, between states, 25
Commission on Narcotic Drugs (CND), 394n20
Commonwealth, State and Territories Agreement on Terrorism and Transnational Crime (2002) (Australia), 165
Communication Assistance for Law Enforcement Act 1994 (USA), 375n15
compensation (*see also* restitution), 194, 195–6, 226, 228
competency, in information technology, 134
'computer', lack of statutory definition of, 246
Computer Crime Act (Japan), 388n42
Computer Crimes Act 1997 (Malaysia), 223, 388n45
Computer Crimes Ordinance (No.23 or 1993), 97, 244, 245, 246, 251, 256, 258
computer data, stored
  access to, 282

preservation of, 278, 321
seizure of, 322–3
computer data, trafficking in, 254
computer emergency response teams (CERTs), 4, 131, 245
Computer Forensic Examination Working Group, 245
computer forensics, 5, 23, 26, 101
computer management, 73–4
Computer Misuse (Amendment) Act 2003 (Singapore), 129
Computer Misuse Act (CMA) (Singapore), 38, 129, 225
Computer Misuse Act 1990 (UK), 244, 257
computer networks
police, 27
protection of, 210, 304–5
'wiretapping', 244
Computer Processing Personal Information Protection Law (Taiwan), 228
Computer Program Protection Act (Republic of Korea), 239
computer programs, 212, 213, 315
computer-related crime, *see* cyber-crime
Computer-related Crime: Analysis of Legal Policy (OECD), 213–4
computer security, *see* cyber-security
Computer Security Institute (USA), 44
computer software, 239
piracy, 229, 230 (table 12.13), 233, 239
computer systems
access to, for dishonest purpose, 223
damage to, 223
interference, 315
integrity of, 149, 154, 163
search of, 322
computer-warfare, 330
computers, misuse, 143–4, 252
connectivity, 1, 2, 16, 347
Constitution (Australia), 145, 388n59, 387n29
Control of Obscene and Indecent Articles Ordinance (Cap. 390), 97
Convention Against Transnational Organised Crime (TOC Convention) (UN), 11–2, 214, 234–6, 345
Convention on Cyber-crime (Council of Europe), 12, 14, 53, 96, 157, 162, 215, 265, 349
Additional Protocol, 262
aims, 278, 304, 311
child pornography, 260
Council of Europe guidelines, basis for, 311
guidance model, 241, 213, 246, 326
offences to be criminalized, 270–1
origin of, 303
provisions, 228, 278, 319–24
ratification, 177, 214, 362n8
signatories, 115, 176, 192, 278–9, 301–2
structure, 312
Convention on Electronic Contracting (UNCITRAL), 129
copyright, 227, 263–5,
infringement, 19, 23, 231, 235, 236, 237, 270, 318
piracy, 230, 232, 233, 350
Copyright Act 1968 (Australia), 239, 240
Copyright Act (India), 233
Copyright Act 1987 (Malaysia), 365n36
Copyright (Amendment) Act 1997 (Malaysia), 240
Copyright Ordinance (Cap. 528), 97, 263–4
Copyright (Suspension of Amendments) Ordinance 2001 (Cap. 568), 389n64, 391n35
costs, 42–4, 46–7, 116, 121–2
charging compliance, 120–1
virus damage, 43, 208, 342, 343

Council of Europe (*see also* Convention on Cyber-crime), 13, 53, 277–8
guidelines on computer crime, 306–7, 310–1
counterfeiting, *see* forgery and counterfeiting
Cox v Riley (1986), 379n28
crackers and cracking (*see also* hackers and hacking), 198, 208, 224, 371n10
penalties, 228
perceptions of, 84
credit cards, 16, 40, 192, 364n30
crime control, theories, 118–9
crime displacement, 23, 25
crime prevention, strategies, 3
Crimes Act 1900 (ACT) (Australia), 379n33, 380n49
Crimes Act 1914 (Cwlth) (Australia), 146–8, 160, 216, 388n46
Crimes Act 1900 (NSW) (Australia), 379n33, 380n49
Crimes Act 1958 (Vic) (Australia), 377n6, 380n51, 380–1n62
Crimes Legislation Amendment Act 1989 (Cwlth) (Australia), 387n27
Crimes Legislation Amendment Act 2000 (NSW) (Australia), 380–1n62
Crimes Ordinance (Cap. 200), 97, 220, 247, 249, 252, 254–5, 257, 258, 265, 391n32
prosecutions under s.161, 245, 250–1, 255–6
Crimes (Overseas) Act 1964 (Cwlth) (Australia), 388n53
Crimes (Property Damage and Computer Offences) Act 2003 (Cwlth) (Australia), 387n30
Crimes (Property Damage and Computer Offences) Bill 2003 (Vic) (Australia), 377n6
criminal behaviour, theories, 3
Criminal Code Act 2002 (ACT) (Australia), 377n5, 380–1n62
Criminal Code Bill 2002 (ACT) (Australia), 377n5
Criminal Code (Cwlth) (Australia), 156, 159, 164, 388n52
Criminal Code (Tas) (Australia), 379n33
Criminal Code 1983 (NT) (Australia), 379n31
Criminal Code Act 1995(Cwlth) (Australia), 166–7, 387n28, 388n52
Criminal Code Amendment Act (No.3) 2001 (NT) (Australia), 377n7
criminal groups, 19
Criminal Investigation Department (CID) (Singapore), 132
Criminal Investigation (Extraterritorial Offences) Act 1987 (Cwlth) (Australia), 388n53
Criminal Jurisdiction Ordinance (Cap. 461), 252
Criminal Law (PRC), 61, 66–7, 68
Criminal Procedure Code (Japan), 111, 112
Criminal Procedure Ordinance (Cap. 221), 265
criminalisation
of computer crime, 10, 144–5
of offences, 296, 298, 299, 306
overcriminalisation, 149
criminality, forms of, 17–8
criminals, computer
rationalisations of, 30
motives, 29–30
cryptographic keys, disclosure, 10
cryptography (*see also* decryption, encryption), 355
Csonka, Peter, xvii–iii, 12, 349
cults, 6, 110
customer migration, 122
Customs Act 1901 (Cwlth) (Australia), 388n52
Customs and Excise Department (Hong Kong), 103, 245
Cyber Angels, 99

cyber-attacks (*see also* Moonlight Maze, Solar Sunrise), 38, 328, 329, 334
cyber-cafés, *see* Internet cafés
cyber-crime, 2, 4–10, 78, 93(table 5.1), 132, 349
  bogus news report as, 243
  control of, 46–7, 48–55
  criminality and, 2–4
  defined, 42, 57, 142, 197–8
  forms of, 31–41, 80–1, 170, 209–10
  losses from, 81
  nature of, 10, 270
  opportunities for, 30–1, 48–9
  policy on combating, 348
  prevention, 202–3
  public understanding of, 92
  research on, 63, 93, 133, 350, 351
  responses to, 17–8, 47, 92, 158–9, 353
  socio-economic impact of, 29–55
  typology, 17
Cyber-crime Act 2001 (Cwlth) (Australia), 141, 144, 145, 149, 160, 161, 163, 216, 381n71, 388n52
Cyber Crime Technology Information Network System, 13
'cyber-dissident', 370n58
'cyber-ethics', 75
cyber-harassment, 192
cyber-security, 1–2, 143, 336, 345
  case studies, 330–44
  people as threat to, 73
  products and services, 137–9
    in Singapore, 126–40
cyberspace, 50, 341, 346
  governance of, 64–78, 355
  threats from, 341–2, 344, 345–6
cyber-stalking, 35, 144, 192
cyber-terrorism, 172, 173, 175–6, 192
  guidelines on countering, 290
Cyber vigilantes, 99

Daewoo Securities, 335
damage, criminal, 254–6
damages, *see* compensation
data, alteration of, 221
data interference, 314–5
'data mining', 45
data protection, 130, 389n4
data retention, costs of, 116
data storage, 32–3
decryption, 129
Delta Information and Communications, 335
'denial of service' attacks, 20, 37, 43, 147, 305,
digital control systems, vulnerability of, 336
digital divide, 16, 347, 350
Digital Evidence Search Kit (DESK), 18, 205, 206, 355
digital signatures, 188, 203, 220
digital technology, 1
  criminal activity facilitated by, 17, 19, 34
  organised crime and, 19–20
digital video disks, *see* optical disks
DiGregory, Kevin, 307
disaster recovery, 131
displacement, of cyber-crime, 23, 25
domain names, registration, 58, 69
dot.com stocks, 90
drug control, 14, 282, 394n20
Duggal, Pavan, xvii, 349

e-business, *see* e-commerce
e-commerce, 1, 16, 127–8, 220, 224, 351
  in China, 77, 80, 86–7, 88
  confidence in, promotion of, 130, 135
  defined, 79
  in Hong Kong, 90, 96
  revenue, 31
  risks to, 81–2, 87
education (*see also* public awareness), 127, 203, 280, 297, 299, 301
  about 'high-tech' crime, 25, 72–3, 245, 266

e-government, 58–9
electronic eavesdropping, 45
Electronic Commerce Act (Philippines), 9, 228, 236, 388n41, 388n44
Electronic Commerce Steering Group (ECSG) (APEC), 294, 302
electronic funds transfer, 40–1
'electronic heroin', 369n42
electronic impersonation, 41
electronic records, 128, 129, 258, 259–60
  defined, 259
electronic signatures, 128
Electronic Transactions Act (BE 2544) (Thailand), 9
Electronic Transactions Act (Singapore), 127–8
Electronic Transactions (CA) Regulations (Singapore), 128
Electronic Transactions Ordinance (Cap. 558), 97, 246, 259–60
e-mail, 46, 76, 114, 340
emergency systems, 131, 133
encryption, 85, 130, 204(fig 11.3), 228, 266, 351
  technology, 33, 41, 290
EPA v Caltex (1993), 362n79
espionage, computer, 212
European Convention on Human Rights, 320
European Police Office (Europol), 14, 289
European Telecommunications Standards Institute (ETSI), 115
European Union (EU), 4, 14, 95, 96, 289
evidence, electronic, 312
  collection and exchange of, 309
  preservation, 18, 20, 272, 309–10, 319
  vulnerability of, 307
Evidence Act (India), 220
Evidence Act (Singapore), 129–30
Evidence Ordinance (Cap. 8), 246
extortion, 36
extradition, 52, 285–6, 297, 298, 300
Extradition Act 1988 (Cwlth) (Australia), 388n53, 392n4
Extradition Act (India), 392n4
Extradition Act (Malaysia), 392n4
Extradition Act (New Zealand), 392n4
Extradition Act (Republic of Korea), 392n4
Extradition Act (Thailand), 392n4
Extradition Law (PRC), 392n4
extradition regimes, 280
extradition treaties, 274, 275

false accounting, 258
Falun Gong movement, 38, 60, 61, 76
Federal Bureau of Investigation (FBI), 20, 21, 337
Felson, Marcus, 3
filtering
  Internet content, 339, 340
  software, 354
  technology, 356
Financial Action Task Force (FATF), 290, 292, 345
forensic computing, 18
  expertise required, 356, 357
forfeiture, of equipment, 228
forgery and counterfeiting, 19, 20, 34, 226–7, 257
  computer-related, 211–2, 316–7
Forgery and Counterfeiting Act (UK), 257
fraud, 226
  computer-related, 211, 257–8, 316–7
  Internet, 6, 16, 102, 104
  investment, 39
  online trading, 335–6
  sales, 39
freedom of expression, 340

Gambling Ordinance (Cap. 148), 97, 263
gambling, online, 263
Gani, Miriam, xvii, 354
Garland, David, 118, 119
Ghosh test, 250

globalisation, 10, 11
threats from, 329
Golden Projects, in China, 58
government agencies, coordination, 332
governments, interface with citizens, 339
Grabosky, Peter, xv–xvi, 17
Group of Eight (G8), 53, 192, 214, 281–2, 303, 325
G 8 Senior Experts Group on Transnational Organised Crime, *see* Lyon Group
Guidelines for the Security of Information Systems and Networks (OECD), 214
Guzman, Onel de, 350

hackers and hacking, 146, 221, 338, 361n1
attacks, 32, 38, 40, 81, 331, 334, 335
behaviour, 80
defined, 198, 371n10
guidelines on countering, 290
offence, 186, 190, 191, 208, 248, 314
penalties, 224, 228
perceptions of, 84
techniques, 199
tools, 364n25
hash values, 205
Heaney v Ireland (2000), 382n79
HKSAR v Chan Chi Kong (1997), 255
HKSAR v Choy yau Pun (2002), 390n19, 390n21
HKSAR v Ko Kam Fai (2001), 255–6
HKSAR v Tam Hei Lun (2000), 251, 255
HKSAR v Tong Ka Kin (1996), 250
HKSAR v Tsun Shi Lun (1999), 250–1
homeland security, 133
Hong Kong, 90–1, 243
displacement of intellectual property pirates, 23
as economic city, 89–90
computer-related crime, 6(table 1.1), 93(table 5.1), 200(tables 11.1–2), 201(table 11.3)
governance, 94–5
electronic, 95–8
Internet, 105–6
legislative framework, 96–8, 244, 246–65
offence provision, 220, 233
response to cyber-crime, 92, 246
Hong Kong Chinese, ethos of, 91–2, 99–100
Hong Kong Computer Emergency Response Team Coordination Centre, 103, 105
Hong Kong Police, 18, 103, 245
Computer Forensics Laboratory, 5
Computer Security Unit, 227
Organised Crime and Triad Bureau, 19
partnership with university, 355
Technology Crimes Division, 5, 101
Hong Kong Telecoms Users Group, 99
Hui, Lucas, xvii, 18
human rights, 320
human security
concept, 328
model, 347
relevance to cyberspace, 329
Hung Hak Sing (1995), 250
Hynds, Len, 21

'I Love You' virus, 9, 18, 305, 306, 344, 350
impact of, 37, 43–4, 207–8, 342–3
identification, of cyber-criminals, 308
identity,
concealment and detection of, 41
data, 117
illegal access (*see also* crackers and cracking, hackers and hacking), 148, 212, 221, 249, 251, 313–4
offence provisions, 247–52
Immigration Department (Hong Kong), 103
incident response teams, 131

Independent Commission Against Corruption (ICAC), 103, 245
India, 24, 227
  Internet use, 183–5
  legislation, 186–96
  offence provisions, 220–1, 233–4
Indian Penal Code, 220
  offences under, 186–9
Indonesia, 9
Info-communications Development Authority (IDA) (Singapore), 7, 126, 128, 130, 136, 338
information and communications technology, 10
  companies, Singapore, 137–9
  control of cyber-crime through, 22, 74
  convergence, 1, 30, 323
  impact, 269
  public awareness, 133–4
information security, 1–2
information sharing, 273
'information system', defined, 246–7
information systems, 32–3
Information Technology Act 2000 (India), 24, 186, 189–96 *passim*, 220, 227, 388n43
Information Technology Standards Committee (Singapore), 134–5
information warfare, 38
infrastructure, *see* national infrastructure
Inland Revenue Ordinance (Cap. 112), 246
Inoue, Masahito, 120
'inspection', substituted for interception, 111
intellectual property
  infringement, 318
  international agreements, 240
  offence provisions, 231–9
  overlap with computer crime, 228–9
  piracy, 22–3
  protection of, 22–4, 69–71
Intellectual Property Court (Thailand), 238
Intellectual Property Crime Action Group, 293
Intellectual Property (Miscellaneous Amendments) Ordinance, 389n64, 391n35
Intellectual Property Rights Working Group (IPEG) (APEC), 294
intercepted material, 253
interception
  of electronic communications, 44–5, 252
  illegal, 212, 314,
  inspection substituted for, 111
  real-time, of content data, 323
interception of telecommunications, 39–40, 111–3, 115
Interception of Telecommunications Ordinance (Cap. 532), 247, 252–3, 389n7
Inter-Departmental Working Group on Computer-Related Crime (Hong Kong), 54, 245, 246, 247, 248, 258, 266, 267, 268
international cooperation, 52–3, 176, 324–6, 351
  challenges to, 271–2
  existing mechanisms for, 272–95
  legal aspects of cyber-crime, 213–5
  need for, 269
  trust as factor in, 333
International Chambers of Commerce (ICC), 44
International Consumer Protection and Enforcement Network, 349
International Covenant on Civil and Political Rights (ICCPR), 320
International Criminal Police Organisation, *see* Interpol
International Federation of Phonographic Industries, 229

international instruments, limited reach of, 11
International Intellectual Property Alliance (IIPA), 230
International Telecommunications Union (ITU), 115
International Telecommunications Union for Asia and the Pacific, 340
'International User Requirements', for telecoms policing, 115
Internet, 16, 79, 327, 338
  adverse impacts by, 369n42
  control of content and access, 65, 67–8, 77, 218–9, 339, 340, 354
  content rating system, 341
  corrupting influence of, 75–6
  development, 58–61
  governance, 95–6, 105–6
  hotline, 9
  inappropriate use, penalties, 341
  policing, 98–104, 106
  security, 60–1, 68–9
    as term, use of, 386n8
  use of, 31, 183–5
  users, 8, 9, 15, 59, 80, 98–100, 170, 363n18
    profiles, 364n24
  vulnerability, 330
Internet banking, 37, 130
Internet cafés, 8, 47, 72
Internet fraud, 6, 16, 102, 104
Internet Fraud Complaint Center (USA), 17
Internet Police (PRC), 71
Internet Service Provider Association, 100
Internet Service Providers (ISPs), 47, 100–1, 130, 266
  retention of transaction data, 357
Internet Watch Foundation, 101
Interpol, 17, 20–1, 292–3, 349, 365n41
investigations, 132, 278, 326
  inadequate procedures, 309
  studies of, 350–1
investigators
  need for specialist, 194
  retention of, 53
investment fraud, 39
IT, *see* information and communication technology
IT Basic Law (Japan), 172, 177

Jackson, Michael, xvii, 14
JANET-CERT, 103
Japan, 111–3, 116–22, 227, 353
  cyber-crime, 6–7, 171(table 9.1), 172–6
  offence provisions, 221, 222(table 12.5), 234
Japanese Interception Law, 112, 375n32
Jiang Ping, 63
Jiang Zemin, 58
journalism, market driven, 91
jurisdiction, 145
  conflict over, 271
  as issue in control of cyber-crime, 51–2, 154–8
  reforms, 157–8
Justice, Department of (Hong Kong), 245

Kaspersen, Professor Henrik W K, 307
Kazakhstan, 10
keyword filtering, 340
Khan v UK (2000), 382n76
Klass v Germany (1978), 382n76
Korean Information and Security Agency (KISA), 7
Korea, Republic of, 227, 335–6, 337, 341, 393n6
  cyber-crime, 7–8
  offence provisions, 221, 222(table 12.6), 235
  virus damage to, 342
Kuan Hsin-Chi, 99

Laos, 10, 16, 35, 347
Lau, Laurie, xix, 354, 355

Lau Sai Kai, 91, 99
Lau, Stephen, 97
Laurence Godfrey v Demon Internet Ltd, 101
law enforcement, 2, 14, 287–8
  at disadvantage, 12
  cyber-crime as core business of, 17
  extraterritorial, 51
  traditional methods, inadequacy of, 20
law enforcement agencies (*see also* private police and policing), 71–2, 104, 193–4, 245
  capacity, 24–5, 26, 53–4, 272, 307, 308
  collaboration with universities, 355
  computer crime units, 5, 101, 227
  cooperation between, 285, 296, 298, 300
  cooperation with private sector, 21, 245, 266, 365n41
  information sharing, 273
  networks, 27
  powers, 160–3
  strengthening, 26–7
  transnational policing, 10–3
Law for International Assistance in Investigation (Japan), 392n4
Law for Judicial Assistance to Foreign Courts (Japan), 392n4
Law of the People's Republic of China on the Preservation of State Secrets, 68
laws, *see* legislation, regulations
legislation, 8, 9, 24–, 50–1, 211, 228–9, 241
  Asia-Pacific, 216–27
  Australia, 146–54
  domestic, 274–5, 304
  gaps in, 244, 295,
  harmonisation, 14, 53, 141, 344
  Hong Kong, 96–8, 244, 246–65
  inadequacy of existing, 146, 208–9, 210–1, 306
  India, 186–96, 220–1, 233–4
  Japan, 174–5, 178–81
  reform, 213, 280
  Singapore, 127–30, 225
  Thailand, 9, 226
Leong, Clement, 7
Leung, Elsie, 246
Li Lanqing, 72
Li Man Wai v Secretary for Justice (2003), 251, 390n18
Li, Richard, 90
Lin Hai, 370n58
Linux, products, 82
Linux User Group, 99
Lipohar v The Queen (1999), 155, 380n52, 380n54
log inspections, 204
log records, 266, 308
losses, 43, 81, 230, 230(table 12.13)
Love Bug, *see* 'I Love You' virus
Luo Yongzhong, 341
Lyon Group, 279–81, 288, 289, 393n18

MacLeod v Attorney-General (NSW) (1891), 380n44
Mafiaboy case, 20
Malaysia
  displacement of intellectual property pirates, 23
  offence provisions, 223, 227, 235
Manning, Peter, 119
Manual on the Prevention and Control of Computer-Related Crime (UN), 214
manuals, computer crime, 292, 394n21
market forces, 49, 356
Measures to Combat Serious and Organised Crime Act (Cwlth) (Australia), 163
media, in Hong Kong, 90–1
'Melissa' virus, 43
Microsoft Corporation, 22, 40, 82, 354
  action against software piracy, 239, 355
misuse, of devices, 315–6
Mitnick, Kevin, 41

mobile phones, 113, 117
Model Criminal Code (Australia), 142
Model Criminal Code Officers Committee (MCCOC) (Australia), 141, 154, 157, 159
Model Data Protection Code (Singapore), 130–1
Model Law on Electronic Commerce (UNCITRAL), 128, 189
Monetary Authority of Singapore (MAS), 130
money laundering, 10, 36–7, 228, 290–2
Mongolia, 10, 347
Moonlight Maze, cyber-attack, 331, 332, 333
Motion Picture Association of America (MPA), 24, 159
motives, computer criminals, 29–30, 48
multilateralism, 277
multilateral relationships, 351
music piracy, 229
mutual legal assistance (MLA), 13, 14, 228, 272, 285, 312
  bilateral
    agreements, 275, 280
    treaties, 276–7
  elements of, 297, 298, 300
  importance, 25, 274
  lack of systematic evaluation, 358
  new regimes required, 308–9
  obstacles to, 306
  traditional mechanisms, 272
Mutual Assistance in Criminal Matters Act 1987 (Cwlth) (Australia), 388n53, 392n4
Mutual Assistance in Criminal Matters Act (1992) (New Zealand), 392n4
Mutual Assistance in Criminal Matters Act (Singapore), 392n4
Mutual Assistance in Criminal Matters Ordinance, 392n4
Myanmar, 10, 16, 341, 347

National Bureau of Investigation (Philippines), 10
National Crime Squad (UK), 104
National Criminal Intelligence Service (NCIS) (UK), 104
National Electronic Computer Technology Centre (Thailand), 9
National Emergency System (Singapore), 133
National High Tech Crime Unit (UK), 17, 21, 104
National Incident Response Team (Japan), 173
National Infocomm Competency Centre (NICC) (Singapore), 134
national infrastructure
  privatisation, 354
  protection, 332, 334, 335
  security threats to, 133
National Infrastructure Protection Center (FBI), 331, 332, 334
National Internet Advisory Committee (Singapore), 130
National Police Agency (NPA) (Japan), 6, 13, 170, 227
National Police Agency (Republic of Korea), 227
National Trust Council (NTC) (Singapore), 135
National Trust Mark Programme, 135, 136
networks, *see* computer networks
New Dimensions of Human Security (UN), 328
New Zealand
  offence provisions, 223, 224(table 12.8), 236
Nguyen Vu Binh, 341
North Korea, 10, 347

obscene publications, 187, 220
offences, 154, 323–4
  adaption of traditional, to cyber-crime, 145–6

categories, 312, 313–8
circumvention of technical protection measures, 240
criminalisation of, 270–1, 296, 298, 299
failure to criminalise, 306
lack of, 208
'minimum list' of, 211–3
provisions for
Asia-Pacific, 216–27
Australia, 150(table 8.1), 151–3(table 8.2)
India, 186–9
Singapore, 132(table 7.1)
offenders, 63–4
profiling, 3
offensive materials, 34–5
Office of Drug Control and Crime Prevention (UN), 282
online auctions, 39, 116
online merchants, 136
online trading, 86–7, 363n20
online share trading, 335–6, 337–8
Operation Bucaneer, piracy investigation, 350
Optical Disk Act 2000 (Malaysia), 365n36
Optical Disk Bill 2000 (Malaysia), 240
optical disks, 264–5, 365n35
piracy, 23, 24, 34, 239–40
Organisation for Economic Cooperation and Development (OECD), 53, 290
organised crime, 19, 110, 215, 227–8
Organised Crime Ordinance, 22
Osama bin Laden, 32
Oxford v Moss (1978), 379n25

Pacific Century CyberWorks (PCCW), 90
paedophilia (*see also* child pornography), 104
Palermo Convention Against Transnational Organised Crime (UN), *see* Convention Against Transnational Organised Crime
passwords, 5, 254
Pavic v R; R v Swaffield (1998), 328n78
payment cards (*see also* credit cards), 9, 19
fraud, 293
classification scheme for counterfeit, 20–1, 365n41
Peking University, survey, 82–3
Penal Code (Law No. 45 of 1907) (Japan), 221, 383n7–384n12
penalties, 129
People's Republic of China, *see* China, People's Republic of
personal data, 117, 44, 45
Personal Data (Privacy) Ordinance (Cap. 468), 97
Philippines National Police, 10
Philippines, Republic of the, 9–10, 228, 343, 393n6, 393n9
laws, inadequate, 208–9, 350
offence provisions, 224, 236
piracy, 33–4, 43
computer software, 229, 230(table 12.13), 233
copyright, 230, 232, 233, 350
intellectual property, 22–3
music, 229
optical disk, 239–40
points of contact, 192, 278, 280
international network, 324–5
Police Cooperation Working Group (EU), 114–5
Police Force Ordinance (Cap. 232), 103
police and policing, *see* law enforcement agencies, private police and policing, telecoms policing
policy development, on cyber-crime, 348
evidence basis for, 350–4

pornography (*see also* child pornography), 100
Post Office Ordinance (Cap. 98), 252
Poulsen, Kevin, 40
Prevention of Child Pornography Ordinance (Cap. 579), 261–2, 389n6
Prevention of Copyright Piracy Ordinance (Cap. 544), 239–40, 263, 264–5
privacy, 16, 248, 314, 337
  threats to, 44–5
  standards, 135
Privacy Commissioner for Personal Data, 97
private police and policing, 12, 13, 101–2
  transnational, role for, 12
private sector, 336
  cooperation with law enforcement agencies, 21, 245, 266, 365n41
  difficulty in enlisting support of, 353
  involvement with public sector, 272, 297, 299, 301, 335, 356–9
  monitoring cyberspace, 49
  role in crime prevention, 159, 306, 355
  resources, 354
private security services, 104
privatisation, national infrastructure, 354
procedural powers, 319–24
  prevention of abuse of, 320
production orders, 321–2
productivity, losses in, 43, 45–6
profiling, 3, 364n24
prosecutions
  coordination of, inter-jurisdictional, 280
  cyber-crime, 250–1, 255–6, 265, 352
  public awareness, 134–4, 174
Public Key Infrastructure (PKI), 127, 128, 135
Public Key Infrastructure Forum (Singapore), 136
public sector
  involvement with private sector, 272, 297, 299, 301, 335, 356–9
  role in policy development, 266–7
Pun, K H, xvii

Quarantine and Prevention of Disease Ordinance (Cap. 141), 389n3
Qu'ran, as basis for content filtering, 340

R v Gold, R v Schifreen (1988), 257
R v Looseley (2002), 381n69
R v Swaffield; Pavic v R (1998), 328n78
R v Turner (1984), 146, 329n28
racist acts, 214, 397n7
racist material, 262, 317
Racketeer-Influenced and Corrupt Organisations Statute (USA), 228
regional cooperation, 13–6
  framework for, 295–301
regional forum, 297, 299, 300–1
Regulation of Investigatory Powers Act (UK), 45, 247, 375n15
regulations
  domain name registration, 69
  information system security, 68–9, 74
  Internet, 8, 67–8
research
  computer crime, 63, 93, 133, 350, 351
  cyber-security, 137
'responsibilisation' strategy, 118–20
restitution, to victims, 228
risk management, 48, 130
risk profiling, 3
risks,
  to e-business, 81–2, 87
  security, perceptions of, 82–3, 85, 88
Royal Canadian Mounted Police, 20
Rule of Law, threat to, 160
Russia, 330, 333

sabotage, computer, 212, 315
sales fraud, 39

sanctions, 209, 265, 270–1, 312
SARS crisis, 243
Saudi Arabia, 339, 340
scanning, of computers, 338
search and seizure, 228
search engines, 340
search warrants, 61, 162, 164
Second-hand Dealing Law (Japan), 116
security, *see* cyber-security
Security Legislation Amendment (Terrorism) Act (Cwlth) (Australia), 164
self-regulation, 96, 100, 337
Senior Officials Meeting on Transnational Crime (SOMTC), 288
sentencing, 353
September 11, 2001, 133, 165, 269, 305, 331, 334,
  terrorist attacks on USA, 141, 175, 176, 290
'serious crime', defined, 12, 284, 285
serious offences, interception of content data in, 323–4
Shannon, Julie, xix, 354, 355
Sheptycki, J W E, 11
Singapore, 7, 102, , 125, 338, 339
  cyber-security
  companies, 137–9
  infrastructure, 126–40
  e-commerce, 127–8, 130, 135
  offence provisions, 225, 237
  Singapore Computer Emergency Response Team, 131
  Singapore Information Technology Federation (SITF), 136–7
'situational crime prevention', 3, 120
'smart cards', 37
Smith, Jayson (2002), 262
smuggling, 19
Sobig.F worm, 37
software, *see* computer software
Solar Sunrise, cyber-attack, 331–2, 333
sovereignty, 306, 326, 345
  issue in cross-border assistance, 273–4
South Korea, *see* Korea, Republic of
'spam' and 'spamming', 7–8, 46, 218
'spoofing', 41
stalking, *see* cyber-stalking
standardisation
  policing processes, 123
  technology, 123
standards
  IT security, 74, 135
  privacy, 135
  Public Key Infrastructure, 135
statistics
  computer use, 31
    reported crime, 4, 6, 7, 9
  cyber-crime, 6(table 1.1), 62–3, 200(tables 11.1–2), 201(table 11.3), 171, 352
statutory damages, *see* compensation
Stewart (1988), 379n25, 379n36
Sub-Committee on Customs Procedures (SCCP) (APEC), 294
Summary Offences Act 1966 (Vic) (Australia), 218
Supervision Bureau for Public Information Security (PRC), 8, 62, 71
surveillance, 49–50, 320
surveys, 82–3, 104
Sussman, M A, 305
Sutherland, E H, 3

Tachiainin system, 7, 111–2,
Taiwan, 228, 330
  offence provisions, 236, 237
Tanabe, Yasuhiro, 13
Tatsuzaki, Masao, xix, 6
tax evasion, 36–7
technology, standardisation, 123
Telecommunication (Interception) Act 1979 (Cwlth) (Australia), 382n80

Telecommunication Interception for Criminal Investigation Law (Japan), 110, 112, 113
telecommunications (*see also* interception of telecommunications, telecoms policing)
anonymising of, 114
defined, 248
theft of services, 36
Telecommunications and Infrastructure Working Group (APEC), 295, 302
Telecommunications Ordinance (Cap. 106), 97, 245, 247, 248–9, 251, 252, 257
'telecommunications services', defined, 378n22
Telecoms Action Task Force (Japan), 123
telecoms policing
case studies, 116–122
costs, recovery, 121–2
defined, 109
needs, policy, 122–3
processes, standardisation, 123
technology needed for, 114
user requirements for, 115
terminatory theory, 155
territoriality, 154, 155
terrorism (*see also* cyber-terrorism), 141, 164–5, 290
text pattern searching, 205
Thailand, 9, 32, 340, 364n31
offence provisions, 226, 238
theft, telecommunications services, 32
Theft (Amendment) Ordinance (No. 45 of 1999), 258
Theft Ordinance (Cap. 210), 97, 256, 258, 390n22
Thomas, Nicholas, xix, 354, 355
Thompson v The Queen (1989), 380n44
TOC Convention, *see* Convention Against Transnational Organised Crime
topography, reproduction of, 212
Trade-Related Aspect of Intellectual Property Rights (TRIPs) Agreement, 240
trade marks, infringement, 231, 232, 233, 236, 237
Trade Marks Act (Australia), 239
traffic data, 272, 308
preservation and disclosure, 321
real-time collection, 278, 319, 323
retention of, 176
training, 27, 286, 292, 296, 298, 306
transnational crime, centre for combating, 288
transnational policing, 10–3
transnational-state-system, 11
Trojan horse virus, 9, 334, 338
trust, 336
as issue in international cooperation, 333
Tsang, W W, xvii
Tung Chee Hwa, 243
'24/7 network', *see* points of contact

Uchimura, Keiji, xx, 6, 353
unauthorised access, *see* illegal access
Unauthorised Computer Access Law (Japan), 170, 171(table 9.2), 174–5, 177, 178–81
unauthorised use, 212, 213
United Kingdom, 100–1, 103, 105–6
media coverage of cyber-crime, 90
policing Internet, 104
research, 93–4
United Nations (UN), 53, 214, 282–6
manual on computer-related crime, 394n21
resolution on information and telecommunications security, 333–4
United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders

(UNAFEI), 13, 53, 283, 286, 349, 362n11
United Nations Commission on International Trade Law (UNCITRAL), 128
United Nations Drug Control Program (UNDCP), 14, 394n20
United States of America (USA), 75, 228, 330, 334, 342
attacks on, 175, 176
Internet governance, 95
treaties, 393n6, 393n9
United States Trade Representative (USTR), 230, 231
University of Hong Kong, 357
Centre for Criminology, xi, 93
Centre for Security and Cryptography, 18, 355
Urbas, Gregor, xx, 13
utility models, intellectual property laws, 239
Uzbekistan, 10

vandalism, electronic, 37–40
victims, of cyber-crime, 104–5, 106
restitution, 228
Vienna Convention Against Illicit Traffic in Narcotics and Psychotropic Substances, 12
Vienna Declaration on Crime and Justice, 214
Vietnam, 10, 16, 341
viruses, computer (*see also* 'I Love You' virus), 2, 9, 18, 305, 344,
attacks, lack of protection against, 343
bounty on creators, 355
detection, 49
guidelines on countering, 290
impact of, 37, 43–4, 207–8, 342–3

Wang Youcai, 76
Ward, 155
Weber, Max, 118
websites, 8, 80, 327, 337
'white-collar' crime, 3, 197
Williams v Keelty (2001), 381–2n74
'wire tapping', computer networks, 244
Wonderland Club, 33
Wong, Georgina, xx
Wong, Kam C, xx–xxi
World Information Technology and Services Alliance (WITSA), 116
World Wide Web
'sweeps' of, 349
as term, use of, 386n8
worms, computer, 2, 18, 37

xenophobic acts, 214, 397n7
xenophobic material, 262

Yang Zhenquan, 73
yearbook, proposal for, 358
Yong Pung How, Chief Justice, 160