

Thomson Reuters (Professional) Australia Limited
100 Harris Street Pyrmont NSW 2009
Tel: (02) 8587 7000 Fax: (02) 8587 7100
LTA.Service@thomsonreuters.com
www.thomsonreuters.com.au
For all customer inquiries please ring 1300 304 195
(for calls within Australia only)

INTERNATIONAL AGENTS & DISTRIBUTORS

NORTH AMERICA
Thomson Reuters
Eagan
United States of America

LATIN AMERICA
Thomson Reuters
São Paulo
Brazil

ASIA PACIFIC
Thomson Reuters
Sydney
Australia

EUROPE
Thomson Reuters
London
United Kingdom

Crime and Justice A Guide to Criminology

Fourth Edition

Edited by

**Marinella Marmo
Willem de Lint
Darren Palmer**

Lawbook Co. 2012

Published in Sydney by

Lawbook Co.
100 Harris Street, Pyrmont, NSW

First edition (Goldsmith, Israel, Daly (eds)) 1996
Second edition (Goldsmith, Israel, Daly (eds)) 2003
Third edition (Goldsmith, Israel, Daly (eds)) 2006

A Cataloguing-in-Publication entry is available upon request from the National Library of Australia.

© Thomson Reuters (Professional) Australia Limited 2012

This publication is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Inquiries should be addressed to the publishers.

All legislative material herein is reproduced by permission but does not purport to be the official or authorised version. It is subject to Commonwealth of Australia copyright. The *Copyright Act 1968* permits certain reproduction and publication of Commonwealth legislation. In particular, s 182A of the Act enables a complete copy to be made by or on behalf of a particular person. For reproduction or publication beyond that permitted by the Act, permission should be sought in writing. Requests should be submitted online at www.ag.gov.au/cca, faxed to (02) 6250 5989 or mailed to Commonwealth Copyright Administration, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600.

Editor: Lara Weeks
Product Developer: Helen Sheridan
Publisher: Robert Wilson

Typeset in Stone Sans and Times Roman, 101/2 on 12 point,
by Midland Typesetters, Australia

Printed by Ligare Pty Ltd, Riverwood, NSW



The paper this book is printed on is in accordance with the rules of the Forest Stewardship Council®. The FSC® promotes environmentally responsible, socially beneficial and economically viable management of the world's forests.

Foreword

Professor Duncan Chappell
*Institute of Criminology, University
of Sydney*

What a difference half a century makes in the life of a criminologist. As I dipped into the pages of this book I was smitten by thoughts of envy at the dazzling array of information it contains about crime and justice. With this book in hand aspiring contemporary students of criminology, as well as veterans in the field, have at their immediate disposal a veritable 'criminological Wikipedia'. Twenty nine tightly written chapters, bolstered by thought provoking questions for discussion in classroom and allied settings, range in content from philosophical queries concerning the nature of crime to the analysis of specific types of criminal conduct and the way in which each is dealt with by the criminal justice system. There is also a vast list of reference material for those who wish to explore any subject more fully, together with a helpful guide about how best to access these resources.

So why my envy? Well more than 50 years ago when I first became interested in studying criminology virtually none of the reference material mentioned in the book existed, nor was there any equivalent criminological text to use as a teaching and information tool. My own initial fascination about the field was undoubtedly influenced by growing up in Tasmania surrounded by constant reminders of our convict past. I can still recall as a child sharing family picnics amidst the ghost ridden ruins of Port Arthur. Later, as an articled law student, I also remember interviewing clients in the old Hobart gaol, long since demolished, which dated back to the convict era.

In my academic studies for an Arts Law degree at the University of Tasmania scant mention was made of this aspect of Tasmanian history. Criminology was not part of the syllabus in my criminal law class and the nearest I came to discussing penology was probably in my English literature class where we read Marcus Clarke's *For the Term of His Natural Life* – a novel first published in 1874 which contains graphic accounts of the brutal system of transportation

of convicts from England to Van Diemen's Land during the early days of white settlement of the nation.

It is rather a shame that no chapter in the present book is devoted entirely to the historical evolution of our contemporary Australian criminal justice system although both Darren Palmer in his chapter on Police and Law Enforcement and Martin Brown in his contribution on Imprisonment and Detention make mention of the way in which our history has shaped the nature and structure of our policing and correctional systems. While there are obviously very dark pages attached to this history, as illustrated in Robert Hughes epic account of our development as a British penal colony in his book *The Fatal Shore* (1987), there are also some more positive stories to be told about this period including the beginnings of the system of parole through the 'ticket of leave' which gave well behaved convicts the opportunity to work in the community, and the linked and successful rehabilitation of thousands of these offenders transported over many decades to the Antipodes from Britain. In my view modern students of criminology should be reminded of this past in order to appreciate more fully how deeply entwined our development as a nation has been influenced by crime and justice issues.

It was not until I reached the University of Cambridge in the early 1960's that I became exposed to the true world of criminology as it then existed. That world was still relatively restricted in the sense that the Cambridge Institute of Criminology where I studied, led by Professor Leon Radzinowicz, was newly established and the fledgling discipline was struggling to gain a foothold in the academic marketplace. When I returned to Australia at the end of 1965 to start teaching criminal law and criminology at the Law School at the University of Sydney I was still only the second person to have graduated with a doctorate from the Cambridge Institute.

As a neophyte law lecturer I encountered the immediate problem of finding appropriate reference material for students in my criminology classes. In reality there were no Australian criminology texts available at that time and local research activity in the field was still in its infancy. It was not until 1968 that the first issue of the *Australian and New Zealand Journal of Criminology* appeared in print, and 1972 when the first edition was published of the *Australian Criminal Justice System* which I co-edited with my colleague and friend Paul Wilson. Both of these publications began the process, which continues today, of building up the 'local content' of Australian criminology.

As this new edition of *Crime and Justice: A Guide to Criminology* (CJGC) vividly demonstrates that local content is now prolific and emanates from a broad range of scholarly and allied sources. Perhaps this is nowhere better shown than in the massive expansion that has occurred in the gathering, dissemination and interpretation of official statistical and allied data about crime and criminal justice matters. This topic forms the substance of Chapter 2 of CJGC, written jointly by Frank Morgan and Joseph Clare of the University of Western Australia. As Morgan and Clare so aptly state:

'[M]easuring crime can be a very tricky business. Official crime statistics in some instances (e.g. homicide or motor vehicle theft) give us a good guide both to the total volume of crime and trends in its incidence..... In yet other instances, however, official crime statistics tell us more about complex institutional responses to crime than they do about crime itself' (CJGC 2:30).

Morgan and Clare's comment jolted my own memory of a personal story about just how tricky it can be as an academic to become involved in the world of measuring crime. Returning for a moment to the 1960's, a time when crime statistics in this country were extremely limited and primitive, I wrote an Op-ed piece for the *Sydney Morning Herald*. In my piece I examined police statistics of reported and cleared serious crimes in New South Wales (NSW) and Victoria. A comparison showed that the NSW police were reporting one half the number of serious crimes recorded in Victoria while claiming a clear up rate that was double that of their southern counterparts. I suggested that either the NSW police were among the finest in the world in both deterring and solving crimes, or that something else was going on within the respective forces in the way in which they gathered, recorded and published data about serious crime.

My Op-ed piece was not well received in official quarters. Within hours of its appearance in print I was summoned to the office of the then Dean of the Law School and informed by him that he had just received a call from the NSW Police Commissioner complaining that my article had unjustly and unfairly criticised the NSW Police Force – a force which had a fine and enviable record of detecting and prosecuting crime. The Dean indicated that if I wished to have a successful and prosperous future in academia I should desist from writing such pieces in the press.

I would hope that in contemporary times academic advice of this type would not be proffered but there is no doubt that the handling of crime statistics can still be a hazardous process for the police themselves, and for those who seek to use and interpret them. As some readers will no doubt recall during the 2010 Victorian State Election the issue by Victorian police of what were said to be misleading crime statistics became a matter of some political controversy. A subsequent investigation of the matter by the State's Ombudsman exposed widespread flaws in the collection and publication of crime data by Victoria Police (Ferguson: 2011) and led in part it would seem to the subsequent decision of the then head of the police force to resign (Dunckley: 2011). It is interesting to note that in most other Australian jurisdictions the police have largely been removed from the process of producing their own statistics through the establishment of more independent and specialised organisations like the NSW Bureau of Crime Statistics and Research (BOCSAR). Bodies like BOCSAR, and the Australian Institute of Criminology and Australian Bureau of Statistics at the national level, have done much in recent decades to de-politicise the dialogue about the state

of crime in the nation although as the chapter on Crime and the Media by Stephen Moston and Garry Coventry reminds us we are still afflicted as a society by media driven moral panics and law and order based diatribes.

Drawing individual attention to the content of each of the 29 chapters contained in this latest edition of CJGC is well beyond the remit of this Preface. Mention should be made, however, that this edition contains six new chapters dealing respectively with environmental crimes, state crimes, international crimes, new explanations for crime, forensic criminology, and criminal justice and human rights. Each of these topics clearly merits a place in the book, and especially that of international crimes. The chapter on this subject, written by Grant Niemann and Marinella Marmo, gives a succinct and informative account of the ongoing development of international criminal law and associated tribunals as well as looking at war crimes, genocide and crimes against humanity. In the past criminologists seem to have been somewhat reluctant to become involved in such an arena, leaving it for comment and review by international law experts and others. This somewhat parochial approach is now being challenged by the realisation that so much of contemporary serious crime, even if not recognised as an international offence, has a transnational component and can only be dealt with through cross border cooperation and assistance.

The three co-editors of this book – Marinella Marmo and Willem de Lint of Flinders University and Darren Palmer of Deakin University – deserve plaudits for a job well done as do all of the individual authors who have made contributions to its content. No doubt a fifth edition will be required in due course since crime and criminals never stand still. Predicting just what new chapters may need to be added in the future is obviously a highly speculative and risky business. Several decades ago while living in Canada and working at the School of Criminology at Simon Fraser University I was naive enough to become involved with a journalist friend in the production of a radio documentary series for the Canadian Broadcasting Corporation (CBC) on the topic of 'The Future of Crime'. Among other things I predicted that international organ theft and trafficking was a strong candidate for mention in the crime futures market. At the time my colleagues fell about laughing at this suggestion as well as another made by a fellow academic that we would eventually be transporting troublesome convicted criminals to a penal colony on the moon.

Regrettably my prediction about organ theft and trafficking has proven to be accurate while to the best of my knowledge no criminal has as yet been dispatched to the moon. But one prediction that was not made in the CBC program was about the amazing growth that we have since experienced in cybercrime, as the chapter in this book by Russell Smith and Peter Grabosky illustrates. Given this track record I will conclude with the thought that crimes in cyberspace will continue to be a growth industry for the foreseeable future but that undoubtedly some entirely new forms of crime and

criminality will emerge as we grapple with the profound issues of climate change, globalisation of trade and commerce and ever rising populations in so many parts of the world who must compete for our declining resources.

August 2011

References

- Chappell, D & Wilson, P (eds) 1972, *The Australian Criminal Justice System* (Butterworths, Sydney).
- Clarke, M 2009, *For the Term of His Natural Life* (Penguin Books, Camberwell, Victoria).
- Dunkley, M 2011, 'Victoria Police Chief Commissioner Overland Resigns', *Financial Review*, 16 June.
- Ferguson, J 2011, "'Widespread flaws" in Crime Data Collection', *The Australian*, 17 June.
- Hughes, R 1987, *The Fatal Shore* (Alfred A Knopf Inc, New York).

Preface

It is now five years since the last edition of *Crime and Justice* and much has changed in this new edition. First, the editorial team is completely new, not due to an editorial equivalent of a 'failed state' subject to a coup but rather a graceful desire for a new team to take up the challenges of keeping the text as a lively, up to date compendium of contemporary criminological thinking suitable for undergraduate students. We acknowledge the legacy of the previous editors – Andrew Goldsmith, Mark Israel and Kathy Daly – all outstanding scholars in their own right but also powerful editors able to bring together experts across the diverse range of criminological issues. Many of the previous chapter authors have continued their involvement with *Crime and Justice*.

The second important change is that all chapters have been revised, sometimes by the previous chapter author(s) but in several instances by new authors giving new perspectives on the topic being addressed, the latter providing a greater spread of authors across Australian universities.

There are seven new topics for this edition, taking the total to 29 chapters which is enough content to properly address a full year of study. These new topics include the growing emphasis on environmental issues, a refocused concern with international crimes and crimes of the state, issues concerning forensic science and the production of knowledge and a chapter on human rights. The closing chapter is intended as a resource for those readers who are approaching crime and criminology for the first time; this chapter stands out for its uniqueness in Australia.

As with previous editions, authors have been asked to identify key questions related to each chapter topic and, where appropriate, current websites where further exploration of the topic can be undertaken. As will be seen, the internet offers considerable scope for the general readership as well as formal students to engage in more in-depth, thorough and more nuanced research through following these links to further resources.

We have also tried to continue the reflective process discussed by the previous authors, wherein we have drawn on our own experiences in using the text and how an expansion of topics covered and the revision of existing topics can be further enhanced to achieve the goal of providing a foundation of *criminological literacy*. It might be asked whether by extending the chapters we have pushed

even further into the critique that the book covers so much as to unravel any sense of discipline coherence or unity. Our response to this is simply that the new topics, as well as revisions of previous topics are designed to provide a sense of the richness and diversity of criminological thought and stimulating the 'criminological imagination' (Barton et al 2006; Whiteha 1985; Young 2011) rather than being fixated by any singular approach to criminology.

Finally, and following from the previous edition we have divided the book into two Parts. Part 1 'Understanding Crime' consists of 16 chapters exploring the conceptual meaning of and different forms of crime. Part 2 'Understanding Criminal Justice' consists of 12 chapters exploring the principles and objectives of criminal justice 'systems', key criminal justice institutions, different approaches to criminal justice as well as the 'failures' of criminal justice.

As with all publications considerable and invaluable work was done to assist with the production of this book. Initially, the work of Sarah Hullah at Thomson Reuters pushed the planning of the new edition. We are indebted to Sarah for her efforts in advocating for this edition. Unfortunately, Sarah changed occupation but this in turn gave us the opportunity to work with Helen Sheridan who provided wonderful guidance in steering the book to completion. We wish to extend our gratitude to a number of people who contributed to this fourth edition by providing different levels of help: Russell Brewer, Ron Layton, Debbie Kuss, Nerida Chazal, Andrew Groves and Derek Dalton. Finally, we have benefitted from the excellent, enthusiastic and thorough editorial assistance work completed by Rhiannon Bandiera. Without the persistence and support they have provided along the way we would have struggled to complete the book.

MARINELLA MARMO
WILLEM DE LINT
DARREN PALMER

August 2011

Associate Professor Adam Sutton, a co-contributor to Chapter 9 White Collar and Corporate Crime and Chapter 23 Crime Prevention and Reduction, passed away before preparation began on this latest edition of *Crime and Justice*. However, his contribution to these chapters remains seminal, despite the most recent changes, and so the decision to retain his name as co-author was made.

References

- Barton, A, Corteen, K, Scott, D & Whyte, D 2006, *Expanding the Criminological Imagination* (Willan, Cullompton).
Whiteha, J 1985, 'The Criminological Imagination: Another View', *Criminal Justice Review*, Fall, vol 10, no 2, pp 22–26.
Young, J 2011, *The Criminological Imagination* (Polity Press).

List of Contributors

- | | |
|----------------------------|--|
| Brown, Mark | Senior Lecturer in Criminology, School of Social and Political Sciences, University of Melbourne |
| Buth, Rhain | Lecturer, School of Law, Flinders University, Adelaide |
| Cherney, Adrian | PhD, Senior Lecturer, School of Social Science, University of Queensland |
| Clare, Joseph | Assistant Professor, Crime Research Centre, School of Law, University of Western Australia, Perth |
| Coventry, Garry | PhD, Co-ordinator, Criminology Programs, Senior Lecturer, School of Arts and Social Sciences, James Cook University, Townsville |
| Daly, Kathleen | Professor, School of Criminology and Criminal Justice, Griffith University, Brisbane |
| Dioso-Villa, Rachel | PhD, Lecturer School of Criminology and Justice, Griffith University, Brisbane |
| Garkawe, Sam | Associate Professor, School of Law and Justice, Southern Cross University |
| Goldsmith, Andrew | Executive Director, Centre for Transnational Crime Prevention, Professor of Law, University of Wollongong; Adjunct Professor of Law and Criminal Justice (Flinders University, Adelaide) |
| Grabosky, Peter | Professor, Regulatory Institutions Network, School of Regulation, Justice and Diplomacy, College of Asia and the Pacific, The Australian National University, Canberra |
| Grigg, Brendan | Lecturer, Flinders Law School, Flinders University, Adelaide |
| Haines, Fiona | Associate Professor, Criminology, School of Social and Political Sciences, University of Melbourne, Melbourne |
| Hanley, Natalia | Lecturer in Criminology, School of Social and Political Sciences, University of Melbourne, Victoria |
| Heseltine, Karen | Forensic Psychologist, Director – ForenPsych, Adelaide |

- Howells, Kevin** Emeritus Professor, Division of Psychiatry, School of Community Health Sciences, University of Nottingham, United Kingdom
- Israel, Mark** Winthrop Professor of Law and Criminology and Associate Dean (Learning and Teaching), Faculty of Law, University of Western Australia
- de Lint, Willem** Professor in Criminal Justice, Flinders Law School, Flinders University, Adelaide
- Marchetti, Elena** Professor, Faculty of Law, University of Wollongong
- Marmo, Marinella** Senior Lecturer, School of Law, Flinders University, Adelaide
- Martin, Greg** Lecturer in Socio-Legal Studies, Department of Sociology and Social Policy, University of Sydney, Sydney
- Morgan, Frank** Director, Crime Research Centre, University of Western Australia, Perth
- Moston, Stephen** Associate Professor, University of Canberra, Centre for Applied Psychology, University of Canberra, Canberra
- Niemann, Grant (Dr)** Associate Dean (Students), School of Law, Flinders University, Adelaide, South Australia
- Osmond, Craig** PhD, Lecturer, School of Social Science, University of Western Sydney
- Palmer, Darren** Associate Professor in Criminology, Deakin University, Geelong
- Pereira, Margaret** Senior Research Assistant and PhD Candidate, School of Justice, Queensland University of Technology, Brisbane
- Ransley, Janet** Associate Professor, Head, School of Criminology and Criminal Justice, Griffith University, Brisbane
- Ross, Stuart** Senior Fellow, School of Social and Political Sciences, University of Melbourne, Victoria
- Sarre, Rick** Professor, School of Law and School of Commerce, University of South Australia, Adelaide
- Heidi Savilla** Liaison Librarian for Law and Legal Studies, Law Library, Flinders University, Adelaide
- Scott, John** Associate Professor, School of Behavioural, Cognitive and Social Science, University of New England, Armidale
- Smith, Russell G** Principal Criminologist, Australian Institute of Criminology, Canberra
- Stewart, Anna** Professor, School of Criminology and Criminal Justice, Griffith University, Brisbane
- Stubbs, Julie** Professor, Faculty of Law, University of New South Wales, Australia

- Sutton, Adam** Formerly, Associate Professor, Department of Criminology, University of Melbourne
- Warren, Ian** Senior Lecturer, Criminology, School of History Heritage and Society, Faculty of Arts and Education, Deakin University, Geelong
- Weber, Leanne (Dr)** Senior Larkins Research Fellow, School of Political and Social Inquiry, Monash University
- Wise, Jenny** Lecturer, School of Behavioural, Cognitive and Social Sciences, University of New England, Armidale
- Wortley, Richard** Professor, Director, Jill Dando Institute of Security and Crime Science, Head, Department of Security and Crime Science, University College London, United Kingdom

Brief Contents

<i>Foreword</i>	<i>v</i>
<i>Preface</i>	<i>xi</i>
<i>List of Contributors</i>	<i>xiii</i>
<i>Table of Contents</i>	<i>ix</i>
<i>Table of Figures</i>	<i>xxv</i>

Part 1 Understanding Crime..... 1

Chapter 1	What is crime and who is the criminal?	3
Chapter 2	The distribution of crime over populations, space and time	25
Chapter 3	Crime and the media.....	53
Chapter 4	Individual explanations for crime	69
Chapter 5	Social explanations for crime	97
Chapter 6	Youth and crime	125
Chapter 7	Crime in the streets	151
Chapter 8	Crime and the home	171
Chapter 9	White-collar and corporate crime	191
Chapter 10	Environmental crime	211
Chapter 11	State crime	231
Chapter 12	Cyber crime	245
Chapter 13	Crimes across borders	275
Chapter 14	International crimes.....	303
Chapter 15	Inequalities of crime	327
Chapter 16	Extending explanations of crime.....	359

Part 2 Understanding Criminal Justice 387

Chapter 17	Aims of the criminal justice system	389
Chapter 18	Policing and law enforcement.....	407
Chapter 19	The criminal process.....	435
Chapter 20	Innovative justice processes	455
Chapter 21	Imprisonment and detention.....	483
Chapter 22	Community-based corrections	507
Chapter 23	Crime prevention and reduction.....	527

Chapter 24	Victims and criminal justice	547
Chapter 25	Experts, lay people and forensics.....	573
Chapter 26	Transnational policing	589
Chapter 27	Failures of justice	609
Chapter 28	Criminal justice and human rights	631
Chapter 29	National and international research resources	657
<i>Glossary</i>		675
<i>Index</i>		695

Table of Contents

<i>Foreword</i>	v
<i>Preface</i>	xi
<i>List of Contributors</i>	xiii
<i>Brief Contents</i>	xvii
<i>Table of Figures</i>	xxv

Part 1 Understanding Crime..... 1

Chapter 1	<i>What is crime and who is the criminal?</i>	3
	<i>Ian Warren</i>	
	Legal definition	4
	Crime as a social and political process.....	9
	Human rights definitions	12
	Who is the criminal?.....	14
Chapter 2	<i>The distribution of crime over populations, space and time</i> .	25
	<i>Frank Morgan, Joseph Clare</i>	
	Origins and current status of official statistics in Australia ...	26
	Police recorded crime statistics and their interpretation	27
	Criticisms of official crime statistics.....	30
	Responses to the criticisms	31
	Other sources of information about crime.....	32
	Modern uses of crime statistics	38
	The uneven distribution of crime	39
Chapter 3	<i>Crime and the media</i>	53
	<i>Stephen Moston, Garry Coventry</i>	
	The nature and extent of crime in the media	54
	Case Study: Studying crime and the media.....	55
	Does the media influence public perceptions about crime and criminal justice system policies?.....	62
Chapter 4	<i>Individual explanations for crime</i>	69
	<i>Richard Wortley, Anna Stewart</i>	
	Philosophical debates.....	70
	Psychological theories of crime	72

Sutherland, E 1945, "Is 'White-collar Crime' Crime?", *American Sociological Review*, no 10, pp 132–139.

White, R 2008, "Depleted Uranium, State Crime and the Politics of Knowing", *Theoretical Criminology*, no 12, pp 31–54.

FURTHER READING

Boas, G 2010, "Soldiers' Work is Life or Death, but they're not above the Law", *The Age* (Melbourne), 13 October.

Fessy, T 2010, "Rwanda rebel FDLR leader Mbarushimana held in France", BBC Africa (online), 11 October, www.bbc.co.uk/news/world-africa-11517549 (accessed 20 June 2011).

Rothe, D, Ross, J, Mullins, C, Freidrichs, D, Michalowski, R, Barak, G, Kauzlarich, D & Kramer, R 2009, "That Was Then, This is Now, What about Tomorrow? Future Directions in State Crime Studies", *Critical Criminology*, vol 17, no 1, pp 3–13.

Ross, J 2000, *Varieties of State Crime and Its Control* (Criminal Justice Press, Monsey).

USEFUL WEBSITES

www.icc-cpi.int/Menus/ICC
International Criminal Court

www.icty.org/sid/10010
International Criminal Tribunal for the former Yugoslavia (ICTY)

www.supranationalcriminology.org
Supranational Criminology

12

Cyber crime

Russell G Smith, Australian Institute of Criminology¹

Peter N Grabosky, Australian National University

Key words	245
Introduction	245
Defining and classifying cyber crime	246
A chronology of cyber crime	247
Countering cyber crime	265
Conclusion	269
Questions	269
References	269
Further reading	273
Useful websites	273
Note	274

Key words computer crime, cyber crime, information security, computer security, identity crime, regulation of cyberspace

INTRODUCTION

[12.10] Information and communications technologies are now established features of life in industrialised societies. They have created untold benefits for education, delivery of health services, recreation, commerce, and government and changed considerably the nature of modern workplaces and patterns of employment. They have also created unprecedented opportunities for crime (see Grabosky & Smith 1998; Grabosky, Smith & Dempsey 2001; Smith, Grabosky & Urbas 2004; Grabosky 2007; Choo, Smith & McCusker 2007; Smith 2010b). Identifying these vulnerabilities, and mobilising appropriate countermeasures, are some of the great challenges of the years to come.

Much technology-related crime lies beyond the capacity of contemporary law enforcement and regulatory agencies to control, if they act by themselves, and security in cyberspace will depend on the collaborative efforts of many institutions, coupled with self-help by potential victims. The ideal configuration will differ, depending upon the activity, but is likely to entail a mix of law enforcement, technological, and market responses. Because cyberspace knows no boundaries and computer crime often crosses national frontiers, effective countermeasures will require a substantial degree of international co-operation (Chapters 13 and 26).

Defining and classifying cyber crime

[12.20] Digital technologies lie at the heart of cyber crime and these include computers, communication technologies (fixed line and mobile) and networked services. There is a wide range of adjectives used to describe computer-related crime. They include: virtual, online, cyber, digital, high-tech, computer-related, internet-related, telecommunications-related, computer-assisted, electronic, ICT-related crime, technology-enabled, and “e-” (as in “e-crime”). It is useful, at the start, to distinguish between *computer crime* and *internet crime*, as not all forms of computer crime involve the use of the internet. There are a number of non-internet-related computer crimes including fixed-line phone fraud, unauthorised network access, electronic counterfeiting, and diversion of funds electronically. The most usual classification, however, distinguishes between crimes that target, and crimes that use digital technologies.

Crimes against digital technologies

[12.30] Examples of offences in which computers are the object or target of offending include obtaining illegal access to computers (hacking); the illegal interception of communications; interference with electronic data such as the dissemination of computer viruses; interference with computer systems such as denial of service attacks or the dissemination of spam; misuse of devices to avoid liability for charges such as “phreaking”; and cyber terrorism. The motives may vary and can include greed, a political agenda, revenge attacks, economic sabotage, and mischief.

Crimes that make use of digital technologies

[12.40] The latter category incorporates two levels of reliance on computers – offences which are *enabled* by computers (those in which a computer is required in order to commit the offence), and offences which are *enhanced* by computers (that is, those which are easier to commit using computers). Examples of offences in which computers are the tool of offending in that the offence is *enabled* by computers include: dissemination of malicious code

(viruses and worms), ATM fraud, and “phishing”. The motives for these include greed, mischief and revenge.

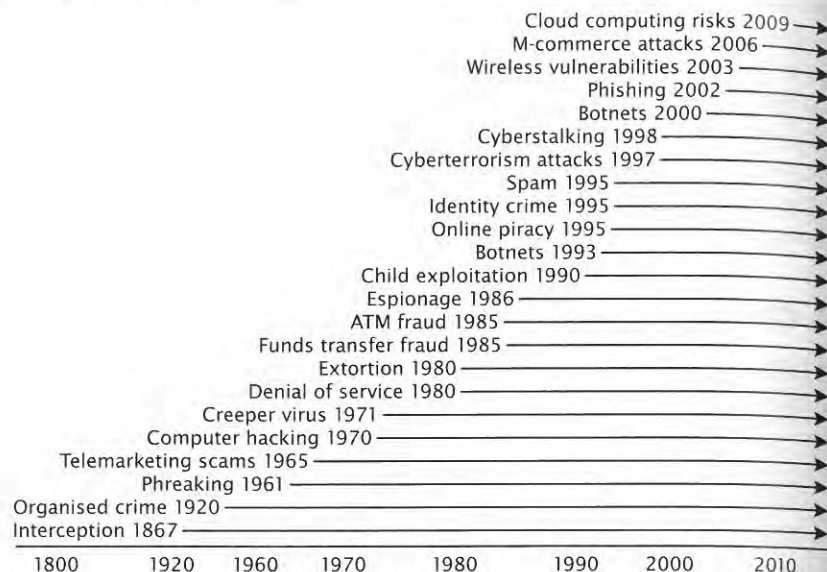
Examples of offences in which computers are the tool of offending in the sense that the commission of the offence is *enhanced* by the use of technologies include: recording payments for drugs in computer databases; establishing databases of victims or potential victims of consumer fraud; identity-related theft; online extortion; communicating between offenders; encrypting secret information or using steganography to hide data. Cases involving each of these offence categories will be presented in the next section.

A chronology of cyber crime

[12.50] Clearly, the variety of criminal activity committed with or against technologies is diverse. Some types are not new in substance; only the medium is new. Others represent entirely new forms of illegality altogether, which have been described by a number of new terms including “phreaking”, “hacking”, “phishing”, and “spamming”.

Wall (2010: 94–98) has identified three “generations” of cyber crime. The first generation of low-end cyber crime involved the use of mainframe computers and their operating systems to assist traditional forms of offending such as theft of funds or information. The second generation involved offending across computer networks, such as hacking and cracking activities. The third generation of crimes, Wall argues, were wholly mediated by technology and were truly distributed and automated, such as occurs in the dissemination of spam using botnets. One way of examining the various kinds of cyber crime is to employ a chronological framework arranged according to the period of time during which the conduct in question first achieved significance. In 1998, Grabosky & Smith developed such a diagrammatic representation of how cyber crime developed and this was up-dated and revised by Smith (2010: 220, see Figure 12.1 with further revisions). The localisation of the introduction of each form of offending in history cannot be isolated with great precision but an indication can be given of which forms of illegality achieved significance earlier rather than later and which are of most recent origin. The various types are not mutually exclusive, nor is the list exhaustive.

Figure 12.1 also allows us to relate the various forms of illegality to the introduction of new technologies – some of which were, themselves, introduced as a crime reduction measure (see Smith 2010b: 216 for a similar chronology of information and communications technologies). A case in point is encryption software. Telecommunications technology was first created in 1837, while the earliest example of illegal interception occurred in 1867. The 1960s saw a rapid expansion in the use of telephony services which corresponded with attempts at obtaining services free of charge through phreaking. The introduction of electronic funds transfer technologies such as ATM and EFTPOS led to the use of such facilities to transfer funds illegally in the 1970s; this was followed

Figure 12.1 A Chronology of Cyber crime (adapted from Smith 2010b: 220)

by the widespread use of computer networks and the commission of hacking offences. Most recently, the introduction of the internet in the late 1980s, cellular phones in the 1990s and wireless and mobile technologies in the 2000s, has created an environment in which crimes occur across international networks.

How, then, are these various types of cyber crime perpetrated and what motives lie behind their commission?

Illegal interception of digital information

[12.60] The interception of communications has a lengthy history which extends back to Oliver Cromwell's time in the 17th century when a state monopoly was established over the delivery of letters, expressly so that they could be intercepted to protect the interests of the state. Telecommunications technology was first created in 1837 and one of the first cases of misuse occurred as early as 1867 when a Wall Street stock broker collaborated with Western Union telegraph operators to intercept telegraph dispatches sent to Eastern newspapers by their correspondents in the West. The intercepted messages were then replaced by counterfeit ones which reported bankruptcies and other financial disasters supposedly befalling companies whose stock was traded on the New York Stock Exchange. After the share prices were driven down, the wiretappers purchased their victims' stock (Grabosky & Smith 1998: 25).

More recently, electronic devices have been used in many ways to intercept communications and to conduct surveillance over people. This includes:

intercepting electromagnetic impulses as they pass along telephone wires or via mobile telephones; bugging, or listening to and recording private conversations using listening devices; tracking an individual's whereabouts using global positioning technologies or by locating mobile phones electronically; monitoring and recording of both visual and sound information through the use of video surveillance devices including mobile phones; and using devices to scan the electromagnetic radiation emitted from computer and peripheral hardware and convert this into visual images. This has been used to collect mobile phone numbers, and information on the screens of computers in a bank. 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 advent of spyware has been used to track people's electronic movements by recording individual keystrokes, allowing access to messaging services, and monitoring websites visited. Illegal interception of digital information is hardly the monopoly of individual offenders. A great deal of illegal surveillance is undertaken by governments. The United States Government, assisted by the telecommunications industry, engaged in widespread illegal interception of telecommunications traffic during the Bush administration (Bamford 2008). In 2011, it was alleged that employees of News International had obtained access to mobile phones of politicians, crime victims and members of the Royal family (Cullinane & Jones 2011).

Communications in furtherance of criminal conspiracies

[12.70] Telephones were introduced around the turn of the last century and became widespread in the 1920s and 1930s. There is evidence of telecommunications equipment being used to facilitate a wide range of criminal activities starting with Al Capone's use of the telephone to manage his rackets in the United States in the 1920s through to organised drug trafficking, gambling, money laundering, child pornography, and trade in weapons in more recent times. Members of the terrorist networks use email and the Web to communicate with each other and to disseminate information and recruit new members. The use of encryption technology is also being used to place criminal communications beyond the reach of law enforcement, and steganography is being used to conceal information in data files such as seemingly innocent pictures.

The use of computer networks to produce and to distribute child pornography is the subject of increasing attention (see Krone 2004, 2005a). These materials can be imported across national borders quickly and many thousands of images have been shared between organised groups of individuals. From what we know from police investigations, there have been a number of networks established, which extend across national borders, use sophisticated technologies of concealment, and have a significant degree of co-ordination (Krone 2005a).

Theft of telecommunications and online services (Phreaking)

[12.80] In the 1950s and 60s, international telephone and telex networks expanded greatly and this led to the opportunity to try to obtain calls for free. The Bell Telephone Company believes that the first case of theft of a long-distance telephone service occurred in 1961 when a local office manager discovered some inordinately lengthy calls to an out-of-area directory information number. In 1969, John Draper, aged 26, used a children's toy whistle, a cereal packet free offer, which produced a 2,600-cycle tone to obtain free calls. Known as Cap'n Crunch, Draper experimented with various other devices to obtain free international calls and was finally apprehended by the FBI making unauthorised calls between San Jose and Sydney in order to listen to the Australian Top Ten (Grabosky & Smith 1998: 64).

Theft of telecommunications services has since become a major criminal industry. Some offenders seek to avoid or to obtain a discount on the cost of a telephone call or internet connection while others, such as illegal immigrants, are unable to acquire legitimate information services without disclosing their identity and their status. There are others still who use information services to conduct illicit business with less risk of detection. All pose a significant challenge to carriers, service providers, and to the general public – who often bear the financial burden of fraud.

The methods of stealing telecommunications services are diverse; they include the “cloning” of cellular phones and the counterfeiting of telephone cards. They also include gaining unauthorised access to an organisation's telephone switchboard (PBX). By gaining access to a 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 sometimes 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. In one New Zealand case, the offender fraudulently used a computer program downloaded from the internet (named *Scavenger*) to evade billing on international telephone calls, amounting to between NZ\$85,000 and NZ\$166,000. He was sentenced to 12 months' imprisonment on three counts, suspended for two years and six months' periodic detention (*R v Borislav Misic* [2001] NZCA 71 (11 April 2001, New Zealand Court of Appeal)).

Internet service providers (ISPs) are increasingly becoming the victims of theft of connection services and time. This extends from hacking to obtain services fraudulently, through to denial of service attacks which can crash ISP servers, costing them both goodwill as well as the income which they would ordinarily have earned had they remained operative. Most recently, interception of wireless laptop connections has also proved possible. In one famous case,

a Yale University student known as “Happy Hardcore”, created, distributed and used his software “AOL4Free” to allow himself and others to gain free access to America Online (AOL) without paying the standard fee of US\$2.95 per hour. AOL4Free worked by exploiting a weakness in AOL's billing system which enabled false commands to be sent to the AOL network to convince the billing system that the user was always using a free area of the service. The offender received a sentence of two years' probation, six months' home confinement, a fine of US\$50 and was ordered to pay restitution of US\$62,000 (Grabosky, Smith & Dempsey 2001: 78).

Electronic sales and investment fraud (cyberscams)

[12.90] With the development of the internet came a range of consumer-oriented fraudulent scams, as offenders now enjoy direct access to millions of prospective victims around the world, instantaneously, and at minimal cost. Examples include so-called advance fee schemes, such as pyramid and Ponzi schemes, the use of chain letters and bulk email, business opportunity schemes, and fraudulent online auctions, prizes and lotteries. Even the notorious “Nigerian letters” which trick unsuspecting recipients into paying money in the expectation of reaping a massive return, now arrive via email instead of post (see Smith, Holmes & Kaufmann 1999). Other consumer frauds carried out through the use of the internet involve the non-delivery of goods and services or the delivery of defective products and services often associated with online auctions (Smith & Budd 2009).

Cyberspace also 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 lotteries (Cella & Stark 1997: 837–844). The digital age has brought unprecedented opportunities for misinformation.

Dialogue box 12.1

Electronic sales and investment fraud

[12.100] In May 1999, a 24-year old man who lived in a Melbourne suburb manipulated the share price of an American company by posting information on the internet and sending email messages around the globe that contained false and misleading information about the company. The messages contained a statement that share value of the company would increase from the then current price of US\$0.33 to US\$3.00 once pending patents were released by the company, and that the price would increase up to 900% within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume. The offender had purchased 65,500 shares in the company

through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A\$17,000. The Australian Securities and Investments Commission prosecuted the offender for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was ordered to serve three months' imprisonment and to be of good behaviour for a further 21 months (*Australian Securities and Investments Commission v Steven George Hourmouzis*, County Court of Victoria, 30 October 2000, Stott J).

Hacking

[12.110] The 1970s also saw the development of a range of activities in which computer networks were compromised, access was obtained illegally, and data damaged maliciously. The key terms in common usage are: *hacking* – in which an individual uses ingenuity to refine existing computer programs; *cracking* – in which an individual intrudes upon computer systems without permission; *vandalism* – in which intrusions hinder a system's operation; and *spoofing* – or electronically impersonating a computer to appear like another in order to gain access without authority.

Western industrial society is dependent upon complex data processing and telecommunications systems. Damage to, or interference with, any of these systems can lead to catastrophic consequences. Whether motivated by curiosity or vindictiveness, electronic intruders cause inconvenience at best, and have the potential for inflicting massive harm. One of the most infamous hackers was Kevin Mitnick, who from the early 1980s until 1995, carried out various schemes to defraud and obtain property by false pretences from a number of major corporations using unauthorised access to computers of software manufacturers and illegal copying of software from these sites (among many other things). Millions of dollars were thought to have been stolen (see Mitnick Security Consulting 2004–2005).

Hacking can occasionally result in serious physical and environmental harm. In Luxembourg, an individual gained access to a hospital's computer system resulting in an operation on a ten-year old boy being delayed for six days while the hospital's computer network was rebuilt. In another incident, a nurse in a hospital modified patient records relating to patients' prescriptions, scheduling of X-rays, and recommended dates for discharge from hospital (Smith 1998). In Australia in 1999, a computer hacker in Queensland caused raw sewage to overflow on the Sunshine Coast by using radio transmissions to alter council sewerage pump stations (Smith, Grabosky & Urbas 2004: 205). Various individuals and protest groups have also hacked the official web pages of governmental and commercial organisations in recent years (Rathmell 1997).

Malware

[12.120] The creation and dissemination of various forms of malicious software (malware), including computer viruses for reasons of curiosity, revenge or extortion, has become an endemic counter-productive consequence of life in the digital age, and has spawned one of the 21st century's growth industries – computer security. Viruses are contaminated program elements which impede the operation of computers and can take a variety of forms. Worms are software which attaches itself to other programs. Bombs are viruses which lay dormant until a pre-determined time (Time Bomb) or event (Logic Bomb), while Trojan Horses are software concealed within another program which, when activated, will impede the operation of the program. Recently, a number of those who have created and sent out viruses have been prosecuted, some with more success than others.

The McAfee (2008) virtual criminology report indicated that cybercriminals are increasingly exploiting vulnerabilities in software and social engineering to spawn a broad range of threats including spyware, phishing, adware, rootkits, spam, and botnets. In 2008, Symantec reported that "the number of new malicious code (also known as malware) signatures increased by 265% over 2007; over 60% of all currently detected malicious code threats were detected in 2008" (Symantec 2009: 15). In the "Australian Business Assessment of Computer User Security" (ABACUS) survey, responses from 4,000 Australian businesses indicated that 14% of the respondents had experienced one or more computer security incidents during the 2006–07 financial year (Richards 2009). According to the survey, the most common type of incident reportedly experienced by the respondents was a virus or other malware code, and the most common effect was corruption of hardware and software. The total financial loss as a result of computer security incidents against businesses in Australia during the 2006–07 financial year was estimated at between \$595 and \$649 million (Richards 2009).

In one case, a 22-year old man in England wrote and then emailed three computer viruses, two of which were designed to stop computers operating and to destroy material when rebooted. Some 27,000 computers were infected in 42 countries. He was sentenced to two years' imprisonment for each of three offences in January 2003 (Smith, Grabosky & Urbas 2004).

In May 2000 a student in the Philippines was alleged to have sent out the so-called "Love Bug virus" infecting Microsoft Windows operating systems by sending email attachments which, when opened, damaged files in the computer and then replicated itself by sending similar messages to all the addresses in the infected computer's address book. The damage caused globally was estimated to be between US\$6.7 billion and US\$15.3 billion. The virus was traced to an ISP in the Philippines who co-operated with police to locate the source of the email. The student was arrested, but the creation and release of a computer virus was not proscribed by Philippine law at the time. Because the conduct was not illegal in the Philippines, the principle of

dual criminality precluded extradition to the United States, where it was a crime under US law (Bell 2002).

Distributed denial of service

[12.130] A related form of computer vandalism is that involving so-called “distributed denial of service” attacks. These incapacitate servers through bulk emailing or through the use of worms or Trojan horses. They are often used as a threat in order to extort money from corporations.

In one case, a former systems administrator for the United States District Court in Alaska launched three denial of service attacks against the United States District Court for the Eastern District of New York. His actions overwhelmed the server with emails to prove that it was vulnerable to external attack. He was convicted of interfering with a government-owned communications system and sentenced to three months’ imprisonment and various consequential orders (Smith, Grabosky & Urbas 2004, p 197). The most recent problem concerns so-called “bot armies” in which thousands of illegally accessed and remotely controlled computers are made to bombard another computer or service causing it to be overloaded and degrade or fail. In September 2009, the Department of Prime Minister & Cabinet and other Australian government agencies’ websites were subject to denial of service attacks perpetrated by a group, “Anonymous”, which was seeking to alter the government’s policy concerning internet filtering. The attack was largely ineffective with only a short loss of functionality for the websites attacked (Moses 2010).

The flyer “Anonymous: used to recruit people for the hack attack”



Source: Moses (2010)

Digital extortion

[12.140] In the 1990s, computer networks began to be used in carrying out acts of criminal extortion – a demand (usually for money) accompanied by the threat of harm in the event that the victim does not comply. 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 ISP's ten servers. The offenders obtained personal information and credit card details of 10,000 subscribers and, communicating via email through one of the compromised accounts, demanded that US\$30,000 be delivered to a mail drop in Germany. Co-operation between American and German authorities resulted in the arrest of the extortionists (Bauer 1998).

Electronic funds transfer crime

[12.150] The proliferation of electronic funds transfer systems has enhanced the risk that such transactions may be intercepted and diverted. Facsimile machines and personal computers have been used dishonestly by offenders to transmit fraudulent instructions to financial institutions. High quality and relatively cheap desktop publishing facilities are widely available through the use of personal computers, scanners, and laser printers, which enable the production of near perfect copies of legitimate business documents. Many of these contain signatures of company officials that have been scanned from annual reports or other official papers. The resulting document, once transmitted to a financial institution electronically, may result in funds being remitted, usually offshore, via some irrevocable channel such as the SWIFT system of electronic funds transfer, making recovery difficult. Substantial losses have been incurred by financial institutions as a result of organised groups using this simple technique.

Dialogue box 12.2

Electronic Funds Transfer crime

[12.160] Between June and October 1994, a group of Russian computer hackers attempted to steal approximately US\$10.7 million from various Citibank customers' accounts in the United States by using a computer terminal in St Petersburg to gain unauthorised access to the computerised fund transfer service of Citibank in Parsippany, New Jersey. The principal offender, Vladimir L Levin attempted to fraudulently make 40 transfers of funds from the accounts of clients of Citibank to accounts which he or his associates controlled manipulating its computerised funds transfer system. Levin gained access to Citibank's funds transfer system using a personal computer and stole passwords and account identification numbers. Using a computer terminal in his employer's office in St Petersburg, he authorised

transfers of funds to accounts which he and his co-conspirators held in California, Finland, Germany, the Netherlands, Switzerland, and Israel. Levin was arrested at Stansted Airport, in England in 1995 and, after protracted legal proceedings which went to the House of Lords, he was extradited to stand trial before the Federal District Court in New York's Southern District. In 1998, he pleaded guilty to conspiracy to defraud and was sentenced to 36 months' imprisonment and to pay Citibank US\$240,015 in restitution. Citibank was able to recover all but \$240,000 of the \$10.7 million worth of illegally transferred funds. None of the bank's depositors lost money. The consequences for Citibank's business reputation were considerable (*R v Governor of Brixton Prison; Ex parte Levin* [1996] 3 WLR 657; *In re Levin*, House of Lords, 19 June 1997).

ATM and plastic card fraud

[12.170] The development and use of plastic cards to carry out financial transactions has created risks of misuse since they were first introduced in the 1950s. Existing systems such as Automated Teller Machines (ATM), and Electronic Funds Transfer at Point of Sale (EFTPOS) technologies have already been the targets of fraudulent activity and the development of stored value "chip" cards will invite some individuals to engage in electronic counterfeiting – although this would be difficult and require the assistance of industry collaboration. Credit card details and other personal information can also be captured by techniques of social engineering (in which offenders persuade cardholders to disclose their PINs), or by hacking into databases. ATMs have been targeted by re-programming them to dispense cash beyond the account holder's credit limit, while technological means have been developed to trick users into revealing their PINs or to retain cash that has been dispensed for later collection by offenders.

Cybercriminals have also developed ingenious ways of compromising the data held on the magnetic stripes of plastic payment cards. A recent example in Australia that resulted in arrests, in March 2009, concerned a syndicate of individuals based in New South Wales who were alleged to have purchased more than \$4.5 million in goods using credit cards bearing bank account details "skimmed" or stolen from legitimate card-holders. The goods, including brand new LCD televisions, lap-top computers, cameras, power tools, GPS systems and iPods, were then allegedly sold on various online auction sites at reduced prices, allowing the syndicate to launder the profits. The syndicate had been in operation for some time and had allegedly sold 6,000 items for \$1.3 million (New South Wales Police Force 2009).

Electronic money laundering and tax evasion

[12.180] For some time, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. New technologies enhance these

efforts. Legitimately derived income may also be more easily concealed from taxation authorities. At present, the movement of funds electronically is closely supervised by government regulators. Computers, however, enable funds to be moved in such a way that regulatory controls can be avoided, such as by making multiple transactions just beneath cash transaction reporting limits. Some forms of electronic cash for use on the internet also by-pass traditional controls on the issue and movement of currency. Traditional underground banks, which have flourished in Asian countries for centuries, enjoy even greater capacity through the use of telecommunications and have created various risks of money laundering and fraud (Rees 2010).

Dissemination of offensive materials

[12.190] Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials (including child pornography), racist propaganda, and instructions for the fabrication of incendiary and explosive devices. For example, in north-western Victoria on 11 July 1999, a 17-year old boy was killed instantly and two of his friends injured when a home-made bomb, constructed from a recipe discovered on the internet, exploded (Butcher 2001). In November 2000, a French judge ordered the United States-based Yahoo! to block Web surfers in France from an auction where Nazi memorabilia was sold. He gave Yahoo! three months to find a way to prevent users based in France from accessing pages on auctions that feature Nazi-related objects, such as swastika-emblazoned flags and daggers. In January 2001, the company announced plans to ban hate-related goods, including Nazi memorabilia, from its United States commerce sites.

A more extensive problem, however, concerns the networks of offenders who have been involved in obtaining and sharing child pornography. One police operation in Australia, Auxin, involved over 700 suspects and led to 150 arrests.

Offenders use secure networks with regularly changed passwords and encrypted content. Many hundreds of thousands of images have been involved (Krone 2005a).

The rich diversity in thresholds of tolerance around the world, combined with the global reach of telecommunications, make the control of offensive content a particularly difficult regulatory challenge. For example, materials offensive to religious leaders in Iran may fail to raise an eyebrow elsewhere.

Information piracy

[12.200] Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, video, and multimedia combinations. It is now possible, for example, to download the latest music and films from the internet, and to copy these to CDs and DVDs. In Australia, the sound recording piracy rate is less than 10% of the total market and the film industry estimates that the film piracy rate was 11% in 2006. An annual global software study

Computers seized during Operation Auxin child internet pornography raid in Adelaide (30 September 2004)



Source: Newspix

estimated that Australia's software piracy rate was 29% in 2006 and Australians have been found to be the leading downloaders of pirated television programs on a per capita basis, with a rate twice as high as the United States. Industry estimates that \$233 million per year is lost to the piracy and counterfeiting of films, and a further \$677 million was lost in sales to the Australian toy, software and video games industry in 2002. This includes \$445.7 million in the business software industry and \$515 million in absolute losses in software piracy in 2006 (Australian Institute of Criminology 2008). As broadband services continue to become available, the potential for copyright infringement involving such works will be enhanced enormously.

Espionage

[12.210] The world's second oldest profession is well served by digital technology. Many states around the world have sought (and continue to seek) to obtain their adversaries' secrets by digital means. One of the earliest examples was the "Cuckoo's Egg" case (Stoll 1991), where the Soviet KGB engaged the services of a young German hacker to gain electronic access to computer systems at defence installations in the United States. In March 2009, it was revealed that a number of computer systems serving the Dalai Lama's Tibetan exile centres around the world had been penetrated by a sophisticated surveillance system. The scale of the surveillance activity, which was traced to three sites

Two policemen inspect the parade ground littered with millions of destroyed pirated copies of CDs worth US\$18.8 million following a destruction ceremony at the Philippine National Police headquarters at Camp Crame, suburban Manila (03 February 2003)



Source: Newspix

in China as well as to a webhosting service in Southern California, seemed to indicate government activity. It was suggested the work may have involved patriotic hackers, associated with, but independent of, the Chinese state. The Chinese government dismissed the suggestion that it was involved in the surveillance (Markoff 2009; Munk Centre 2009). Among the many classified US Government documents published by Wikileaks in November 2010 were allegations that the Chinese Government orchestrated a systematic campaign of computer intrusions, including "government operatives, private security experts," and specially recruited "internet outlaws" (Shane and Lehen 2010).

Digital technology has also been a great boon to industrial espionage. In the competitive global economy, obtaining a competitor's trade secrets and other economic information of a sensitive nature can be extremely lucrative. Depending on the methods employed, it can also be extremely illegal (Nasheri 2005). Traditional espionage techniques are now complemented by high tech methods. Given that much, if not most, information today exists in digital form, industrial espionage will have its digital manifestations. Web-based research through open sources may be legitimate. But the insertion of a Trojan horse or backdoor into a competitor's computer network is quite another matter. The vulnerability of wireless technology and internet telephony to industrial espionage goes without saying.

In the United States on 9 December 2010, two former tyre engineers were convicted of stealing trade secrets from the Goodyear Tire and Rubber Company. The jury found them guilty of one count of conspiracy to commit trade secret theft, one count of trade secret theft, one count of unlawful photographing of trade secrets, three counts of transmittal of trade secrets, one count of possession of trade secrets, two counts of wire fraud and one count of conspiracy to commit wire fraud. According to the evidence, their company secured a US\$1.2 million contract in early 2007 with a Chinese tyre manufacturing company to supply tyre building equipment for use in producing radial "off the road" tyres, which are used on very large earth moving and mining equipment. In order to build the equipment, the offenders needed a special piece of machinery that they knew Goodyear had developed. They arranged to visit the Goodyear plant in Kansas to service their own equipment which was located in the Goodyear plant and then used a cell phone camera to surreptitiously take seven unauthorised photographs of the Goodyear machinery which they then emailed to employees at their subsidiary company in England. The trade secret information contained in the photographs was then used to complete a similar piece of tyre building equipment for use in the Chinese contract (United States Department of Justice 2010).

Cyberbullying

[12.220] In recent years, a new form of bullying, including harassment targeting children and young users, has emerged. It makes use of ICT such as blogs, email, text messaging, chat rooms, mobile phones, mobile phone cameras and social networking sites. Cyberbullying can also include online fights, denigration, impersonation, trickery, and cyberstalking. There is now evidence of the extent of cyberbullying. In an Australian youth poll in 2008, more than a fifth of respondents aged between 15 and 20 years reported being upset or feeling threatened by someone they had come into contact with online (Despoja 2008: 13). In another study, of the 91 student respondents enrolled in the Youth Unit at Northern Melbourne Institute of TAFE, 63% reported experiences of being cyberbullied although only 9% reported being cyberbullied by another student at the same institution. A significant percent (58%) of the respondents admitted to being a cyberbully themselves (Reeckman & Cannard 2009).

Cyberstalking

[12.230] Telecommunications systems can also be used for harassing, threatening or intrusive communications, from the traditional obscene telephone call to its contemporary manifestation in "cyberstalking", in which persistent messages are sent to an unwilling recipient. In one case a Melbourne resident was accused of stalking a woman in Canada by sending letters, email messages and using the telephone and the internet. The Canadian woman

complained to police in Toronto who referred the case to Victoria police. The case went on appeal to the Supreme Court over the question of jurisdiction but it was held that the defendant could be dealt with in Victoria even though the victim was located in Canada (Smith, Grabosky & Urbas 2004: 222).

In another case a rejected suitor in Los Angeles posted invitations on the internet under the name of a 28-year old woman, the would-be object of his affections, saying that she had fantasies of rape and gang rape. He then communicated via email with men who replied to the solicitations and gave out personal information about the woman, including her address, phone number, details of her physical appearance and how to bypass her home security system. Strange men turned up at her home on six different occasions and she received many obscene phone calls. While the woman was not physically assaulted, she would not answer the phone, was afraid to leave her home, and lost her job (Raney 1999).

Identity crime

[12.240] Theft and misuse of personal information have become increasingly commonplace in the 21st century (Smith 2010a). Simple instances may involve the theft and subsequent use of a credit card, while more elaborate schemes involve hacking into databases of personal information and incurring liabilities in the name of an unsuspecting individual or business. The aim, invariably, is to obtain some financial benefit dishonestly, although often offenders seek simply to disguise their identity – making detection and prosecution of a range of crimes difficult. In the past, forgery of documents used to provide evidence of identity was a highly skilled task which few criminals were able to undertake convincingly. Since the advent of digital technologies, however, it is much easier to scan an official document electronically, alter the image as it appears on a screen, and print out a counterfeit version using high quality laser, colour printers – all from the comfort of one's home office. In Australia, identity-related fraud has recently been estimated to cost \$1.1 billion a year (Cuganesan & Lacey 2003).

Dialogue box 12.3

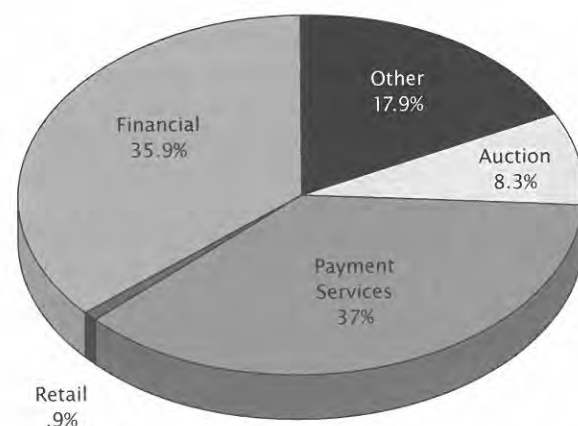
Identity-related crime

[12.250] One of the most prolific identity crime offenders, Albert Gonzalez, was indicted in multiple cases, including the *Shadowcrew* case (1.5 million data items stolen), the *TJX Companies* case (46 million) and the *Heartland Payment Systems* case (130 million). The stolen information, in addition to being used to withdraw cash from ATMs, was sold to conspirators in Eastern Europe. His guilty plea resulted in a forfeiture order of US\$1.6 million along with other assets (United Nations Office on Drugs and Crime 2010, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (UNODC, Vienna), p 208).

Phishing

[12.260] A recent form of online identity fraud is so-called “phishing” which involves the use of spam emails asking online banking customers to click on a hyperlink in the message to confirm their bank account details, passwords and to provide other personal information. If they do so, they are diverted to the offender’s website where the personal information is captured. There has been a substantial increase in the number of phishing cases since the year 2000. An industry group, the Anti-Phishing Working Group, has been collecting data on phishing since December 2003. In December 2003, 113 unique phishing attacks were reported, with eBay and Citibank being the two most targeted brands. By March 2010, this had increased to 30,577 unique phishing attacks being reported with 29,879 unique websites detected (Anti-Phishing Working Group 2010: 4). The most targeted industry sector was payment services in March 2010, followed by financial services (Figure 12.2).

Figure 12.2 Most targeted industry sectors for phishing, first quarter 2010



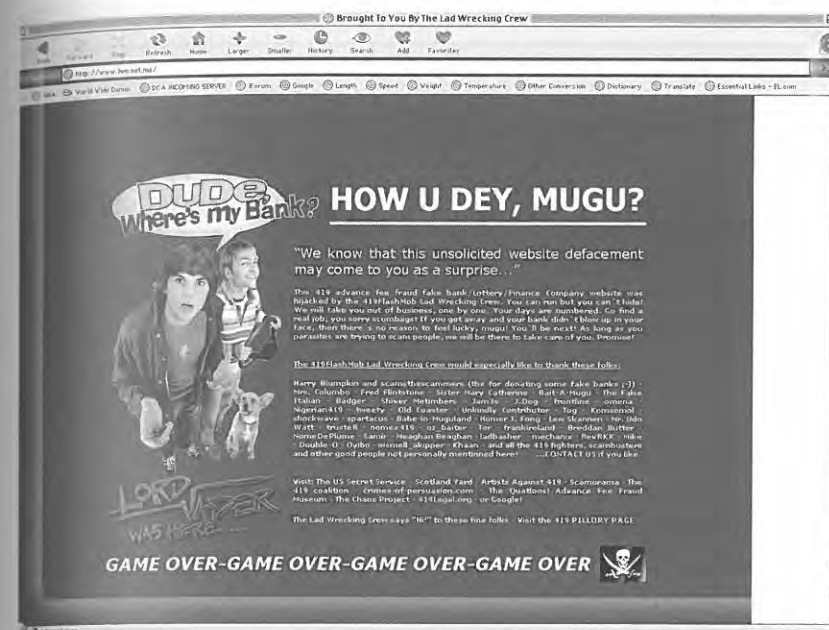
Source: Anti-Phishing Working Group (2010: 7)

Some hackers have acted as vigilante groups, illegally defacing sites that they think are conducting phishing operations.

Spam

[12.270] The problem of spam generally is extensive. Spam is defined as unsolicited commercial email messages. At present, as much as 65% of all email is spam which leads to productivity losses for businesses each year and is increasingly being used for the commission of crime. About 95% of spam is concerned with marketing the provision of goods and/or services and some 60% of spam messages originate from the United States (McCusker 2005b).

This computer screen shot from www.lwc.net.ms/ shows a website “Dude, where’s my bank” from the British hacker group called the Lad Wrecking Crew.



Source: Newspix

Spam may not only contain dishonest content, but can also contain Trojans and other viruses.

Cyber terrorism

[12.280] Cyber terrorism involves premeditated, politically motivated attacks on computer systems for the purpose of political intimidation or, alternatively, for purposes of coercion. Related acts include the use of digital technology by terrorists for recruitment, training and dissemination of propaganda (in addition to financing of terrorist activities and money laundering). To date, most activity has involved ancillary activities using technology, rather than actual electronic attacks against infrastructure. For example, in Australia, Faheem Khalid Lohdi was convicted of plotting to bomb Australia’s national electricity grid in October 2003 and sentenced to 20 years in prison for acts including downloading electricity grid maps from the internet (*R v Lohdi* [2006] NSWSC 691).

Security vulnerabilities in computer systems are ideal targets for cyber terrorists, particularly auto-executables such as ActiveX controls and JavaScript. Institutional computer systems, such as those on which governments and the military depend, have also been subjected to increasingly sophisticated attacks,

some of which appear to be politically motivated. In addition, other forms of cyber crime such as identity theft and online fraud may be used by terrorists (both cyber and conventional) to conceal or support their activities (Urbas 2005). Computers can also be used by terrorists to communicate with each other, to maintain data bases of information and intelligence, and the internet can be used as a source of information such as how to manufacture bombs (Denning 2010). The terrorist attacks on 11 September 2001 drew formal attention to the use which the terrorists made of electronic funds transfers as well as informal remittance systems. The bulk of funding for the 9/11 attacks was transferred through the formal banking system via wire transfers and credit cards although the 9/11 Commission's report maintained that Osama Bin Laden relied generally on established *hawala* networks operating in Pakistan, Dubai and throughout the Middle East. The Indian procedure of *hawala* involves the transfer of the value of currency without physically relocating it by exchanging value through trusted intermediaries independent of the regulated banking environment (Rees 2010).

Mobile communications

[12.290] Recent technological developments now enable transactions to be conducted through the use of mobile telephones and messaging services. Examples include the use of wireless devices to gain access to banking accounts and to pay bills, to receive stock quotes and to initiate, buy or sell transactions, or to receive special promotions and to generate orders from any place at any time. M-Commerce transactions might increase the impulsiveness and immediacy of transactions, and the absence of a cooling-off period could result in some consumers engaging in transactions that superficially appear sound but which in fact involve deception and are difficult, if not impossible, to undo. An added concern relates to the theft of portable hardware such as mobile telephones and hand-held computers. Unless secured by appropriate authentication devices, a stolen phone could enable a thief to access considerable amounts of personal information about its owner, including bank account numbers and other key identifying details. Mobile technologies are especially popular with young users who may be more easily targeted by criminals.

Identity crime facilitated through the internet is also beginning to be perpetrated through wireless communication systems, some of which have less robust security measures in place than desktop PCs. In one survey conducted by AusCERT of the security measures used by a sample of 1,001 adult home computer users with internet access in Australia, it was found that 16% of those surveyed used insecure wireless networks, with 5% of those surveyed admitting to using a neighbour's wireless connection (AusCERT 2008).

The term "war driving" has been coined to refer to the act of locating and logging wireless access points (or "hot spots") while in motion. Toward the end of 2003, one began to see prosecutions for unauthorised access to

wireless systems from "mobile hackers". In November of that year, two men in Michigan were charged with cracking a home improvement store's nationwide network from a car parked outside one of the stores (Poulsen 2003). There are also concerns that some SMS messages may not be adequately encrypted on servers.

Future risk areas

[12.300] The most recent area of cyber crime risk concerns manipulation and compromise of cloud computing systems. Cloud computing can be defined as a pool of virtualised computing resources that allows users to gain access to applications and data in a web-based environment on demand. Crime risks in this area arise in each of the various cloud architecture and usage models that have been developed (Choo 2010). In one study, for example, a team of computer scientists from the University of California, San Diego and Massachusetts Institute of Technology examined the widely-used Amazon EC2 services. It was found to be possible to map the internal cloud infrastructure, identify where a particular target virtual machine is likely to reside, and then instantiate new virtual machines until one is placed co-resident with the target. This enabled the research team to load eavesdropping software onto the same servers hosting targeted websites. By identifying target virtual machines, attackers could potentially monitor the cache (a small allotment of high-speed memory used to store frequently-used information) in order to steal data hosted on the same physical machine. This represents just one of a number of potential crime risks that face cloud infrastructure in the years ahead (Choo 2010).

In relation to computer-facilitated fraud, attacks are moving away from large operations such as global spam attacks to smaller, more focused attacks on particular individuals who receive personally addressed invitations. Phishing will move to Voice over Internet Protocol (Vishing) and mobile SMSs (SMiShing) where phishing filters are less effective. Context-aware phishing will also emerge with images and content more easily able to trick users (Smith 2010b: 231).

Theft of virtual property from Social Networking Sites such as *World of Warcraft* and *Second Life* will also take place (Warren and Palmer 2010). For example, police in China have investigated cases of virtual theft, including instances of organised gangs engaging in online robbery. In 2006, officers from Shenzhen arrested more than 40 suspects who were accused of stealing up to 700,000 yuan worth of virtual items from users of the social networking site "QQ" (Johnson 2007).

Countering cyber crime

[12.310] There are, arguably, three precursors to the commission of most crimes. These are the presence of a motivated offender, an available opportunity

to act illegally (or the presence of a suitable target), and the absence of a capable guardian or someone who might prevent the crime from being committed (Cohen & Felson 1979: 589). Although motivations for acting illegally may well have remained fairly constant over time, technological developments have created many new opportunities for people to act illegally. At the same time, the computer security industry has also increased its capacity as “electronic capable guardians”.

The criminal justice system is not, however, always effective in controlling crime, and crime prevention requires the contribution of a wide range of stakeholders. Law enforcement agencies, regulators, legislators, the information technology industry (including carriers, ISPs, and hardware and software manufacturers), businesses, educational bodies, public interest groups including the media, and, most importantly, computer users themselves all play a role in regulating cyberspace.

The traditional response has been to devise a range of situational measures (Chapter 23) that seek to make the commission of crime less attractive to potential offenders. Such measures aim to increase the levels of effort and skill required to commit offences, to create a greater risk of apprehension of offenders, and to decrease the potential rewards that offenders seek to derive from their illegal activities. Smith, Wolanin and Worthington (2003) have summarised the various crime prevention measures designed to reduce cyber crime employing the categorisation of traditional crime prevention measures developed by Clarke (1995: 109; see also Newman and Clarke 2003). Table 12.1 shows some of the possible situational strategies that have been used to prevent cyber crime.

Table 12.1 Situational cyber crime prevention measures

Crime prevention measure	Cyber crime application
Increasing the effort	
Target hardening	Firewalls, tempest security (against electro-magnetic radiation scanning), laptop anti-theft devices
Access control	Passwords, tokens, biometrics and encryption
Deflecting offenders	Use of computer games and the internet
Controlling facilitators	Registration of computer users with Public Key Registration Authorities, ISPs, and carriers
Increasing the risks	
Entry / exit screening	Checks on use of passwords
Formal surveillance	Analysis of usage patterns using neural networks to analyse transaction patterns

Surveillance by employees	Workplace PC surveillance using CCTV
Natural surveillance	Reporting of colleagues by IT personnel, reporting hotlines

Reducing the rewards

Target removal	Government or industry funded services
Identifying property	Registration of computer hardware
Removing inducements	Restricted publicity of crimes
Rule setting	Codes of conduct for internet usage

The importance of prevention

[12.320] The trite homily that prevention is better than cure is nowhere more appropriate than in cyberspace. It is unwise to leave one’s house unlocked when heading off to work in the morning. It is equally foolish to leave one’s information systems accessible to unauthorised persons. Prevention takes a variety of forms, including risk analyses of information systems and the creation of effective policies and procedures to protect them from damage or misuse. Each workplace should have policies to guard against misuse of information systems by employees. Individual users should have basic anti-virus software. Large institutions should have appropriate security technologies in place. Perhaps the simplest strategy is to exercise care with personal information such as passwords and PINs – which often are used as the pivotal link in a chain of deception.

Self-help

[12.330] Another key principle in the prevention of digital crime is the need to raise awareness on the part of prospective victims to the risks that they face. Individuals and institutions should be made aware of the potential consequences of an attack on their information assets, and of the basic precautionary measures that they should take. Although financial institutions may need to expend many millions of dollars in devising fraud resistant technologies, individual consumers can simply “say no” to the many attractive offers that fraudsters make online. This is the principal message that consumer fraud awareness campaigns promote, such as those conducted by the Australasian Consumer Fraud Taskforce (www.scamwatch.gov.au).

The use of non-governmental resources

[12.340] With diminishing state resources to control crime, it is desirable to enlist the assistance of private sector and community interests in the prevention and detection of digital crime. Information security specialists can

advise individual and organisational clients about risks and can recommend preventive measures. Passwords or biometric technologies of authentication, such as finger prints or retinal images, can help to guard against unauthorised use. Virus checkers or intrusion detection software can protect against a hacker attack. Objectionable content can be addressed at the individual level by blocking and filtering software, which can prevent access to certain types of sites.

Enhancing the capacity of law enforcement

[12.350] As new technologies are exploited by criminals, it becomes important for law enforcement not to be left behind. This is a significant challenge, given the emerging trend for skilled investigators to be “poached” by the private sector. The collaboration of law enforcement with specialised expertise residing in the private sector will be a common feature in years to come. It will also be important for public and private sector managers to develop close ties with law enforcement, to report suspected illegality to them, as well to provide them with assistance when required. One key initiative is to co-ordinate services available for the reporting of victimisation – which can help in gathering intelligence that can be crucial to the identification of new risks as they emerge. The Australian Federal Police’s High Tech Crime Operations Division, which is staffed by law enforcement personnel who work with private sector investigators, provides a useful model.

The importance of international co-operation

[12.360] The global nature of cyberspace necessitates the development of new strategies to combat criminal activity which can originate from the other side of the world. The basic approach to overcoming the transnational issues of digital crime lies in developing co-operation between nations (Chapter 26). Enlisting the assistance of overseas authorities is not an automatic process, and often requires pre-existing agreements relating to formal mutual assistance in criminal matters. Nevertheless, there are numerous examples of successful measures, and the web of mutual assistance is being woven ever more tightly. Examples include the work of the United Nations Office on Drugs and Crime (2009) which is developing normative approaches to dealing with identity crime, the Anti-Phishing Working Group (2010) which is a collaborative industry group established to respond to phishing, and the Joint London Action Plan and Contact Network of Spam Authorities which includes two prominent international anti-spam enforcement networks: the London Action Plan and the European Contact Network of Spam Enforcement Authorities. These groups focus on promoting international enforcement co-operation on spam, spyware, and other internet-related issues, including exploring new models for public-private co-operation and facilitating the exchange of information and intelligence among enforcement agencies (see www.londonactionplan.org/).

CONCLUSION

[12.370] The shrinking world created by ICT has benefits and costs. Many people, especially in affluent nations, now enjoy economic, cultural, and recreational opportunities that were previously inaccessible to them. On the other hand, the rapid movement of people, money, information, ideas, and commodities, has provided new opportunities for crime. We have identified and illustrated the varieties of cyber crime and the problems and potentials for law enforcement and crime prevention. The main danger arising from zealous enforcement and crime prevention is over-regulation. This may chill investment and innovation. There is a need to seek a balance between a tolerable degree of illegality and creative development of new technologies.

QUESTIONS

1. How might we measure the scope and financial impact of cyber crime?
2. On which cyber crimes should police focus their investigations? Why?
3. To what extent can preventive measures and the market place provide better solutions to the problems of cyber crime than legal interventions?
4. Drawing on the material on the websites below, explain how and why Nigerian or 419 scams work
5. Explain how the latest technological developments could be misused by criminals in the future, and how these risks could best be prevented.

REFERENCES

- Anti-Phishing Working Group 2010, *Phishing Activity Trends Report* – 1st quarter 2010 (San Francisco), www.antiphishing.org/reports/apwg_report_Q1_2010.pdf (accessed 7 January 2011).
- AusCERT 2008, *Home Users Computer Security Survey* (AusCERT, Brisbane).
- Australian Institute of Criminology 2008, “Intellectual Property Crime and Enforcement in Australia”, *Research and Public Policy Series*, no 94 (Canberra).
- Bamford, J 2008, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (Doubleday, New York).
- Bauer, J 1998, “Testimony to the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary” (United States Senate, 20 May), www.securitymanagement.com/library/bauer.html (accessed 7 January 2011).
- Bell, RE 2002, “The Prosecution of Computer Crime”, *Journal of Financial Crime*, vol 9, no 4, pp 308–325.
- Butcher, S 2001, “Ban urged on Internet bomb ‘recipes’”, *The Age* (Melbourne), 17 January, p 7c.

- Cella, JJ & Stark, JR 1997, "SEC enforcement and the Internet: Meeting the challenge of the next millennium", *The Business Lawyer*, no 52, pp 815–849.
- Choo, K-KR 2010, "Cloud Computing: Challenges and Future Directions", *Trends and Issues in Crime and Criminal Justice*, no 400 (Australian Institute of Criminology, Canberra).
- Choo, K-KR, Smith, RG & McCusker, R 2007, "Future Directions in Technology-enabled Crime: 2007–09", *Research and Public Policy Series*, no 78 (Australian Institute of Criminology, Canberra), pp 1–131.
- Clarke, RV 1995, "Situational crime prevention" in Tony, M & Farrington, DP (eds), *Building a Safer Society: Strategic Approaches to Crime Prevention* (University of Chicago Press, Chicago), pp 91–150.
- Cohen, LE & Felson, M 1979, "Social Change and Crime Rate Trends: A Routine Activity Approach", *American Sociological Review*, vol 44, pp 588–608.
- Cuganesan, S & Lacey, D 2003, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent* (SIRCA, Sydney).
- Cullinane, S & Jones, A 2011, "Phone-hacking Row as it Happened", *BBC News*, 18 July, www.bbc.co.uk/news/uk-14183281 (accessed 19 July 2011).
- Denning, D 2010, "Terror's Web: How the Internet is Transforming Terrorism", in Jewkes, Y & Yar, M (eds), *Handbook of Internet Crime* (Willan Publishing, Cullompton), pp 194–213.
- Despoja, NS 2008, *Youth Poll 2008*, www.natashastottdespoja.com/cms_resources/Youth%20Poll%20May%202008.pdf (accessed 7 January 2011).
- Gold, S 1999, "BT Starts Switchboard Anti-hacking Investigation", *Newsbytes*, 11 January, www.infowar.com/, (accessed 7 January 2011).
- Grabosky, PN 2007, *Electronic Crime* (Pearson Prentice Hall, Upper Saddle River NJ).
- Grabosky, PN & Smith, RG 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (Federation Press, Sydney).
- Grabosky, PN & Smith, RG 1997, "Telecommunications and Crime: Regulatory Dilemmas", *Law and Policy*, vol 19, no 3, pp 317–341.
- Grabosky, PN, Smith, RG & Dempsey, G 2001, *Electronic Theft: Crimes of Acquisition in Cyberspace* (Cambridge University Press, Cambridge).
- Johnson, B 2007, "Virtual Robber Nabbed for Real", *The Age* (Melbourne), 16 November, www.theage.com.au/news/world/virtual-robber-nabbed-for-real/2007/11/15/1194766867217.html (accessed 7 January 2011).
- Krone, T 2004, "A typology of online child pornography offending", *Trends and Issues in Crime and Criminal Justice*, no 279 (Australian Institute of Criminology, Canberra), www.aic.gov.au/publications/tandi2/tandi279.html (accessed 7 January 2011).
- Krone, T 2005a, "International Police Operations against Online Child Pornography", *Trends and Issues in Crime and Criminal Justice*, no 296 (Australian Institute of Criminology, Canberra), www.aic.gov.au/publications/tandi2/tandi296.html (accessed 7 January 2011).
- Krone, T 2005b, "Phishing", *High Tech Crime Brief*, no 9 (Australian Institute of Criminology, Canberra), www.aic.gov.au/publications/htcb/htcb009.html (accessed 7 January 2011).
- Littman, J 1997, *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen* (Little Brown, Boston).
- McAfee 2008, *McAfee Virtual Criminology Report: Cybercrime versus Cyberlaw* (McAfee Santa Clara, CA).
- McCusker, R 2005, "Spam: Nuisance or Menace, Prevention or Cure?", *Trends and Issues in Crime and Criminal Justice*, no 294 (Australian Institute of Criminology, Canberra), www.aic.gov.au/publications/tandi2/tandi294.html (accessed 7 January 2011).
- Markoff, J 2009, "Tracking Cyberspies Through the Web Wilderness", *The New York Times*, 29 May, www.nytimes.com/2009/05/12/science/12cyber.html?scp=106&sq=dalai+lama&st=nyt (accessed 7 January 2011).
- Mitnick Security Consulting 2004–2005, Home Page, www.kevinmitnick.com/ (accessed 7 January 2011).
- Moses A 2010, "Operation Titstorm: Hackers Bring Down Government Websites", *Sydney Morning Herald*, 10 February, www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-websites-20100210-nqku.html (accessed 7 January 2011).
- Munk Centre for International Studies 2009, *Tracking GhostNet: Investigating a Cyber Espionage Network* (Munk Centre, Toronto), www.nartv.org/mirror/ghostnet.pdf (accessed 7 January 2011).
- Nasheri, H 2005, *Economic Espionage and Industrial Spying* (Cambridge University Press, Cambridge).
- New South Wales Police Force 2009, "Police and eBay Smash Multi-million Dollar Fraud Syndicate", *Media Release*, 10 March (Sydney).
- Newman, G & Clarke, RV 2003, *Superhighway Robbery: Preventing E-commerce Crime* (Willan Publishing, Cullompton).
- Poulsen, K 2003, "Wireless Hacking Bust in Michigan", *Security Focus*, November 12, www.securityfocus.com/news/7438 (accessed 7 January 2011).
- Raney, RF 1999, "Internet Stalking Case Ends in Plea", *New York Times*, 29 April, www.nytimes.com/library/tech/99/04/cyber/articles/29stalk.html (accessed 7 January 2011).
- Rathmell, A 1997, "Cyber-terrorism: The Shape of Future Conflict?", *Royal United Services Institute Journal*, October, pp 40–46.
- Reeckman, B & Cannard, L 2009, "Cyberbullying: A TAFE Perspective", *Youth Studies Australia*, vol 28, no 2, pp 41–49.
- Rees, D 2010, "Money Laundering and Terrorism Financing Risks Posed by Alternative Remittance in Australia", *Research and Public Policy Series*, no 106 (Australian Institute of Criminology, Canberra).
- Richards, K 2009, "The Australian Business Assessment of Computer User Security: A National Survey", *Research and Public Policy Series*, no 102

- (Australian Institute of Criminology, Canberra).
- Shane, S & Lehren, AW 2010, "Leaked Cables Offer Raw Look at U.S. Diplomacy", *The New York Times*, 28 November, www.nytimes.com/2010/11/29/world/29cables.html?hp (accessed 7 January 2011).
- Smith, RG 1998, "The Regulation of Telemedicine", in Smith, RG (ed), *Health Care, Crime and Regulatory Control* (Hawkins Press, Sydney), pp 190–203.
- Smith, RG 2010a, "Identity Theft and Fraud", in Jewkes, Y & Yar, M (eds), *Handbook of Internet Crime* (Willan Publishing, Cullompton), pp 273–301.
- Smith, RG 2010b, "The Development of Cybercrime", in Lincoln, R & Robinson, S (eds), *Crime Over Time: Temporal Perspectives on Crime and Punishment in Australia* (Cambridge Scholars Publishing, Newcastle upon Tyne), pp 211–236.
- Smith, RG & Budd, C 2010, "Consumer Fraud in Australia: Costs, Rates and Awareness of the Risks in 2008", *Trends and Issues in Crime and Criminal Justice*, no 382 (Australian Institute of Criminology, Canberra).
- Smith, RG, Grabosky, PN & Urbas, GF 2004, *Cyber Criminals on Trial* (Cambridge University Press, Cambridge).
- Smith, RG, Holmes, MN & Kaufmann, P 1999, "Nigerian advance fee fraud", *Trends and Issues in Crime and Criminal Justice*, no 121 (Australian Institute of Criminology, Canberra), www.aic.gov.au/publications/tandi/tandi121.html (accessed 7 January 2011).
- Smith, RG, Wolanin, N & Worthington, G 2003, "E-crime Solutions and Crime Displacement", *Trends and Issues in Crime and Criminal Justice*, no 243 (Australian Institute of Criminology, Canberra), www.aic.gov.au/publications/tandi/tandi243.html (accessed 7 January 2011).
- Stoll, C 1991, *The Cuckoo's Egg* (Pan Books, London).
- Symantec 2009, *Symantec Global Internet Security Threat Report Trends for 2008: vol xiv*, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (accessed 7 January 2011).
- United Nations Office on Drugs and Crime 2009, *International Cooperation in the Prevention, Investigation, Prosecution and Punishment of Economic Fraud and Identity-related Crime*, Report of the Secretary-General, E/CN.15/2009/1 (Commission on Crime Prevention and Criminal Justice Eighteenth Session, Vienna).
- United Nations Office on Drugs and Crime 2010, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (UNODC, Vienna).
- United States Department of Justice 2010, "Two Engineers Found Guilty of Stealing Goodyear Trade Secrets" (Computer Crime & Intellectual Property Section, Department of Justice, Washington), www.cybercrime.gov/howleyPlea.pdf (accessed 7 January 2011).
- Urbas, G 2005, "Cyber Terrorism and Australian Law", *Internet Law Bulletin*, vol 8, no 1, pp 5–8.
- Wall, DS 2010, "Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'", in Jewkes, Y & Yar, M (eds), *Handbook of Internet Crime*

- (Willan Publishing, Cullompton), pp 83–103.
- Warren, I & Palmer, D 2010, "Crime Risks of Three-dimensional Virtual Environments", *Trends and Issues in Crime and Criminal Justice*, no 388 (Australian Institute of Criminology, Canberra).

FURTHER READING

- Casey, E 2000, *Digital Evidence and Computer Crime* (Academic Press, San Diego).
- Denning, D 1999, *Information Warfare and Security* (Addison Wesley, Boston).
- Grabosky, PN 2007, *Electronic Crime* (Pearson Prentice Hall, Upper Saddle River NJ).
- Grabosky, P & Smith, RG 1998, *Crime In the Digital Age* (Federation Press, Sydney).
- Grabosky, P, Smith, RG & Dempsey, G 2001, *Electronic Theft: Crimes of Acquisition in Cyberspace* (Cambridge University Press, Cambridge).
- Jewkes, Y & Yar, M (eds) 2010, *Handbook of Internet Crime* (Willan Publishing, Cullompton), pp 194–213.
- Power, R 2000, *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace* (Que Books, Indianapolis).
- Smith, RG, Grabosky, PN & Urbas, GF 2004, *Cyber Criminals on Trial* (Cambridge University Press, Cambridge).

USEFUL WEBSITES

- www.aic.gov.au/en/crime_types/cybercrime.aspx
Australian Institute of Criminology publications on cyber crime
- www.scamwatch.gov.au
Website of the Australian Competition and Consumer Commission and the campaign portal for the Australasian Consumer Fraud Taskforce
- www.antiphishing.org
Website of the Anti-phishing Working Group
- www.cybercrime.gov
Website of the Computer Crime & Intellectual Property Section of the United States Department of Justice
- www.cybercrimeforum.org
Website of the Virtual Forum against Cybercrime
- www.anu.edu.au/people/Roger.Clarke
Roger Clarke's Home Page: Australian content on electronic commerce and information privacy

www.cyber-rights.org

Cyber crime from a United Kingdom and civil liberties perspective

www.infowar.com

An encyclopaedic collection of materials on computer crime and information warfare

www.cs.georgetown.edu/~denning

Dorothy Denning's Home Page with links relating to computer security

www.webcrunchers.com/crunch/Play/history/home.html

John Draper's website on Phone Phreaking

www.universityofnigeria.com

Satirical response to advanced fee electronic frauds

www.419legal.org

South African Police Services site on 419 scams

NOTE

- 1 Opinions expressed in this chapter are those of the authors and not necessarily those of the Australian Institute of Criminology or the Australian Government.

13

Crimes across borders

Andrew Goldsmith, University of Wollongong

<i>Key Words</i>	275
<i>Introduction</i>	275
Understanding transnational crime	276
Major kinds of transnational crime	282
<i>Conclusion</i>	295
<i>Questions</i>	296
<i>References</i>	297
<i>Further reading</i>	300
<i>Useful websites</i>	301
<i>Note</i>	301

Key words transnational crime, money-laundering, terrorism, illicit drugs, arms smuggling, people trafficking, people smuggling, global village

INTRODUCTION

Breaking down borders

[13.10] Until recently, crime was mainly viewed as a domestic problem. That is, each country has defined its own crimes using domestic criminal law to do so, and responded to the occurrence of such crimes using its own justice processes. Until well into the 20th century, almost all crimes were local in nature, committed by citizens or other entities (eg, a corporation) of a nation-state against fellow citizens or other entities of the same state. Many such crimes would be committed against those who lived in the same town, village, or urban neighbourhood. Today however, crimes can be committed against persons in other countries. Modern systems of communication and transportation have enabled crimes to be the victimisation of persons living on the other side of the globe. Email-based fraud is a good example of this kind of criminal capability in an increasingly connected world. Individual countries find these kinds of crime very difficult to tackle by themselves.