

# CYBER-CRIME

## The Challenge in Asia

Edited by Roderic Broadhurst & Peter Grabosky

# CYBER-CRIME

## The Challenge in Asia

"This collection is innovative and original. It introduces new knowledge and is very timely because of the current high profile of the international public discourse over security, the internet and its impact upon the growth of the information economy. The book will be very useful to a wide range of readers because it will both inform and provide the basis for instruction." — **David S. Wall**, Professor of Criminal Justice and Information Technology, University of Leeds School of Law; editor of *Cyberspace Crime and Crime and the Internet*.

"This book significantly advances the scholarly literature available on the global problem of cyber-crime. It also makes a unique contribution to the literature in this area. Much of what has been written focuses on cyber-crime in the United States and in Europe. This much-needed volume focuses on how cyber-crime is being dealt with in Asian countries. It explains how law enforcement is responding to the complex issues cyber-crime raises and analyzes the difficult policy issues this new type of transnational crime generates. This book is an invaluable addition to the library of anyone who is concerned about online crime, computer security or the emerging culture of the Internet." — **Susan W. Brenner**, NCR Distinguished Professor of Law and Technology, University of Dayton School of Law

"Broadhurst and Grabosky have assembled a comprehensive and timely work on cyber-crime in Asia, which features the scholarly works of an impressive collection of experts from such critical disciplines as technology, law enforcement and academia. This highly readable book defines the scope and magnitude of the cyber-crime problem in the Asia region, provides a guide to the current state of both government and non-government efforts, and presents a roadmap of where we, as a society, need to dedicate resources and effort if we are to have an impact on these very real crimes. A major theme of this authoritative collection is the imperative for government and the private sector to join forces and share not only responsibility but also expertise, technology and information. I highly recommend this book to anyone interested in the latest challenges of the Digital Age." — **Richard LaMagna**, Legal and Corporate Affairs, Microsoft

**Roderic Broadhurst** is an Associate Professor, Department of Sociology, and Senior Fellow, Centre for Criminology, University of Hong Kong. His research interests include violence, repeat offending, professional delinquency and crime in developing countries.

**Peter Grabosky** is a Professor in the Regulatory Institutions Network, Australian National University. He specialises in criminal justice and public policy with an emphasis on computer crime and policing.



香港大學出版社  
HONG KONG UNIVERSITY PRESS  
www.hkupress.org

IT, Law, Crime

ISBN 962-209-724-3



9 789622 097247

# CYBER-CRIME

Hong Kong University Press thanks Xu Bing for writing the Press's name in his Square  
Word Calligraphy for the covers of its books. For further information, see p. iv.

# **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

© Hong Kong University Press 2005

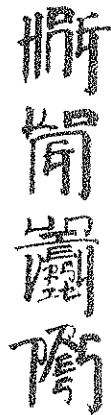
ISBN 962 209 735 9 (Hardback)  
ISBN 962 209 724 3 (Paperback)

All rights reserved. No portion of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage or retrieval system, without prior permission in writing from the publisher.

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
<i>Justice K Bokhary, Hong Kong Court of Final Appeal</i>	
Acknowledgements	xiii
Contributors	xv
Abbreviations	xxiii
1. Computer-Related Crime in Asia: Emergent Issues	1
<i>Roderic Broadhurst and Peter Grabosky</i>	
2. The Global Cyber-Crime Problem: The Socio-Economic Impact	29
<i>Peter Grabosky</i>	
3. Cyberspace Governance and Internet Regulation in China	57
<i>Kam C Wong and Georgiana Wong</i>	
4. Cyber-Crime and E-Business in China: A Risk Perception Perspective	79
<i>Ivan S K Chui</i>	

5.	Governance in the Digital Age: Policing the Internet in Hong Kong <i>Laurie Yiu Chung Lau</i>	89
6.	Third Party 'Responsibilisation' Through Telecoms Policing <i>Keiji Uchimura</i>	109
7.	Cyber-Security: Country Report on Singapore <i>Clement Leong and Chan Keen Wai</i>	125
8.	Cyber-Crime in the 21st Century: Windows on Australian Law <i>Simon Bronitt and Miriam Gani</i>	141
9.	Cyber-Crime: Current Status and Countermeasures in Japan <i>Masao Tatsuzaki</i>	169
10.	Cyber-Crime in India: The Legal Approach <i>Pavan Duggal</i>	183
11.	Computer Crimes: What Everyone Should Know About Them <i>K H Pun, Venus L S Cheung, Lucas C K Hui, K P Chow, W W Tsang, H W Chan, C F Chong</i>	197
12.	Cyber-Crime Legislation in the Asia-Pacific Region <i>Gregor Urbas</i>	207
13.	Law Enforcement in Cyberspace: The Hong Kong Approach <i>Michael Jackson</i>	243
14.	International Cooperation in Combating Cyber-Crime in Asia: Existing Mechanisms and New Approaches <i>Jeffrey G Bullwinkel</i>	269
15.	The Council of Europe Convention on Cyber-Crime: A Response to the Challenge of the New Age <i>Peter Csonka</i>	303
16.	Human Security and Cyber-Security: Operationalising a Policy Framework <i>Julie Shannon and Nick Thomas</i>	327

17.	The Future of Cyber-Crime in Asia <i>Peter Grabosky and Roderic Broadhurst</i>	347
	Notes	361
	References	403
	Index	419

## Lists of Tables and Figures

	<i>Page no.</i>
<b>List of Tables</b>	
Table 1.1 Computer-related crimes reported in Hong Kong	6
Table 2.1 Top ten countries by piracy rate (%)	34
Table 3.1 CNNIC statistics on the development of China's Internet, 1997–2003	59
Table 3.2 Statistics of cyber-crime in China, 1998–2001	62
Table 3.3 Jiang's analysis of computer crime cases, 1989–99	63
Table 3.4 A brief chronology of China's intellectual property protection	70–71
Table 4.1 Personal experience of hackers / crackers	84
Table 4.2 Threat of hackers / crackers to society	84
Table 4.3 Self-description on the effects of invasion by hackers / crackers	84
Table 4.4 Sending personal or important information	85
Table 4.5 Agree that purchasing from e-commerce websites is a widespread practice in your society	86
Table 4.6 Proportion visiting and purchasing from e-business websites	86
Table 4.7 Preferred method of payment for online purchases	87
Table 5.1 Computer-related crimes: reported cases in Hong Kong, 1993–2003	93
Table 7.1 Computer-related offences, 1997–2002	132
Table 8.1 Computer crime offences by jurisdiction: non-Model Criminal Code offences	150
Table 8.2 Computer crime offences by jurisdiction: Model Criminal Code offences	151–153
Table 9.1 Analysis of Cyber-Crime	171
Table 10.1 Internet penetration, March 1997 to March 2005	185
Table 11.1 Technology crimes recorded in Hong Kong, 2000–03	200
Table 11.2 Computer crime cases in Hong Kong, January to June 2003	200
Table 11.3 Monthly computer crime cases in Hong Kong, 2002	201
Table 12.1 Computer crime offence provisions, Australia	217
Table 12.2 Computer crime offence provisions, PR China	219

Table 12.3 Computer crime offence provisions, Hong Kong	220
Table 12.4 Computer crime offence provisions, India	221
Table 12.5 Computer crime offence provisions, Japan	222
Table 12.6 Computer crime offence provisions, Republic of Korea	222
Table 12.7 Computer crime offence provisions, Malaysia	223
Table 12.8 Computer crime offence provisions, New Zealand	224
Table 12.9 Computer crime offence provisions, Philippines	224
Table 12.10 Computer crime offence provisions, Singapore	225
Table 12.11 Computer crime offence provisions, Taiwan	226
Table 12.12 Computer crime offence provisions, Thailand	226
Table 12.13 Software piracy rates and US dollar losses in the Asia-Pacific region	230
Table 12.14 Intellectual property offence provisions, Australia	231
Table 12.15 Intellectual property offence provisions, PR China	232
Table 12.16 Intellectual property offence provisions, Hong Kong	233
Table 12.17 Intellectual property offence provisions, India	234
Table 12.18 Intellectual property offence provisions, Japan	234
Table 12.19 Intellectual property offence provisions, Republic of Korea	235
Table 12.20 Intellectual property offence provisions, Malaysia	235
Table 12.21 Intellectual property offence provisions, New Zealand	236
Table 12.22 Intellectual property offence provisions, Philippines	236
Table 12.23 Intellectual property offence provisions, Singapore	237
Table 12.24 Intellectual property offence provisions, Taiwan	237
Table 12.25 Intellectual property offence provisions, Thailand	238

### List of Figures

Figure 9.1 Trends in Internet Penetration in Japan	170
Figure 9.2 Arrest trends for Cyber-Crime	171
Figure 9.3 The IT security chain of command	172
Figure 9.4 Major government policies	173
Figure 9.5 Unauthorised Computer Access Law	175
Figure 10.1 Internet growth in India	184
Figure 10.2 Projected growth of the Internet in India	184
Figure 11.1 A hacking example using the Buffer Overflow technique	199
Figure 11.2 Use of digital signatures	203
Figure 11.3 Use of data encryption to protect confidentiality	204

## Foreword

For two principal reasons, this very useful book is highly representative of the valuable work done by the University of Hong Kong's Centre for Criminology. So much so that the book is almost emblematic of the centre. First, the subject-matter of the book, cyber-crime, is one to which the centre has devoted much attention as one of the great problems of today. Secondly, the book, like the centre itself, draws on and co-ordinates the learning and experience of persons from academia, industry and law enforcement throughout Asia and the Pacific Rim.

As a matter of form, this book can be described as a collection of essays. Between them, the essays cover the emerging trends and key issues which Asian and the Pacific Rim jurisdictions face in their efforts to combat computer-related crime. Discussed are crimes committed with computers (such as online fraud), crimes committed against computers (such as hacking) and crimes in which computers are incidentally involved (as, for example, where the records of illegal activities are stored in computers).

In the course of my opening address at the centre's Second Asia Cyber-Crime Summit in November 2003, I ventured to observe that in no other field of criminal activity are international borders more porous than they are in cyber criminal activity, and that this presents the family of nations with a unique challenge. This book makes a significant contribution to the means by which that challenge can be met. In addition to the need for international and transnational co-operation on an unprecedented scale, cyber-crime has

given rise to a need, which this book brings out and explains, for closer co-operation between the public and private sectors.

This book is suitable for use as a textbook in advanced criminology courses. Over and above that, it deserves a wide readership in academic, business, government and professional circles.

The Hon Mr Justice Bokhary PJ,  
Hong Kong Court of Final Appeal.

## Acknowledgements

This collection is the work of many hands. First we would like to thank all of the contributors for their patience, and for their prompt attention to our editorial entreaties.

We would also like to thank the Centre for Criminology of the University of Hong Kong, and its sponsors for hosting the two Asia Cyber-Crime Summits that provided the inspiration for this book. The partnerships between industry, law enforcement and the university that ensured the success of these meetings continued to aid us in the preparation of this volume. We are especially grateful for the wonderful support and assistance given to us by the officers of the Hong Kong Police Technology Crime Division. We are also grateful to Venetia Somerset, Bronwyn McNaughton and Yeung Oi Yan for their masterful editorial contributions, encouragement and support.

Finally we would like to extend our appreciation to Hong Kong University Press and in particular Dennis Cheung for bringing this book to life.

If, despite the efforts of those above, there are any shortcomings in the book, they remain ours alone.

Federic Broadhurst  
Hong Kong

Peter Grabosky  
Canberra

January 2005

## 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 infocommunications 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](http://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 LL.M. 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.

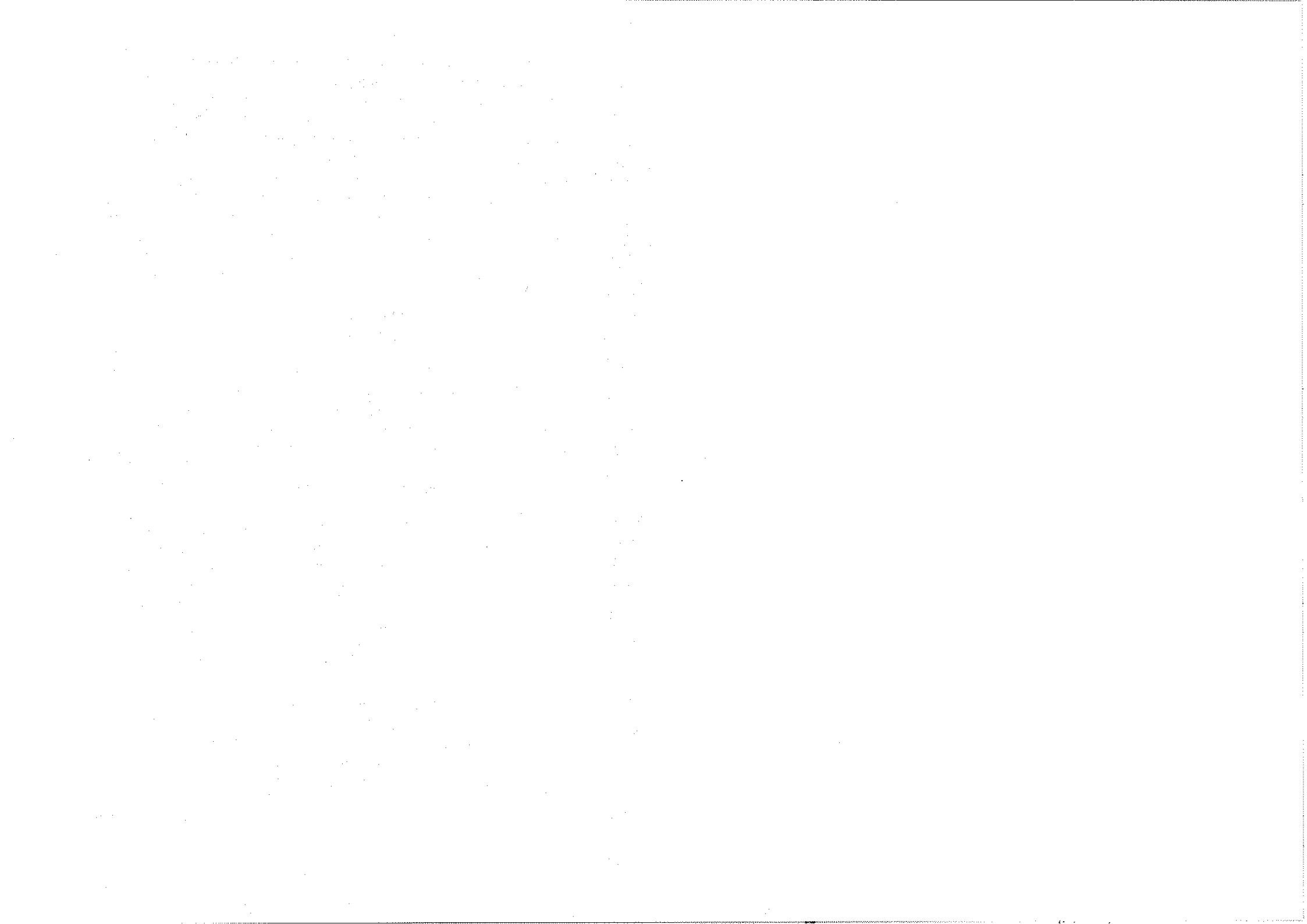
Keiji Uchimura is a Professor in the Applied Technology Department, National Police Academy (Japan). He was previously Staff Officer of the First Criminal Investigation Division at Keishicho (Metropolitan Police Department) from 1997–98, and was Assistant Director in the Investigative Planning Division, 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.



## The Future of Cyber-Crime in Asia

Peter Grabosky and Roderic Broadhurst

Asia is an interesting and important region, indeed a crucial region, in which to observe the trajectory of digital technology and the criminal risks that accompany it. In some places, such as Singapore and Hong Kong, levels of connectivity are among the highest in the world. In the People's Republic of China, the rate of uptake of digital technology has been nothing short of stunning, as the Wong and Wong chapter in this volume illustrates. Information technology industries in places like Japan, Korea and Taiwan are world leaders; Malaysia and Thailand are committed to joining their ranks.

At the same time, there are Asian countries that have yet to benefit significantly from the digital revolution. For political and economic reasons, digital technology remains a relative novelty in countries like Myanmar, Laos, Mongolia, Cambodia and North Korea. This digital divide, as it exists in Asia, has a number of implications.

For those countries that have well and truly entered the digital age, progress is accompanied by risk. They have, within their borders, a greater proportion of potential victims and more potential perpetrators of cyber-crime. To the extent that techno-savvy offenders in foreign lands perceive these countries' information systems as attractive, the risk is that much greater. For these reasons, countries in the forefront of digital technology have begun to develop the legal and human resources appropriate to achieve security and prosperity in cyberspace. Substantive and procedural criminal laws, investigative skills, a vibrant information security industry, and mechanisms

for cross-national cooperation are all hallmarks of those countries where economic security and cyber-security are inextricably intertwined.

By contrast, in countries for which the digital age has only just begun to dawn, circumstances differ dramatically. Commerce and infrastructure are less dependent on information technology, and there are fewer prospective cyber victims and cyber-perpetrators. Laws and investigative resources are often inadequate to cope with terrestrial criminality, much less high-technology crime. To the extent that connectivity exists in these countries, the ability of prospective offenders to operate with relative impunity is that much greater. Not only are risks to the few existing domestic targets considerably higher, but risks to the more abundant targets in the region and indeed around the world are also real.

The chapters in this volume have provided an important overview of progress to date in the prevention and control of cyber-crime. In this concluding chapter, we seek to address two practical issues:

- What still needs to be done in terms of policy development?
- What research is needed to provide an evidence base for future policy?

In addition, we raise some additional questions about the role of the private sector in combating cyber-crime.

## ■ Policy Development

Jeff Bullwinkel mapped out ideal policy directions in his chapter. These include:

- The enactment of substantive and procedural laws adequate to cope with current and anticipated manifestations of cyber-crime
- The development of forensic computing skills by law enforcement and investigative personnel
- The achievement of a modicum of legal harmonisation in the region and indeed globally
- The creation of mechanisms for operational cooperation between law enforcement agencies from different countries: 24/7 points of contact for investigators, and mechanisms for mutual assistance in cyber-criminal matters generally.

Although Asia is and will remain a diverse region, its nations should continue to strive for the realisation of each of these goals. Given the

diversity of legal traditions in the Asian region, it is unrealistic to expect uniformity in law, policy and practice. Nevertheless, this basic framework should serve as a roadmap for continuing efforts.

The most technologically sophisticated of Asian nations are already at the forefront of IT but face the new challenges that accompany the rapid development of compression and wireless technology. While it may be unrealistic to expect that all nations of the region will think alike in matters of law and practice in relation to content regulation, there is potential for wider consensus in matters relating to economic crime. And frameworks for cooperation in the investigation and prosecution of cyber-crime in Asia are now under construction.

Some of these frameworks are global in origin, and others more distinctively Asian as, for example, shown in Pavan Duggal's chapter on India's response to cyber-crime. As early as 1989, the Council of Europe published a study and recommendations addressing the need for new laws relating to computer crime. By the mid-1990s, as detailed in the chapter by Peter Csonka, the Council began developing a comprehensive Cyber-crime Convention. Several countries that do not belong to the Council participated in the negotiations that developed the Convention, including Japan, the United States and Australia. Asian observers who may be inclined to take a long-term view of policy development should note that the treaty took four years to negotiate and underwent more than 20 drafts.

Interpol established the Computer Crime Steering Committee in 1995 in an effort to rationalise and optimise regional responses to cyber-crime, and established four regions across the globe. In our region, the Interpol Asia-South Pacific Regional Working Party of IT Crime has been active since 1997. Among other projects, it has engaged in a survey of e-crime issues in the region; a survey of forensic and investigative tools used in Asia; and an assessment of Asian training strategies and facilities. The leader of this latter project was the Hong Kong Police. The activities of UNAFEI, discussed by Jeff Bullwinkel in his chapter, reflect the contribution that Japan is making to regional capacity-building in the area of cyber-crime control.

Other specific types of cyber-crime have elicited a wide international response. Given the global nature of cyberspace and its increasing use as a medium of commerce, regulators around the world must cooperate in the detection and suppression of market-related illegalities. The International Consumer Protection and Enforcement Network, a consortium of countries including Japan, Korea, Australia and New Zealand, conducts annual 'sweeps' of the World Wide Web in search of fraudulent sales pitches. Representatives of all participating nations search the Web for 'get rich quick' schemes and

'miracle cures' and report suspicious activities to authorities in the country from which the offending conduct appears to originate.

Through regional initiatives or overseas developments, the basic models of international cooperation, are there for adoption and adaptation to Asian conditions.

## ■ Evidence Base

The task of providing an evidence base for future policy development is challenging. Research on cyber-crime is in its infancy. Knowledgeable individuals and institutions, both in the public and private sectors, may for commercial, political or national security reasons be disinclined to share their wisdom with researchers. Information that finds its way on to the public record often may actually be misinformation or disinformation.

Despite these handicaps, it is important to develop a knowledge base, so we can begin to narrow the digital divide that exists in Asia today. Given the global nature of cyberspace, and the persistent risk of cross-border offending, a broader knowledge base will benefit the digital 'haves' as well as the digital 'have-nots'.

Country case studies, focusing either on individual incidents or on more general developments, can help raise public awareness of policy imperatives. The experience of the Philippines, whose substantive criminal laws were inadequate to respond to the 'I Love You' virus, was illustrative. The legislative 'patch' introduced in the aftermath of the incident may have stood the Philippines in good stead since then, but it was too late to apply to the alleged perpetrator, Onel de Guzman.

Similarly, case studies of individual investigations, successful or otherwise, can also be instructive. Success stories can help build confidence among new investigators, or among public officials generally in those countries that are on a steep cyber-forensics learning curve. 'Recipes' for success may also be useful for training purposes. The success of Operation Buccaneer, a large-scale international copyright piracy investigation, is illustrative. The coordinated international effort resulted in the execution of more than 60 searches in six different nations (see [www.cybercrime.gov/ob/OBMain.htm](http://www.cybercrime.gov/ob/OBMain.htm), visited 11 February 2004).

Studies of unsuccessful investigations are no less important. Despite the fact that individuals or agencies do not like to dwell on failure, it is important to understand what went wrong, to reduce the likelihood of subsequent similar mishaps. Just as hospital staff meet in regular mortality and morbidity

conferences, and aviation safety specialists analyse the circumstances of aircraft accidents, so too should cyber-crime specialists reflect systematically on cases that 'go wrong'. This information, too, can be useful for training specialists in cyber-forensics.

Other issues call out for comparative study. One of these might be the ways in which law enforcement agencies of different countries cope with evidence of possible criminal activity that may be encrypted. When evidence exists in a form that is not accessible to investigators, what do they do? Do they seek to mobilise decryption technology to 'break' the code (a strategy that has become much less effective given the widespread availability of strong encryption technology)? Do they issue, subject to judicial oversight, 'decryption orders' requiring assistance in rendering the evidence intelligible, with penalties for non-compliance? Do they use high-technology means of identifying encryption keys, such as keystroke logging devices or the technologies of remote search? Obviously, solutions will vary from country to country, depending on the rights accorded to suspects in criminal cases. But a comparative study could be useful as well as informative.

The ease of cross-border offending has posed new challenges for law enforcement agencies. It would be instructive to analyse some of the cases of cross-border offending that have come to official attention. Were 24/7 arrangements in place, and did they function as intended? Were the laws of the country from which the cross-border offending originated adequate to deal with the matter? Was there agreement or disagreement on the part of authorities of the two countries as to whether domestic prosecution was preferable to extradition? Was the outcome satisfactory to all parties?

The importance of bilateral and multilateral relationships to respond to cross-national cyber-criminality is the theme running through many chapters in this book. Tightening the web of relationships that was described in the chapter by Jeff Bullwinkel is a goal for all nations seeking security and prosperity in cyberspace. To monitor the progress towards this goal, periodic mappings of the 'density' of these relationships (including intelligence-sharing networks) would be useful.

The future of electronic commerce, in Asia and indeed, globally, depends on the continued confidence of current and prospective customers in the integrity and security of e-commerce systems. The chapter by Ivan Chiu reported research on public perceptions of e-commerce in the People's Republic of China. Observing trends in public confidence in e-commerce over time in one country is important. Similar research could be conducted on a cross-national comparative basis. Comparing findings relating to public confidence with actual levels of e-commerce can also be useful.

Statistics about the prevalence of computer-related crimes are notoriously poor. The most artful of cyber-crimes are not detected in the first place. Of those that are, many are never reported to police. Those proportionately few incidents that do reach official attention may be classified as generic offences such as fraud, and reference is rarely made to the technology applied to achieve the offence.

While it may be unrealistic to aspire to a situation of omniscience about the incidence of computer crime, this is not a ground for abandoning an attempt at useful measures of incidence. Rather than seeking a perfect picture, we should endeavour to build a mosaic, using hard evidence of events where that may exist, and approximations or estimates when nothing better is available. In any event, this task should be approached as systematically as possible, lest we be open to the criticism that we are inventing estimates, over-dramatising rare events or playing fast and loose with the truth. What might some of the components or fragments of an evidence-based surveillance system look like? They could perhaps include the following:

- Software and entertainment industries regularly estimate their losses resulting from electronic piracy. They will continue to do so, and should be encouraged to articulate fully the assumptions on which these estimates are based.
- Other strategies to complement official crime statistics include victim surveys. For example in many countries, large accounting firms conduct periodic surveys of their client base, or of industry generally, to determine the incidence and prevalence of computer-related crime that they have experienced. These should continue, but survey methods must be clearly specified if they are to meaningfully contribute to any 'overall picture'. Cyber-crime victimisation surveys therefore complement official statistics as a means of estimating the volume of cyber-illegality.

Not all reported cyber-crimes are prosecuted. There will be cases that do not receive police attention because of limited resources. Some investigations will founder because the complexity of the crime exceeds the technical capacity of law enforcement. Of cases that are referred for prosecution, prosecutors may themselves lack the ability to deal with them. Alternatively, evidence may be insufficient to sustain a prosecution. More complete knowledge about the attrition of cases from initial detection through to prosecution will point to where improvements in the administration of justice may be required.

Most incidents of cyber-crime do not proceed to conviction. Of those that do, we know little about the eventual sentences imposed. While it may be unrealistic to strive for consistency across nations in the sentences imposed on cyber-criminals, the reduction of disparity *within* countries is desirable given the transnational nature of offending. Systematic studies of sentencing can contribute to this goal and help clarify the role of deterrence-based responses to cyber-crime.

We know very little from any country about what constitutes aggravating or mitigating circumstances in cyber-crime cases. Some electronic pirates are in it for the money, while others do it for free. To what extent should motive matter, or should the financial loss to the copyright owner be the key factor in sentencing? In cases involving the release of a crippling virus, or a distributed denial of service attack resulting in thousands of dollars of down time and lost e-business, to what extent should it matter that the offender is a juvenile? What is regarded as an appropriate penalty in such cases?

Asian countries, no less than countries around the world, differ in terms of their policy priorities. For example, Keiji Uchimura's chapter illustrates the difficulties in Japan of enlisting private industry technical staff in the supervision of interception and the investigation of cyber-crime. These priorities are by no means constant and may vary over time depending on internal political and technological developments, and external exigencies. It would be useful to develop an overview of priorities in the Asia-Pacific region, and to observe how priorities change, both within individual countries and in such multilateral forums as the APEC high-tech group and ASEAN.

What are individual countries concerned about? What kinds of cyber-crime take precedence: hacking, fraud or theft of intellectual property? Are governments more concerned about infrastructure protection or child pornography? What explains the elevation or decline of an issue on the public agenda? Lobbying by the affected industries or a real increase in the underlying behaviour or international pressure?

Governments across Asia will continue to mobilise a variety of responses to cyber-crime; these will meet with varying degrees of success and entail costs. In times of fiscal restraint, it is important to ask which of these responses are most effective, and at what price. Whether the response to cyber-crime is driven by government agencies, by the private sector, or by some combination of the two, it will be useful to observe whether the response in question achieves its purpose without producing adverse unintended consequences, or 'collateral damage'. We noted earlier that there might be a tension between security and user-friendliness. A 'bullet-proof' system that turns off prospective

clients may lose money in the long run. Filtering software that is overbroad may restrict access to legitimate sites. Limiting access to the Internet in order to discourage communication on behalf of political dissidents may also have the unintended consequence of inhibiting the development of electronic commerce. One could perhaps be forgiven for asking if there is a tolerable level of crime that we must endure to enjoy the maximum economic, cultural, educational benefits of digital technology. What tradeoffs are we prepared to make?

While government has necessarily driven much of the activity in response to cyber-crime, the private sector will play a crucial role in the prevention and control of crime in the digital age. To this we now turn.

### ■ Fostering Market Solutions

One of the more noticeable trends in contemporary public affairs has been the privatisation of state-owned assets. Governments around the world are shedding roles that were previously regarded as core functions; they are selling off assets that were once regarded as integral public property. And so it is that a great deal of national infrastructure — electric power, communications, transportation and financial systems — once owned by governments, now resides in private hands. Threats to this infrastructure are inimical to national security no less today than when these assets were public. As noted by John Shannon and Nick Thomas, securing this infrastructure has thus become a joint public-private responsibility.

When ownership and control of key assets are dispersed across a number of private institutions, challenges of co-ordination in furtherance of security are at least equal to those once faced by big government, where consistency and cooperation between agencies was often illusory. Private institutions may be ignorant of their vulnerabilities, or, if they are aware of them, they may be most reluctant to publicise this. Consequently, developing a coherent national programme of infrastructure protection becomes that much more difficult.

As noted in Laurie Lau's chapter, the information technology industry itself is largely private. Not only do industry giants such as Microsoft command resources and expertise that overshadow those of many nation-states, but other players in the global information industry also have significant roles. Even smaller companies, be they specialised information security firms or Internet service providers, are extremely knowledgeable. As Simon Bronitt and Marwan Gani observed in their chapter, private sector organisations are often better situated to prevent cyber-crime. They are also sometimes better placed to

gather evidence of those crimes that are committed; in some cases they even provide expertise and resources to fund police investigations. Unilateral initiatives by the private sector show considerable promise. These include Microsoft's bounty on virus software writers, IFPI's general focus on deterring individual 'music pirates', and BSA's deployment of automated 'web crawling' software to identify bogus or illegal websites.

Collaboration between police and educational institutions can also be beneficial. The Hong Kong Police have developed a partnership with the Hong Kong University of Science and Technology to offer a professional diploma in computer forensics. The Centre for Information Security and Cryptography at the University of Hong Kong has developed DESK, which enables investigators to search for patterns in both Chinese and English, as well as to identify encoded or deleted files. The Korean Ministry of Information and Communication and KISA have also developed strong links with higher education institutions such as the specialist Information and Communication University and its Research Centre for Information Security. The potential for similar collaboration between law enforcement agencies and universities throughout the region is no doubt substantial.

The chapters in this volume by Lau and by Shannon and Thomas spoke of the 'governance' of cyberspace. By this was meant the various institutions, public and private, that exercise surveillance and control over one or more aspects of computing and communications. The state plays an important role, but there are many other players, both public and private. Indeed, the role of the private sector in the prevention and control of cyber-crime is arguably greater than in the domain of conventional criminality. It is certainly varied. Let us look at just a few of the ways in which private enterprise can become involved in the co-production of cyber-crime control.

In the first instance, systems can be designed to lessen their vulnerability to criminal exploitation. Cyber-crime is often facilitated by vulnerable software, much of which is designed with user-friendliness and convenience in mind rather than security. The common industry response is for manufacturers to structure their licence conditions to avoid potential liability, then to make 'patches' available as vulnerabilities become apparent later on. Whether market forces will eventually drive the widespread development of truly secure software remains to be seen.

Other information security technologies are becoming household words. Cryptography can help secure electronic commerce, while firewalls and other security technology can protect against hackers. Access controls can detect anomalous patterns of system use and raise the alarm about potential misuse. Biometric authentication technologies can guard against unauthorised entry.

Blocking and filtering technologies can help screen out undesirable content. Owners of intellectual property can create content that degrades when copied without authority or in violation of licence. In adopting such measures, commercial enterprises may be in a position to achieve more protection than poorly resourced law enforcement agencies can deliver.

Some may ask whether it is possible to harness market forces in furtherance of cyber-crime control. History, we believe, will answer this question in the affirmative. Half a century ago, motor vehicle manufacturers subordinated fuel efficiency, safety and vehicle security to such considerations as performance and style. Gradually government regulatory authorities imposed safety standards that were grudgingly accepted by industry. A few brave manufacturers sought to go beyond regulation, and actually market their products as safe and fuel-efficient as possible. They soon became market leaders. There are lessons here for those in the information industries of Asia and the world generally.

## ■ Public-Private Collaboration

The degree of expertise residing in the private sector makes a degree of public-private collaboration in policing inevitable. We envisage three basic forms of relationship between the public and private sectors. Private interests may be required by law to assist government agencies; they may be engaged by government on a fee-for-service basis; or they may donate goods or services on a *pro bono* basis. Each of these has limits, which have yet to be fully explored in the context of cyber-crime. Each also has costs and benefits.

The first of these, *mandatory assistance*, refers to circumstances in which a private actor is required by law to assist government in some manner or other. For example, some countries require ISPs to assist in the identification and reporting of illegal content that comes to their attention, or to retain certain transaction details for investigative purposes.

The second is *commercial exchange*. Governments can rent or hire expertise to assist in one or more activities. Special expertise in forensic computing or cryptography may not reside within the ranks of police or other government agencies and therefore temporary engagement of private sector talent may be necessary.

The third form of relationship is that of *gift*. By this we mean private sponsorship of, or donations to, some aspect of the promotion of cyber law enforcement. Perhaps the most familiar manifestation of this is the assistance provided to public law enforcement agencies by the software, payment card

and entertainment industries in response to electronic piracy and theft of intellectual property. Gift might also entail the *pro bono* secondment of specialised staff by private sector IT security firms to public law enforcement agencies.

Depending on the circumstances, each of these relationships would entail costs and benefits to the general public, the state agency, and the private actor involved. Ideally, the distribution of the costs and benefits will be equitable across the three sectors.

Requiring ISPs to retain large volumes of transaction data for lengthy periods of time can entail considerable expense. Nor may this approach be as effective as before, given the widespread adoption of anonymous stored value 'smart chip' and other untracked means of obtaining revenue. Taken to an extreme, this could have a chilling effect on a dynamic sector of the economy. Just how much of a burden should states impose on ISPs?

To what extent should states rely on contracting-in private sector expertise in forensic computing? Private sector salaries tend to be much higher than the salaries paid to public police, and over-reliance on private sector expertise can become prohibitively expensive. For reasons noted in the introduction, a degree of familiarity with digital technologies is now already essential for nearly all police. There may be an optimal level of police-private cooperation that will vary from country to country, and that will also change within a given country over time.

Those who suffer financial loss as the result of piracy or other theft of intellectual property may possess both the resources and the incentive to assist the government in the investigation and prosecution of such cases. Where governments lack the will or the resources to attend to these matters, industry co-production of enforcement may be the only alternative. When private interests offer their services in furtherance of a cyber-crime investigation, what safeguards exist to ensure that they themselves abide by the law? Should gifts (in the form of sponsorships and direct services) be explicitly or implicitly conditional? Is it possible for rich private interests to endow, in whole or in part, the computer crime squad of a poorly resourced national police agency? At what point does this support distort law enforcement priorities, such that police are acting for a private rather than the public interest?

It is not mere hyperbole to suggest that the environment of cyber-crime, in both the Asian region and globally, is constantly changing. Developing a body of knowledge about cyber-crime in Asia would be useful not just to future historians but also to contemporary policymakers. The periodic Asia Cyber Crime Summits convened by the University of Hong Kong constitute one forum for observing these changes, and help to set the agenda for law and

policy that changing circumstances may dictate. A yearbook of Asian cyber-crime, which would chronicle important events, best practices and landmark cases for each of the countries of Asia, would be a valuable resource. Such a chronicle of major developments would not only provide a useful platform for policy deliberations in the Asian region but would help complete the bigger picture for those around the world who are confronting cyber-crime and its transnational scope.

Regardless of a given nation's trajectory into the digital age, cyber-crime will continue to pose challenges to the nations of Asia and to the region collectively. The challenges will be faced, and the responses crafted, by institutions of the state, the private sector, and individuals. Asia has seen increased sophistication in the forms of criminal activity and a shift towards profit-focused offences, especially fraud and deception-like offences. The involvement of organised crime is also apparent, especially in the exploitation of intellectual property through mass copyright infringement. One has also seen a notable increase in the virulence and sophistication of malicious code. This will require timely, substantial, and coordinated responses from CERT or equivalent agencies.

In response to consumer and market forces there has been increasingly coordinated action by the private sector against cyber-crime and in ways more complementary to government capabilities. There has been a shift away from 'alarm raising' by industry towards more collaborative action. Fortunately, the willingness and capacity of the private sector to protect its own assets have also increased. The private sector has begun to develop creative solutions to some the challenges of cyber-crime. In addition to providing technical support and information to state law enforcement agencies, they have begun to pursue civil law remedies with a view towards sending a deterrent message to prospective offenders.

Although recent years have seen a quickening of governmental and cross-national cooperation, there is still a long way to go. The lack to date of any systematic evaluation of the progress made in developing truly comprehensive forms of mutual legal assistance is itself telling. Action is necessary to map and assay the effectiveness of MLA in closing the gaps in the international legal system so crucial to combating computer crime.

Given the pace of technological change, the training and retaining of expertise requires continued investment. The parlous state of some law enforcement agencies in the region poses a continuing risk of cyber-crime safe havens. Doubtless the concerns of law enforcement agents will not be limited to those offences committed with or against computers. The associated involvement of digital technology will become no less prominent in 'ordinary

crime cases. Increasing connectivity means that IT in some form will soon be present at almost every crime scene.

Four issues continue to dominate the agenda of those seeking to control cyber-crime in Asia: the quest for a truly viable international law enforcement mechanism; the challenge of transnational criminal networks; the need for even closer private and public cooperation; and the continued need for research and training. Periodic assessments of regional developments, such as those contained in this volume, can help keep abreast of the rapidly evolving environment of cyber-crime.

