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.
Contents

Lists of Tables and Figures viii
Foreword xi
   Justice K Bokhary, Hong Kong Court of Final Appeal xiii
Acknowledgements xv
Contributors xxiii
Abbreviations xxvii

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

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

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

   Ivan S K Chui 79
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Governance in the Digital Age: Policing the Internet in Hong Kong</td>
<td>89</td>
</tr>
<tr>
<td></td>
<td>Laurie Yu Chung Lau</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Third Party 'Responsibilisation' Through Telecoms Policing</td>
<td>109</td>
</tr>
<tr>
<td></td>
<td>Keiji Uchimura</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clement Leong and Chan Keen Wei</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Simon Bronitt and Miriam Gani</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Masao Tatsuzaki</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Cyber-Crime in India: The Legal Approach</td>
<td>183</td>
</tr>
<tr>
<td></td>
<td>Pavan Duggal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>K H Pun, Venus L S Cheung, Lucas C K Hui, K P Chow, W W Tsang, H W Chan, C F Chong</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Cyber-Crime Legislation in the Asia-Pacific Region</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>Gregor Urbas</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Law Enforcement in Cyberspace: The Hong Kong Approach</td>
<td>243</td>
</tr>
<tr>
<td></td>
<td>Michael Jackson</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jeffrey G Bullwinkel</td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>The Council of Europe Convention on Cyber-Crime: A Response to the Challenge of the New Age</td>
<td>303</td>
</tr>
<tr>
<td></td>
<td>Peter Csonka</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Julie Shannon and Nick Thomas</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>The Future of Cyber-Crime in Asia</td>
<td>347</td>
</tr>
<tr>
<td></td>
<td>Peter Grabosky and Rodaric Broadhurst</td>
<td></td>
</tr>
</tbody>
</table>

Notes 361

References 403

Index 419
# Lists of Tables and Figures

## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1.1</td>
<td>Computer-related crimes reported in Hong Kong</td>
<td>6</td>
</tr>
<tr>
<td>Table 2.1</td>
<td>Top ten countries by piracy rate (%)</td>
<td>34</td>
</tr>
<tr>
<td>Table 3.1</td>
<td>CNNIC statistics on the development of China’s Internet, 1997–2003</td>
<td>59</td>
</tr>
<tr>
<td>Table 3.2</td>
<td>Statistics of cyber-crime in China, 1998–2001</td>
<td>62</td>
</tr>
<tr>
<td>Table 3.3</td>
<td>Jiang’s analysis of computer crime cases, 1989–99</td>
<td>63</td>
</tr>
<tr>
<td>Table 3.4</td>
<td>A brief chronology of China’s intellectual property protection</td>
<td>70–71</td>
</tr>
<tr>
<td>Table 4.1</td>
<td>Personal experience of hackers / crackers</td>
<td>84</td>
</tr>
<tr>
<td>Table 4.2</td>
<td>Threat of hackers / crackers to society</td>
<td>84</td>
</tr>
<tr>
<td>Table 4.3</td>
<td>Self-description on the effects of invasion by hackers / crackers</td>
<td>84</td>
</tr>
<tr>
<td>Table 4.4</td>
<td>Sending personal or important information</td>
<td>85</td>
</tr>
<tr>
<td>Table 4.5</td>
<td>Agree that purchasing from e-commerce websites is a widespread practice in your society</td>
<td>86</td>
</tr>
<tr>
<td>Table 4.6</td>
<td>Proportion visiting and purchasing from e-business websites</td>
<td>86</td>
</tr>
<tr>
<td>Table 4.7</td>
<td>Preferred method of payment for online purchases</td>
<td>87</td>
</tr>
<tr>
<td>Table 5.1</td>
<td>Computer-related crimes: reported cases in Hong Kong, 1993–2003</td>
<td>93</td>
</tr>
<tr>
<td>Table 7.1</td>
<td>Computer-related offences, 1997–2002</td>
<td>132</td>
</tr>
<tr>
<td>Table 8.1</td>
<td>Computer crime offences by jurisdiction: non-Model Criminal Code offences</td>
<td>150</td>
</tr>
<tr>
<td>Table 8.2</td>
<td>Computer crime offences by jurisdiction: Model Criminal Code offences</td>
<td>151–153</td>
</tr>
<tr>
<td>Table 9.1</td>
<td>Analysis of Cyber-Crime</td>
<td>171</td>
</tr>
<tr>
<td>Table 10.1</td>
<td>Internet penetration, March 1997 to March 2005</td>
<td>185</td>
</tr>
<tr>
<td>Table 11.1</td>
<td>Technology crimes recorded in Hong Kong, 2000–03</td>
<td>200</td>
</tr>
<tr>
<td>Table 11.2</td>
<td>Computer crime cases in Hong Kong, January to June 2003</td>
<td>200</td>
</tr>
<tr>
<td>Table 11.3</td>
<td>Monthly computer crime cases in Hong Kong, 2002</td>
<td>201</td>
</tr>
<tr>
<td>Table 12.1</td>
<td>Computer crime offence provisions, Australia</td>
<td>217</td>
</tr>
<tr>
<td>Table 12.2</td>
<td>Computer crime offence provisions, PR China</td>
<td>219</td>
</tr>
<tr>
<td>Table 12.3</td>
<td>Computer crime offence provisions, Hong Kong</td>
<td>220</td>
</tr>
<tr>
<td>Table 12.4</td>
<td>Computer crime offence provisions, India</td>
<td>221</td>
</tr>
<tr>
<td>Table 12.5</td>
<td>Computer crime offence provisions, Japan</td>
<td>222</td>
</tr>
<tr>
<td>Table 12.6</td>
<td>Computer crime offence provisions, Republic of Korea</td>
<td>222</td>
</tr>
<tr>
<td>Table 12.7</td>
<td>Computer crime offence provisions, Malaysia</td>
<td>223</td>
</tr>
<tr>
<td>Table 12.8</td>
<td>Computer crime offence provisions, New Zealand</td>
<td>224</td>
</tr>
<tr>
<td>Table 12.9</td>
<td>Computer crime offence provisions, Philippines</td>
<td>224</td>
</tr>
<tr>
<td>Table 12.10</td>
<td>Computer crime offence provisions, Singapore</td>
<td>225</td>
</tr>
<tr>
<td>Table 12.11</td>
<td>Computer crime offence provisions, Taiwan</td>
<td>226</td>
</tr>
<tr>
<td>Table 12.12</td>
<td>Computer crime offence provisions, Thailand</td>
<td>226</td>
</tr>
<tr>
<td>Table 12.13</td>
<td>Software piracy rates and US dollar losses in the Asia-Pacific region</td>
<td>230</td>
</tr>
<tr>
<td>Table 12.14</td>
<td>Intellectual property offence provisions, Australia</td>
<td>231</td>
</tr>
<tr>
<td>Table 12.15</td>
<td>Intellectual property offence provisions, PR China</td>
<td>232</td>
</tr>
<tr>
<td>Table 12.16</td>
<td>Intellectual property offence provisions, Hong Kong</td>
<td>233</td>
</tr>
<tr>
<td>Table 12.17</td>
<td>Intellectual property offence provisions, India</td>
<td>234</td>
</tr>
<tr>
<td>Table 12.18</td>
<td>Intellectual property offence provisions, Japan</td>
<td>234</td>
</tr>
<tr>
<td>Table 12.19</td>
<td>Intellectual property offence provisions, Republic of Korea</td>
<td>235</td>
</tr>
<tr>
<td>Table 12.20</td>
<td>Intellectual property offence provisions, Malaysia</td>
<td>235</td>
</tr>
<tr>
<td>Table 12.21</td>
<td>Intellectual property offence provisions, New Zealand</td>
<td>236</td>
</tr>
<tr>
<td>Table 12.22</td>
<td>Intellectual property offence provisions, Philippines</td>
<td>236</td>
</tr>
<tr>
<td>Table 12.23</td>
<td>Intellectual property offence provisions, Singapore</td>
<td>237</td>
</tr>
<tr>
<td>Table 12.24</td>
<td>Intellectual property offence provisions, Taiwan</td>
<td>237</td>
</tr>
<tr>
<td>Table 12.25</td>
<td>Intellectual property offence provisions, Thailand</td>
<td>238</td>
</tr>
</tbody>
</table>

## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 9.1</td>
<td>Trends in Internet Penetration in Japan</td>
<td>170</td>
</tr>
<tr>
<td>Figure 9.2</td>
<td>Arrest trends for Cyber-Crime</td>
<td>171</td>
</tr>
<tr>
<td>Figure 9.3</td>
<td>The IT security chain of command</td>
<td>172</td>
</tr>
<tr>
<td>Figure 9.4</td>
<td>Major government policies</td>
<td>173</td>
</tr>
<tr>
<td>Figure 9.5</td>
<td>Unauthorised Computer Access Law</td>
<td>175</td>
</tr>
<tr>
<td>Figure 10.1</td>
<td>Internet growth in India</td>
<td>184</td>
</tr>
<tr>
<td>Figure 10.2</td>
<td>Projected growth of the Internet in India</td>
<td>184</td>
</tr>
<tr>
<td>Figure 11.1</td>
<td>A hacking example using the Buffer Overflow technique</td>
<td>199</td>
</tr>
<tr>
<td>Figure 11.2</td>
<td>Use of digital signatures</td>
<td>203</td>
</tr>
<tr>
<td>Figure 11.3</td>
<td>Use of data encryption to protect confidentiality</td>
<td>204</td>
</tr>
</tbody>
</table>
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
Foreword

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 Venetta
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.

Roderic 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 Organized 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
Contributors


(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 information 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 Chu 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
cyberCrime 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 written
articles, chapters and books on East Asian regionalism, human security, and
Hong Kong politics. His most recent book is Re-Orienting Australia-China
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 Urbaś, 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 Global Cyber-Crime Problem: The Socio-Economic Impact

Peter Grabosky*

This chapter discusses current and emerging forms of computer-related illegality. It reviews 11 generic forms of illegality involving information systems as instruments or as targets of crime, and discusses in general terms the costs imposed by computer-related crime, and attempts to control it within and across nations.

It will suggest that much computer-related illegality lies beyond the capacity of contemporary law enforcement and regulatory agencies alone to control, and that security in cyberspace will depend on the efforts of a wide range of institutions, as well as on a degree of self-help by potential victims of cyber-crime. The ideal configuration may be expected to differ, depending on the activity in question, but is likely to entail a mix of law enforcement, technological and market solutions. These themes are explored in greater detail in two books (Grabosky & Smith 1998; Grabosky, Smith & Dempsey 2001).

Before we begin to review the various forms of criminality involving information systems as instruments and / or as targets, and the most appropriate means of controlling them, let us first look at the questions of motivation and of opportunity.

1 Motives and Rationalisations of Computer Criminals

The motives of those who would commit computer-related crime are diverse,
but hardly new. Computer criminals are driven by time-honoured motives, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to taste ‘forbidden fruit’. The ability to make an impact on large systems may, as an act of power, be gratifying in and of itself. The desire to inflict loss or damage on another may also spring from revenge, as when a disgruntled employee shuts down an employer’s computer system, or to ideology, as when one defaces the web-page of an institution that one regards as abhorrent. Much activity on the electronic frontier entails an element of adventure, the exploration of the unknown. The very fact that some activities in cyberspace are likely to elicit official condemnation is enough to attract the defiant, the rebellious, or the irresistibly curious. Given the degree of technical competence required to commit many computer-related crimes, there is one other motivational dimension worth noting here. This, of course, the intellectual challenge of mastering complex systems.

None of the above motives is new. The element of novelty resides in the unprecedented capacity of technology to facilitate acting on these motives.

Alongside motives are the justifications or excuses that offenders will put forward to rationalise or justify their activities. These will, of course, vary with the offence in question but might include blaming the victim (as when one maintains that the CIA deserves to have its website defaced); claiming that the activity was harmless (the hacker who claims to have been just looking, and didn’t take anything); arguing that the victim could afford it (my piracy of Microsoft product won’t effect Bill Gates’ wealth); or suggesting that the practice is so widespread as to be legitimate (everybody takes music off the Web).

Rationalisations in turn may be paralleled by legal defences and, in the event of conviction, evidence in mitigation of sentence. Not all of these rationalisations are believable and, indeed, not all are genuinely believed by the offender. They may include the claim that the offence occurred by accident, it was in furtherance of legitimate research, or resulted from personal stress or from Internet addiction. These and other excuses are discussed more fully in Smith, Grabosky & Urbas (2004).

Increasing Opportunities for Computer-Related Crime

Recent and anticipated changes in technology arising from the convergence of communications and computing are truly breathtaking, and have already had a significant impact on many aspects of life. Banking, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on information technology and telecommunications for their operation. We are moving rapidly to the point where it is possible to assert that ‘everything depends on software’ (Edwards 1995). The exponential growth of this technology, the increase in its capacity and accessibility, and the decrease in its cost, has brought about revolutionary changes in commerce, communications, entertainment, and education. Along with this greater capacity, however, comes greater vulnerability.

Statistics on computer use and connectivity are notoriously evanescent. They are out of date before they appear in print. But the following data give a general sense of the growth and penetration of digital technology in recent years.

Internet use in general and the volume of electronic commerce are increasing exponentially. Worldwide, approximately 605 million people were online as of September 2002, up from 254 million in January 2000. Of that 605 million, roughly 187 million are from the Asia-Pacific region (Nua.com 2002). Internet users worldwide are expected to double to 1.05 billion by 2006.

China had over 45 million regular Internet users as of July 2002, a fourfold increase in little more than two years. Chinese may well become the dominant language on the Internet by the end of this decade.

E-commerce revenue is estimated to reach US$650 million worldwide in 2006, a tenfold increase from 2001, while over this time Asia-Pacific e-commerce will expand over 20 times to US$894 billion (Reuters 2002). By 2005, business-to-business Internet commerce in the Asia-Pacific region will account for 28% of the worldwide total (Pastore 2001).

Not only does the increasing connectivity increase the number of prospective victims of computer-related crime, it also increases the number of prospective offenders. Let us look now at the various forms that cybercrime may take.

■ The Varieties of Computer-Related Crime

The variety of criminal activity that can be committed with or against information systems is quite diverse. Some of these are not really new in substance, only the medium is new. Others represent new forms of illegality altogether. The following generic forms of illegality involve information systems as instruments and / or as targets of crime. They are not mutually exclusive, nor is the following list necessarily exhaustive.
Theft of telecommunications services

The 'phone phreakers' of three decades ago set a precedent for what has become a major criminal industry. By gaining access to an organisation's telephone switchboard (PBX), individuals or criminal organisations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties (Gold 1999). Offenders may gain access to the switchboard by impersonating a technician, by fraudulently obtaining an employee's access code, or by using software available on the Internet. Some sophisticated offenders loop between PBX systems to evade detection. Additional forms of service theft include capturing 'calling card' details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

It has been suggested that up to 5% of total industry turnover has been lost to fraud (Schieck 1995: 2–5; Newman 1998). Costs to individual subscribers can also be significant. In one case, computer hackers in the United States illegally obtained access to Scotland Yard's telephone network and made £620 000 worth of international calls for which Scotland Yard was responsible (Tendler & Nuttall 1996).

A Chinese citizen was jailed for 11 years in March 2002 for fraudulently leasing telephone trunk lines from state-owned Shanghai Telecommunications, then billing US customers for Internet-routed calls to Vietnam. During one week in July 2001, he managed to steal services worth 2.3 million yuan (SCMP 2002).

The proliferation of Internet services has also made them an attractive target for theft. Recently in India, a computer engineer was charged with allegedly stealing 100 hours of Internet time from a client (The Hindú 2000). A number of hackers in Thailand were reported to have succeeded in accessing customer accounts at a Singapore ISP and to have used them freely (BizAsia 2000).

Communications or data storage in furtherance of criminal conspiracies

Just as legitimate organisations in the private and public sectors rely on information systems for communications and record-keeping, so too are the activities of criminal organisations enhanced by technology.

There is evidence of telecommunications equipment being used to facilitate organised drug trafficking, child pornography and terrorism. The use of information technology by Osama bin Laden and his associates was noted months in advance of 11 September 2001 (Associated Press 2001; Kelley 2001). The use of encryption technology may place some criminal communications beyond the reach of law enforcement.

The use of computer networks to produce and distribute child pornography has become the subject of increasing attention. Today, these materials can be imported across national borders at the speed of light (Grant, David & Grabosky 1997). The more overt manifestations of Internet child pornography entail a modest degree of organisation, as required by the infrastructure of IRC and WWW, but the activity appears largely confined to individuals.

By contrast, some of the less publicly visible traffic in child pornography appears to entail a greater degree of organisation. Although knowledge is confined to that conduct which has been the target of successful police investigation, there appear to have been a number of networks that extend cross-nationally, use sophisticated technologies of concealment, and entail a significant degree of coordination.

Illustrative of such activity was the Wonderland Club, an international network with members in at least 14 nations ranging from Europe, to North America, to Australia. Access to the group was password protected, and content was encrypted. Police investigation of the activity, codenamed 'Operation Cathedral' resulted in approximately 100 arrests around the world, and the seizure of over 100 000 images in September 1998.

Information piracy, forgery, and counterfeiting

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed for free distribution, has proved irresistible to many. According to the Straits Times (8 November 1999) a copy of the James Bond film The World is Not Enough was available free on the Internet before its official release.

When creators of a work, in whatever medium, are unable to profit from their creations, there can be a chilling effect on creative effort generally, in addition to financial loss. But the victims of piracy are not always large companies. Musicians, authors and small software developers all suffer. In recent years, one popular Chinese rock band released two CDs, each of which was pirated on the Internet before it was available for legitimate purchase (McDonald 2000). Rampant piracy can stifle the growth of information technology and the economic development on which it is based. It has been
suggested that globally, one in three compact disks (CDs) sold is a counterfeit copy (White House 2000).

The emergence of new technologies such as digital video disks (DVD) creates new opportunities for piracy. An estimated 43 million illegal video CDs and 3.5 million conventional videocassettes were seized worldwide as long ago as 1998 (Europe Information Service 1999).

The following estimates from the Business Software Alliance (BSA) indicates a high prevalence of piracy in some Asian countries.

<table>
<thead>
<tr>
<th>Table 2.1 Top ten countries by piracy rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vietnam</td>
</tr>
<tr>
<td>China</td>
</tr>
<tr>
<td>Indonesia</td>
</tr>
<tr>
<td>Ukraine / Other CIS</td>
</tr>
<tr>
<td>Russia</td>
</tr>
<tr>
<td>Lebanon</td>
</tr>
<tr>
<td>Pakistan</td>
</tr>
<tr>
<td>Bolivia</td>
</tr>
<tr>
<td>Qatar</td>
</tr>
<tr>
<td>Bahrain</td>
</tr>
</tbody>
</table>

Source: BSA 2002, 2003

Digital technology also permits perfect reproduction of documents such as birth certificates or other papers that may be used to construct a false identity for use in a variety of subsequent criminal activities, as well as the counterfeiting of currency and other negotiable instruments. Identity-related crime has become a serious problem around the world, and Southeast Asia is renowned as a centre for document forgery.

**Dissemination of offensive materials**

Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials, racist propaganda, online gambling sites, and instructions for the fabrication of incendiary and explosive devices. What is significant here are the differences across the world in what various sovereign states deem to be offensive. What is treasonous in one country may be celebrated in another; what is blasphemous in one country may fail to raise an eyebrow elsewhere. In Laos, for example, authorities forbid the online promotion of activities that might disturb the peace and happiness of the Lao People's Democratic Republic. This includes distribution of news stories that the government considers harmful or misleading (Nua.com 2000).

The world may in some sense be described as a global village, but differences in values persist. Indeed, there may be profound differences in a single country about what is offensive and what is not. As one might imagine, this will pose significant impediments to international cooperation.

**Stalking**

Telecommunications systems can also be used for harassing, threatening or intrusive communications, from the traditional obscene telephone call to its contemporary manifestation in 'cyber-stalking', in which persistent messages are sent to an unwilling recipient (Ogilvie 2000). Messages may be sent directly by the offender, or the offender may incite others to send the offending communication.

Malaysian Police reported a number of incidents in 2001 where women's personal information had been posted on the Internet. In one case, a man in Malaysia allegedly dialled into a Singapore-based website and posted a sex-for-hire ad that included the telephone number of his estranged wife. She subsequently received obscene telephone calls from Singapore, Thailand and Brazil (Reuters 2001). A similar case in Thailand, in which a man posted the telephone number of a student on a bulletin board, and alleged that she was a prostitute, resulted in a conviction for defamation (ABC News 2002).

One man in Delhi is reported to have logged on to an Internet chat room using the identity of a woman. The offender allegedly used suggestive language, and disclosed the woman's telephone number. She subsequently received harassing telephone calls, one from as far away as Kuwait. The offender was located through the IP address used in contacting the chat room and was subsequently arrested (Duggal 2001).

One former university student in California used e-mail to harass five female students in 1998. He bought information on the Internet about the women using a professor's credit card and then sent 100 messages including death threats, graphic sexual descriptions and references to their daily activities. He apparently made the threats in response to perceived teasing about his appearance (Associated Press 1999). Similar cases have been reported in Hong Kong (Lo 2000).
Extortion

Computer networks may also be used in furtherance of extortion. The Sunday Times (London) reported in 1996 that over 40 financial institutions in Britain and the United States had been attacked electronically over the previous three years. The victims were reported to have paid significant amounts of money to sophisticated computer criminals that threatened to wipe out computer systems (Sunday Times, 2 June 1996). The article cited four incidents between 1993 and 1995 where companies, convinced that the extortionists could crash their computer systems, paid out £42.5 million to avoid the execution of the threat (Denning 1999: 233–4).

One case, which illustrates the transnational reach of extortionists, involved a number of German hackers who compromised the system of an ISP in South Florida, disabling eight of the ISPs ten servers. The offenders obtained personal information and credit card details of 10,000 subscribers and, communicating via electronic mail through one of the compromised accounts, demanded that US$30,000 be delivered to a mail drop in Germany. Cooperation between US and German authorities resulted in the arrest of the extortionists (Bauer 1998).

The Asian region is by no means immune to extortion. One hacker reportedly launched a denial of service attack against a Korean company and demanded 100 million Won to desist. Electronic mail can also be used for sending threatening letters in furtherance of extortion. Early in 2000, a Hong Kong ISP discovered unauthorised alterations to its web-page. It subsequently received a message demanding that several thousand US dollars be deposited in a Russian bank account in order for the attacks to cease (Lo 2000).

Electronic money laundering and tax evasion

For some time now, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains. Legitimately derived income may also be more easily concealed from taxation authorities. It was alleged that nearly US$70 billion has been transferred from Russian banks through the small Pacific island nation of Nauru via the Internet (Seneviratne 2000).

Large financial institutions will no longer be the only ones with the ability to achieve electronic funds transfers transiting numerous jurisdictions at the speed of light. The development of informal banking institutions and parallel banking systems may permit central bank supervision to be bypassed, but can also facilitate the evasion of cash transaction reporting requirements in those nations which have them. Traditional underground banks, which have flourished in Asian countries for centuries, will enjoy even greater capacity through the use of telecommunications. The Asia-Pacific Secretariat of the Financial Action Task Force has advised that increased use of new technologies such as Internet banking and smart cards is making money laundering easier (Infosec.com 1998).

With the emergence and proliferation of various technologies of electronic commerce, one can easily envisage how traditional countermeasures against money laundering and tax evasion may soon be of limited value. I may soon be able to sell you a quantity of heroin, in return for an untraceable transfer of stored value to my ‘smart-card’, which I then download anonymously to my account in a financial institution situated in an overseas jurisdiction which protects the privacy of banking clients. I can discreetly draw on these funds as and when I may require, downloading them back to my stored value card (Wahlert 1996).

Electronic vandalism, and terrorism

As never before, industrial society is dependent on complex data-processing and telecommunications systems. Damage to, or interference with, any of these systems can have catastrophic consequences. Whether motivated by curiosity or vindictiveness, electronic intruders cause inconvenience at best, and have the potential for inflicting massive harm (Schwartzau 1994; Hundley & Anderson 1995; Denning 2000).

While this potential has yet to be fully realised, experience to date gives some indication of the scope of risk. The ‘Melissa’ virus, the ‘Love Bug’ virus (which appears to have originated in the Philippines) and the ‘Anna Kournikova’ virus have disrupted computer systems around the world in recent years. It was reported that about 85% of computers in China were infected with a computer virus during 2003 (BBC 2003). The Sobig.F worm, which struck in August of that year and spread with unprecedented speed, was estimated to have quickly infected one-third of the nation’s computers (Mail Utilities 2003).

The distributed denial of service attacks against Yahoo, Amazon.com and other commercial sites in early 2000 illustrated the vulnerability of systems to the mischief of a mere teenager acting alone. Such attacks not only threaten public confidence in electronic commerce, they also pose risks to nations’ critical infrastructure.
In March 2000, an Indonesian student residing in Australia gained access to a computer in Singapore and altered a number of files. After subsequently relocating to Singapore, he was prosecuted under the Singapore Computer Misuse Act (Tan 2000). In China, financial institutions such as banks and securities firms have also been targeted by hackers (Kwan 1999; Yeang 2001). Authorities there have expressed concern about the vulnerability to hacking of hospital records, with consequent threats to public health (Chan 1998). In September 2002, supporters of the Falun Gong movement were reported to have hacked into a national satellite TV system and disrupted normal programming (Associated Press 2002).

In 1996, intruders were reported to have inserted user IDs of over 100 government officials on a Singapore government website (Goh 1996). In Malaysia, a Perak State government website was hacked into in 1997, giving rise to concerns that changes to website content might create a negative image for the state (New Straits Times 1997). It was reported that the content of Malaysia’s Parliament website was erased late in 2001 (Yeang 2001).

In March 2001, hackers based in South Korea caused the crash of a website at the Japanese Ministry of Education in protest against a newly approved history textbook (BBC 2001). Korean computers were themselves targets of nearly 600 attacks in 1999, approximately half of them originating in foreign countries (McCardle et al. 2000: 12). Recent attacks on websites in Hong Kong, Singapore, Myanmar and Malaysia have also been reported (Goh 1996; Lee 2000; McCardle et al. 2000; Yeang 2001). Long-simmering tensions between India and Pakistan are reflected in a number of recent hacking incidents, and attempts have also been made to disrupt the computer systems of the Sri Lankan government (Associated Press 1998; Joseph 2000).

Readily available programs that break into networks and Internet accounts can be easily downloaded from the Internet. Such technology appears to have been used by 12 youths in Singapore who were arrested for breaking into a website of the University of California in 1997 (LeBlond & Lin 1997).

Defence planners around the world are investing substantially in information warfare — a means of disrupting the IT infrastructure of defence systems (Institute for the Advanced Study of Information Warfare 2001). McCardle and colleagues (2000: 9) report that Chinese military computer systems have been the subject of malicious attack. Whether the intruder is bent on rampant destruction or electronic vandalism, or is merely taking a look around, intrusions and attempted intrusions often occupy the energies of systems administrators.

**Sales and investment fraud**

As electronic commerce becomes more prevalent, the application of digital technology to fraudulent endeavours will be that much greater. The use of the telephone for fraudulent sales pitches, deceptive charitable solicitations, or bogus investment overtures is increasingly common. Online auctions are an increasing source of consumer complaints; in Japan, consumer hotlines reported nearly a threefold increase from 1999 to 2000 (Nikkei Weekly 2001).

In addition, cyberspace now abounds with a wide variety of investment opportunities, from traditional securities such as stocks and bonds, to more exotic opportunities such as coconut farming, the sale and leaseback of automatic teller machines, and worldwide telephone lottery. Indeed, the digital age has been accompanied by unprecedented opportunities for misinformation. Fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously and at minimal cost. In 1999, a man in Australia posted false financial information on the Internet, causing the price of a particular company’s shares on the US NASDAQ to double. The offender sold his own shares in the company at a handsome profit, before the information was repudiated and the price of the shares fell (Australian Associated Press 2000).

Classic pyramid schemes and ‘Exciting, Low-Risk Investment Opportunities’ are not uncommon. The technology of the World Wide Web is ideally suited to investment solicitations. In the words of two staff of the US Securities and Exchange Commission, ‘At very little cost, and from the privacy of a basement office or living room, the fraudster can produce a home page that looks better and more sophisticated than that of a Fortune 500 company’ (Cell & Stark 1997: 822).

As the Internet becomes increasingly a medium of commerce, it will become increasingly a medium of fraud. Japan’s experience of complaints related to online auctions, and of individuals’ credit card details being published on the Internet (Nikkei Weekly 2001) are similar to those of other countries. Trust is the fundamental basis of society and of commerce. If cyberspace becomes widely regarded as a jungle, electronic commerce, and the economic development that depends on it, will suffer.

**Illegal interception of telecommunications**

Developments in telecommunications provide new opportunities for electronic eavesdropping. From activities as time-honoured as surveillance
of an unfaithful spouse, to the newest forms of political and industrial espionage, telecommunications interception has increasing applications. Here again, technological developments create new vulnerabilities. The electromagnetic signals emitted by a computer may themselves be intercepted. Cables may act as broadcast antennas. Existing law may not prevent the remote monitoring of computer radiation.

It has been reported that the notorious American hacker Kevin Poulsen was able to gain access to law enforcement and national security wiretap data prior to his arrest in 1991 (Littman 1997). In 1995, hackers employed by a criminal organisation attacked the communications system of the Amsterdam Police. The hackers succeeded in gaining police operational intelligence, and in disrupting police communications (Rathmell 1997). More recently, the unauthorised access to Microsoft source code in October 2000 indicates the vulnerability of companies to industrial espionage (Associated Press 2000).

**Electronic funds transfer fraud**

Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited. In 1999, seven Hong Kong teenagers were arrested for using stolen credit card numbers on the Internet to purchase computer products worth more than HK$1 million (Lo 1999). In Malaysia, criminals attached a device to an ATM and captured credit card and PIN details for use in counterfeiting credit cards (Datatime 2000). Hackers broke into a leading Thai retail website, stole the credit card information of 2000 customers, and posted it on the Internet (McCordie et al. 2000: 10). More recently, Japanese Internet users are reporting that their phone and credit card numbers are being published on the Internet, making them even more vulnerable to criminal exploitation (Nikkei Weekly 2001).

A decade ago, the financial controller of a Hong Kong company made false computer entries and shifted HK$2.6 million in company assets to his personal accounts (Cook 1993). In Singapore that year, counterfeit ATM cards were used to steal about S$95,000 (Tan 1994). According to one report, a bank in Singapore was defrauded of A$18.7 million over the course of two years between 1995 and 1997 (Leung 1999). It has been suggested that the assets of the national bank of a small country in the Asia-Pacific region came close to being the subject of an illicit electronic transfer. Individuals too can suffer. One customer of a Hong Kong bank lost up to HK$900,000 stolen from online accounts (Bowman 2001). The European Union Bank, which operated exclusively on the Internet, collapsed in 1997 leaving depositors stranded.

In December 1998, two brothers in China manipulated a bank's computer to transfer US$31,000 into their accounts (Yeung 2001). In January 2001, two Indian IT specialists were arrested allegedly attempting to hack into the information systems of the State Bank of India (Bloomberg News 2001). Similar cases have been reported elsewhere in Asia.

The above forms of computer-related crime are not necessarily mutually exclusive and need not occur in isolation. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy. Computer-related crime may be compounded in nature, combining two or more of the generic forms outlined above. The various activities of Kevin Mitnick, as described in Halter & Markoff (1991) are illustrative.

In addition, a number of themes run through each of these forms of illegality. Foremost among them are technologies for concealing the content of communications. Encryption technologies can limit access by law enforcement agents to communications carried out in furtherance of a conspiracy, or to the dissemination of objectionable materials between consenting parties (Denning 1999).

Also important are technologies for concealing a communicator's identity. Electronic impersonation, colloquially termed 'spoofing,' can be used in furtherance of a variety of criminal activities, including fraud, criminal conspiracy, harassment, and vandalism. Technologies of anonymity further complicate the task of identifying a suspect (Fromkin 1993).

Beyond the aforementioned reluctance of victims to report, the technologies of secrecy and anonymity noted above often make detection of the offender extremely difficult. Those who seek to mask their identity on computer networks are often able to do so, by means of 'looping' or 'weaving' through multiple sites in a variety of nations. The Hong Kong extortion case noted above involved messages transiting sites in Canada, France and the United States (Lo 2000). Anonymous remitters and encryption devices can shield one from the scrutiny of all but the most determined and technologically sophisticated regulatory and enforcement agencies. Some crimes do not result in detection or loss until some time after the event. Considerable time may elapse before the activation of a computer virus, or between the insertion of a 'logic bomb' and its detonation.
The Size of the Problem

The cost of cyber-crime

The task of accurately estimating the cost of cyber-crime is futile. Monetary estimates of the cost of computer-related crime should be regarded as broadly indicative at best. First, a great deal of computer-related crime never reaches official attention. Victims may be unaware that they have become victims, or may for a variety of reasons choose to keep their misfortune to themselves. For example a business, which falls victim to a form of electronic fraud, may conclude that the immediate financial loss would be outweighed by the damage to its commercial reputation, should its misfortune become public knowledge. Moreover, the likelihood of recovering its losses may be minimal. In addition, there may be a concern that publicising a successful crime may encourage imitative or 'copy cat' behaviour. So it is that an unknown but presumably very large proportion of computer-related crime never reaches official attention in the first place.

Of those incidents that do reach official attention, law enforcement agencies may be disinclined to take further action or may lack the capacity to do so. Because the definitional boundaries of what constitutes cyber-crime, and how it might be counted, will vary across jurisdictions, there can be no standard statistical database on known offences.

In addition, there may also be temptations on the part of various interests to either overstate or understate the volume and the seriousness of computer-related crime. Those perpetrators of computer-related crime who are given to boasting may seek to exaggerate their exploits. Victims may be tempted to inflate the extent of their losses in order to lobby for stricter laws and penalties. Moral entrepreneurs who object to specific types of online content may seek to overstate the nature and the severity of the content in question. Law enforcement agencies seeking greater powers or material resources may be inclined to invoke the spectre of catastrophe. And purveyors of information security products and services may wish to increase the size of their market.

This is not to suggest that computer-related crime is a non-problem. Rather, estimates that one does encounter from time to time should not be accepted uncritically, and certainly should not be given the status of absolute truth. And there are some adverse impacts of computer-related crime, such as violations of privacy, which are arguably unquantifiable.

Those offences that are detected can be difficult to cost. It may be instructive to look at cost on three dimensions. There can be direct out-of-pocket losses sustained by victims; costs in lost productivity while systems are 'down'; costs involved in repairing and securing information systems which have been subject to attack; and the costs of economic opportunities forgone when individuals avoid e-commerce because of lack of trust. Some of these losses are more readily measurable than others.

According to the BSA, Asia-Pacific regional dollar losses due to software, music and data piracy increased from US$4.1 billion in 2000 to more than US$4.7 billion in 2001, accounting for almost half of the revenue losses worldwide. The industry is quick to note that the economic costs of piracy also include lost jobs, smaller tax revenues, and lower economic growth (BSA 2003b).

Data from just one country are illustrative of the magnitude of the problem. In August 2000, a Malaysian Copyright Task Force raided a factory, seizing 100 CD stampers, 200 000 counterfeit CDs and 20 PCs, worth an estimated US$480 million (Smith & Ubars 2001: 58). This is by no means a recent phenomenon. In the ten years before 1996, an estimated RM 888 569 in pirated goods was seized in Malaysia (Farinordin 1996).

Estimates of job losses attributable to piracy will vary from country to country. The Malaysian government has recognised that the Malaysian software industry and the development of its Multimedia Super Corridor (MSC) would be threatened by uncontrolled counterfeiting (Kasim 1996). Industry estimates of the costs of software piracy in Malaysia in 1996 were RM 92 million (Farinordin 1996).

Estimates suggest that the economic impact of virus attacks on information systems around the world amounted to US$12.1 billion in 1999 and US$17.1 billion in 2000 (Business Wire 2000; Computer Economics 2002). The person who pleaded guilty to releasing the Melissa virus of 1999 admitted to causing US$80 million in damage, the highest point on the scale of United States sentencing guidelines. Estimates of the full losses attributable to the Melissa virus ranged up to US$393 million in lost productivity (Bloomberg News 1999).

The distributed denial of service attacks against Yahoo and Amazon.com in February 2000, apparently the work of a lone Canadian teenager, illustrate the damage that can be inflicted by concerted effort. The Yahoo site was offline for approximately three hours, depriving users of services and costing the company from US$200 000 to US$500 000 in lost revenues from advertising and sales (Krochmal 2000; see also http://www.cicsa.net/html/communities/ddos/index.shtml).

The 'I Love You' virus released from the Philippines in May 2000 may have entailed lost productivity amounting to billions of dollars around the
world. It was estimated that two-thirds of the Fortune 500 companies took their mail servers down at the time (Masterson 2000).

But quantification can still be deceptive. What appears to be a trivial matter may in fact be the tip of a very big iceberg. A classic illustration was provided by Stoll (1991) whose pursuit of a US$0.75 accounting error in a computer account led to the discovery of an international espionage ring.

Some attempts are being made to develop a systematic overview of the incidence of crime in cyberspace. Surveys are conducted periodically by major accounting firms, and by specialised organisations such as the Computer Security Institute in the United States. Turnbull (2000) reports the results of a recent survey that found a third of companies in Hong Kong had detected security breaches in the previous 12 months. National and multinational organisations are also moving to establish databases of risks and remedies.

The International Chamber of Commerce (ICC) has opened a new division to assist 7000 member companies around the world to protect themselves against computer-related crime. In addition to identifying how and where attacks occur, the chamber seeks to provide security information to members. The new ICC cyber-crime unit is developing a database on criminal activities in cyberspace, and will facilitate information exchange between the private sector and law enforcement (ICC 2001).

There are, however, more hidden costs. To the extent that every legitimate move one makes in cyberspace is potentially traceable, this can have a chilling effect on individual expression, and may discourage full use of digital technology.

Privacy

Digital technology poses significant threats to personal privacy. Whether by accident or by design, personal details may become accessible to the world, or to particular institutions or individuals that one would prefer remain ignorant of one's affairs. And governmental responses to cyber-crime may themselves jeopardise privacy.

In 1998, a hacker broke into the computer network of a Japanese company, and published the names, bank account numbers, and other personal details of the company's customers on a website (Daily Yomiuri 2000).

Governments have always been inclined to encroach on individual privacy.

Today, law enforcement and security agencies around the world are seeking and obtaining greater powers to intercept electronic communications in democratic societies where the rule of law tends to prevail, these powers are generally subject to a degree of judicial oversight. In Great Britain, the Regulation of Investigatory Powers Act (RIPA) provides for monitoring and interception of electronic mail. In the United States, a system called 'carnivore' assists the scanning and capture of e-mail packets. In addition, a globally integrated communications intelligence system known as 'ECHELON' operated by the United States, Great Britain, Canada, Australia and New Zealand, permits the systematic collection and analysis of telecommunications content (Campbell 1999, 2000; Whitaker 1999).

Governments have been joined, if not surpassed, by large commercial organisations that would exploit, legally or otherwise, the increasing volume of personal details that accumulate in cyberspace. The use of a credit card for purchases now leaves an electronic trail. Technologies of data manipulation that permit merging of databases and matching of individual identities now facilitate the aggregation of data from disparate sources (Clarke 1998). The term 'data mining' is commonly used to refer to such practices. The linking of disparate data is facilitated by the existence of identification numbers, which are common in most industrial societies; the nine-digit Social Security Number in the United States is a classic example. Through the collation of disparate personal details, the whole becomes greater than the sum of its parts.

Technologies may facilitate electronic eavesdropping by individuals as well. A recently identified but commonly available technology allows the originator of an e-mail message to see what the recipient wrote when it is forwarded on to another user. A few lines of JavaScript can be embedded in an e-mail message and thereby direct the recipient's mail to be returned to the original sender. It only works, however, if the recipient's e-mail program is set to read JavaScript (Evans 2001).

Of course, a great deal of personal information may be disclosed by accident. Medical records of thousands of patients have appeared on the Internet (Grabosky, Smith & Dempsey 2001: Ch. 10). Whether at the hands of the government or the private sector, by design or by blunder, the loss of one's private life is often accompanied by a decline in spontaneity, creativity, and a diminished sense of self.

Lost productivity

The unauthorised use of IT resources by the employees of both public and private sector organisations can entail significant losses in productivity. Whether the errant employee engages in behaviour as relatively innocuous
as sending personal e-mail or reading the newspapers, or in conduct more questionable such as visiting pornographic sites on the Web, this may be regarded as theft of an employer's time. One company, for example, analysed the websites visited by its employees and found that 20 people had visited more than 1000 sexually explicit sites each in less than a month. Another company found that 15% of websites visited by its employees contained sexually explicit material. In a survey of executives conducted by PC World, 20% of the 200 companies surveyed had disciplined staff for misusing Internet access; the most common offences involved visits to pornographic websites, shopping, using chat lines, gambling, and downloading illegal software (Denning 1999: 360-1).

The epidemic of unsolicited commercial e-mail, colloquially referred to as 'spam,' has taken a significant toll. According to one estimate, spam accounts for 15 billion e-mail messages per day, and some US$20 billion in lost productivity per year (Blackman 2003).

The costs of controlling cyber-crime

At the outset, it is important to recognise that cyber-crime has no universal definition. What is, and is not, cyber-crime varies over time and space, depending on what the authorities in a given jurisdiction define as criminal. And so the cost of controlling cyber-crime will be a function of what authorities in a given country define as cyber-crime. A country, which defines online depictions of naked people as criminal, is likely to devote more resources to the suppression of this content than one that does not.

Among the considerations that may contribute to a nation's priorities for cyber-crime control will be the capacity of state law enforcement or regulatory agencies, and the existence and capacity of quasi-regulatory institutions that exist outside the public sector. These might include the software and publishing industries, telecommunications carriers and ISPs, those who deal in IT security products and services, and concerned citizens. In some countries there may be institutions in the private sector with the capacity to prevent, detect and investigate computer-related crime. Indeed, the expertise residing within these organisations may exceed that which exists within law enforcement agencies.

The cost of securing the national infrastructure and of providing a safe and secure platform for electronic commerce — the costs of preventing cyber-crime — may be formidable, but the costs of inaction will be even greater.

The limited availability of law enforcement resources in the face of the widespread threat of cyber-crime means that states will be required to determine:

- What kinds of behaviour in cyberspace should even attempt to control
- The amount of resources they choose to devote to policing cyberspace
- The burdens they wish to impose on non-state actors by enlisting them for co-production or devolving responsibility on them for self-defence

Some governments may be tempted to share the burden of policing cyberspace by sharing or delegating responsibility to other institutions or interests. This raises the question of who ultimately will bear the cost of this co-production. Internet service providers, for example, may be asked to retain detailed records of their subscribers' transactions for an indefinite period. Because this would require considerable storage space, it would significantly increase the cost of providing Internet services. This cost would either be prohibitive for the ISP, or passed on to the consumer of Internet services. In any event, this could significantly limit the citizen's uptake of digital technology. The Netherlands recently imposed legal requirements on its ISPs to install expensive network-monitoring equipment. An estimate of the cost for a medium-sized ISP was around US$600,000, and an increase in the cost of Internet access of up to 25% (Evers 2000). China requires Internet cafés to install software to block restricted websites and record user activities (BBC 2002).

The responsibility for exercising some degree of control in cyberspace can be shared with other traditional institutions in society. Parental supervision of their children's online activities may be a more feasible strategy than state surveillance. In addition, there may well be market solutions, in the form of information security technology, which can contribute to the enhancement of security and prosperity in cyberspace.

Some governments may respond to some manifestations of cyber-crime in the belief that they can eliminate it completely. Other governments, recognising that their powers are not unlimited, may respond in a manner that creates a hostile climate for the target behaviour, and thereby achieve partial success. Other governments will respond symbolically, with verbal denunciation but no enforcement activity. The challenge facing societies today is to exploit the benefits of digital technology while minimising the downside risk.
The Challenge of Controlling Computer-Related Crime

Controlling contributing factors

Motives

Recall from the earlier discussion that crime can be explained in part in terms of the supply of motivated offenders. Motives, whether on the part of individuals or in the aggregate, are very difficult to change. Training in computer ethics is important, but its impact will be marginal at best. For this reason, the most strategically advantageous approaches to computer-related crime will be concerned with the reduction of opportunities, and with the enhancement of surveillance.

Opportunities

The most effective way of eliminating opportunities for online crime is simply to pull the plug. This is, of course, unrealistic; the affluent nations of the world are now highly dependent on information technology. For the poorer nations, IT is probably a necessary, if not sufficient, path to economic development. Thus the challenge lies in managing risk so as to achieve the maximum benefits that flow from new technologies, while minimising the downside. A merchant could scrutinise every credit card transaction so as to drastically reduce the risk of fraud, but in the process drive away legitimate customers. At a higher level, nations around the world are in the process of forging policies on where to draw the line on such fundamental questions as the balance between the citizen’s privacy and the imperatives of law enforcement, and freedom of expression versus the protection of certain cultural values.

There are many technologies, which reduce the opportunity to commit computer-related crime. Given that so much computer-related crime depends on unauthorised access to information systems, access control and authentication technologies have become essential. Sophisticated advice and products for computer crime prevention are provided by one of the world’s growth industries of today, namely computer security.

Denning (1999) offers a comprehensive inventory of technologies for reducing opportunities for computer crime. She describes technologies of encryption and anonymity, which permit concealment of the content of communications (such as a consumer’s credit card details), or of the identity of the communicator (not all participants in discussion groups on reproductive health wish to disclose their identities). Denning also outlines technologies of authentication, from basic passwords, to various biometric devices such as fingerprint or voice recognition technology, and retinal imaging, which greatly enhance the difficulty of obtaining unauthorised access to information systems.

Surveillance

The third basic factor that contributes to computer-related crime is the absence of adequate surveillance. Capable guardianship has evolved over human history from feudalism, to the rise of the state and the proliferation of public institutions of social control, to the post-modern era in which employees of private security services vastly outnumber sworn police officers in many industrial democracies.

Technology can also enhance surveillance. Denning (1999) describes various technologies for detecting attempted intrusions into information systems. Alarms can indicate when repeated login attempts fail because of incorrect passwords, or when access is sought outside of normal working hours. Other anomaly detection devices will identify unusual patterns of system use, including atypical destination and duration of telephone calls, unusual spending patterns using credit cards.

Market forces can also enhance surveillance. A market is currently emerging for ISPs specialising in content suitable for family consumption, guaranteed to be free of sex, violence, and vilification.

Market forces may also generate second-order controlling influences. As large organisations begin to appreciate their vulnerability to electronic theft and vandalism, they may be expected to insure against potential losses. It is very much in the interests of insurance companies to require appropriate security precautions on the part of their policyholders. Indeed, decisions to under and price insurance may well depend on security practices of prospective assureds. Subcontractors may also be required to have strict IT integrity programmes in place as a condition of doing business.

Citizen co-production can complement activities undertaken by agencies at the state. Grassroots concern about the availability of undesirable content has given rise to the private monitoring and surveillance of cyberspace. In the Asia-Pacific region, an NGO website known as ‘Kids.ap’, supported by UNESCO, contains information that aims to eradicate child pornography and
the activities of child molesters via the Internet. http://www.kidsap.org/ (visited 14 April 2001). And the motion picture, music and software industries have developed considerable capacity to detect piracy, to assist governments in investigation and prosecution, and to undertake private civil action against offenders. The policing of terrestrial space is now very much a pluralistic endeavour, and so too is the policing of cyberspace. In cyberspace today, as on terrestrial space two millennia ago, the first line of defence will be self-defence — in other words, minding one’s own store.

**Legislative issues**

It is becoming increasingly apparent that the economic well-being of nations depends on their integration into the global economy. As cyberspace becomes the dominant medium for commerce, it becomes increasingly important that there be a secure legal platform for electronic commerce.

For any jurisdiction to protect itself against computer-related crime, a basic legislative foundation is required. This will involve the substantive criminal law, the law of search and seizure, and the law of evidence. Because of the global nature of cyberspace and the transjurisdictional nature of much computer offending, a degree of harmony and consistency, if not uniformity, is desirable across nations.

The laws of some countries are relatively elastic, able to embrace new circumstances without having to be amended. Other legal systems are quite rigid, necessitating amendment for new forms of crime. In the common law world, for example, fraud means obtaining something of value by means of deception. Deception entails the involvement of the mind of a human victim. Where fraud is carried out against an electronic system (such as an ATM), new legislation may be necessary. Similarly, the law of theft or damage in some countries may extend only to tangible items. That is, it may not be a crime to steal or to damage property in digital form.

Most basically, the substantive criminal law should provide for the following:

- Unauthorised access to a computer or computer system
- Interference with lawful use of a computer or a computer system
- Destruction or alteration of data within a computer system
- Theft of intangible property
- Obtaining value by deception (including electronic systems).

Similarly, the laws of evidence and procedure should accommodate search and seizure in an electronic environment, and should permit the admissibility of electronic evidence in judicial proceedings.

Jurisdictions such as Hong Kong have undertaken systematic reviews of their legislative requirements with respect to the prevention and control of computer-related crime (Hong Kong Security Bureau 2000).

**Extra-territorial issues**

One of the more significant aspects of computer-related crime is its global reach. While international offending is by no means a uniquely modern phenomenon, the global nature of cyberspace significantly enhances the ability of offenders to commit crimes in one country that will affect individuals in a variety of other countries. This poses great challenges for the detection, investigation and prosecution of offenders.

Two problems arise in relation to the prosecution of telecommunications offences which have an inter-jurisdictional aspect: first, determination where the offence occurred so it can be decided which law to apply and, second, obtaining evidence and ensuring that the offender can be located and tried before a court. Both these questions raise complex legal problems of jurisdiction and extradition (see Lanham et al. 1987; Tan 2000). If an online financial newsletter originating in the Bahamas contains fraudulent speculation about the prospects of a company whose shares are traded on the Tokyo Stock Exchange, where has the offence occurred?

Even if one is able to decide which law is applicable, further difficulties may arise in applying that law. In a unitary jurisdiction, such as Singapore, where there is one law and one law enforcement agency, determining and applying the applicable law is difficult enough. Criminal activities committed across the globe, however, pose even greater problems. Sovereign governments are finding it difficult to exercise control over online behaviour at home, not to mention abroad. A resident of Bangkok who falls victim to a telemarketing scam originating in Albania, for example, can expect little assistance from law enforcement agencies in either jurisdiction. As a result, regulation by territorially based rules may prove to be inappropriate for these types of offences.

Extraterritorial law enforcement costs are also often prohibitive. The time, money and uncertainty required by international investigations and, if successful, extradition proceedings, can be so high as to preclude attention to all but the most serious offending. Moreover, the cooperation across international boundaries in furtherance of such enforcement usually requires
a congruence of values and priorities that, despite prevailing trends towards globalisation, exists only infrequently.

Other issues which may complicate investigation entail the logistics of search and seizure during real time, the sheer volume of material within which incriminating evidence may be contained, and the encryption of information, which may render it entirely inaccessible, or accessible only after a massive application of decryption technology.

Traditionally, the jurisdiction of courts was local. That is, courts could only entertain prosecutions in respect of offences committed against local laws where there existed a sufficient link between the offence and the jurisdiction in question. There is, however, always the possibility that legislatures will confer extraterritorial jurisdiction for some crimes. Some common examples include offences committed on the high seas, counterfeiting offences, crimes committed by members of the defence forces, and, recently in Australia and elsewhere, sexual relations between Australians and children overseas who are under 16 years of age.

In rare circumstances, a nation's laws may apply to acts committed overseas by foreign nationals. Recent war crime prosecutions in Australia involved defendants resident elsewhere at the times the alleged offences were committed. These circumstances are, to say the least, most unusual. But in a shrinking world where the financial burdens of extradition are unlikely to decline, they may become more common.

To the extent that international computer-related crime is amenable to international enforcement, it will require concerted international cooperation. Past performance in the context of other forms of criminality would suggest that this cooperation is unlikely to be forthcoming except in the relatively infrequent types of illegality where there is widespread international consensus about the activity in question (such as child pornography, or fraud on a scale likely to destabilise financial markets), and about the desirability of suppressing it. In many instances, extradition is likely to be more cumbersome the greater the cultural and ideological distance between the two parties. At the best of times, international extradition can be expensive.

There are nonetheless examples of extradition between countries following successful investigation of computer crime. In January 2000, Canadian authorities returned a suspect in a fraud case to officials of the Public Security Bureau in Beijing (People's Daily Online, 2000). In August 2001, Thai authorities agreed to a US request to commence extradition proceedings against a US national, but reserved the right to prosecute him first after discovering child pornography downloaded from the Internet in his possession (Bangkok Post 2001).

Even so, this would assume a seamless world system of stable sovereign states; such a system does not exist today, nor is it likely to exist in our lifetime. Law enforcement and regulatory vacuums exist in some parts of the world, certainly in those settings where the state has effectively collapsed. Even where state power does exist in full force, the corruption of individual regimes can impede international cooperation.

Nevertheless, some excellent progress has been made in furtherance of international harmonization of laws relating to computer crime and its investigation. For an example of movement toward consistency in legislative response, one may look to the Council of Europe's Draft Convention on Cybercrime. This draft convention contains general sections relating to the substantive criminal law, search and seizure of electronic data, jurisdiction, and mutual assistance. Measures to be taken at national level with regard to the substantive criminal law included the adoption of measures to criminalise illegal access to computer systems; illegal interception of, or interference with, data; the production, sale or procurement of 'hacking' tools or software; computer-related fraud and forgery; offences relating to child pornography; and offences relating to copyright infringement. http://conventions.coe.int/ (visited 8 October 2000).

In addition, the work of the United Nations (including its affiliated Institutes such as UNAFED), the G8, the OECD, the Council of Europe and Interpol are other examples of international cooperation. In our region, one may look to the Interpol Asia and South Pacific Regional Working Party of IT crime, established in 1995.

Such international efforts at capacity building are essential for, issues of trans-border criminality aside, many law enforcement agencies as we know them lack the capacity on their own to control computer-related crime which occurs entirely within their own jurisdiction. This arises from a number of factors, not the least of which is resource constraint. In most countries around the world, police are being asked to do more with less. The broad sweep of the criminal law and the abundance of criminal activity mean that police must often choose which matters to pursue and which to ignore. This is even more the case with transnational electronic crime than it is with domestic offending.

Another fundamental issue, at least at the present historical moment, is the difficulty faced by police services around the world in retaining expert computer crime investigators. Very attractive opportunities exist in the private sector for persons with forensic computing skills. A competent police officer may well be able to double or triple his or her salary in the private sector, whether working for one of the big multinational accounting firms or for a large financial institution. Whether this 'brain drain' will continue indefinitely,
or slow down as the supply of highly computer literate individuals in both public and private sectors catches up with demand, remains to be seen. For the time being, however, police will not be able to go it alone. They will remain dependent on private and non-profit institutions to help combat crime in cyberspace.

In general, this division of labour will include elements of self-protection by prospective victims of telecommunications-related illegality; market-based commercial solutions; self-regulatory initiatives by the targets of regulation; traditional law enforcement or regulatory intervention by the state; and third party 'co-production' of surveillance by private individuals and citizens’ groups.

**Conclusion**

Total control of cyber-crime may be achievable, but only at great cost. Most new technologies are accompanied by a downside risk. The advent of the internal combustion engine has led to millions of deaths and injuries, and massive property damage, not to mention deterioration in environmental quality. The advent of the telephone has greatly enhanced the efficiency of communications among criminals and the photocopyer made counterfeiting and forgery easier. Our response has been not to forgo or to discard these technologies but rather to regulate their use or to design them in a manner that will reduce their exploitation for criminal purposes.

So we build safer cars, with cleaner engines. We design safer roads, and impose speed limits, which we employ police to enforce. In so doing, we accept that these solutions will not be perfect. We seek an optimal solution, one that would maximise the benefits and minimise the costs.

Every country must decide for itself what kind of future it seeks, and what kinds of behaviours are acceptable. In these undertakings, contradictions and tradeoffs are inevitable. For the most part, prosperity is very difficult to achieve without a degree of economic freedom. Conversely, state control over the economy and information is difficult, if not impossible to achieve without sacrificing a degree of prosperity.

The control of computer crime is about tradeoffs. The reduction of opportunities to commit cyber-crime, if carried out solely through the curtailment of connectivity, would be counterproductive. Where the economy is not already linked with global forces, it will become increasingly so. ‘Pulling the plug’ will only impede commerce. The Hong Kong Inter-Departmental Working Group on Computer-Related Crime observed the risk of overkill that can arise from excessive regulation of information technology in a free market economy (Hong Kong Security Bureau 2000). Responsibilities for the control of computer crime will be similarly shared between agents of the state, information security specialists in the private sector, and the individual user. In cyberspace today, as on terrestrial space two millennia ago, the first line of defence will be self-defence — in other words, minding one's own store.