International Journal of Cyber Criminology
Vol 2 Issue 2 July - December 2008

Book Review of Cybercrime and Society[1]

Russel Smith[2]
Australian Institute of Criminology,[3] Australia

Cybercrime and Society Majid Yar (2006) London, Sage Publications, 185 pp, ISBNs 101412907535, 101412907543, 139781412907538, 139781412907545.

The last decade has seen not only a proliferation of instances of cybercrime take place globally, but also a substantial increase in public discussion, legislation, and policy debate concerning the use of computing and information technologies (ICT) in the commission of illegal activity. Until recently, universities around the world have remained on the periphery of cybercrime research and teaching, with most debate being conducted within policing and government circles. Majid Yar has, with Cybercrime and Society, successfully taken up the challenge of gathering current discourse on this topic into a single volume that can be used for teaching tertiary courses in criminology, sociology, media studies, policing, public policy and law.

There is no dearth of intrinsic interest in these topics, which cover child exploitation, consumer seams, online stalking and piracy, to name a few. Students in a range of disciplines will find the information presented in a clear and concise way with a number of novel tools to guide their study. These include individual chapter overviews, lists of key terms, an extensive glossary, study questions and directions for further reading. The model is similar to a number of other criminology texts, saves for the omission of photographs, website URLs, and boxed case studies, which could have been included. Nonetheless, the style is accessible and, for a high-tech topic, free of unnecessary jargon.

Although a welcome addition to teaching in Britain (its primary geographical and informational focus), the book has some limitations. It is, perhaps, unfair to level the criticism that some of the information is out of date, as the world of cybercrime moves at a rapid pace. Although published in January 2006, it is a pity that some of the most recent and intriguing high-tech crime issues are omitted. These include: the crime risks associated with the use of mobile and wireless technologies; online gaming; threats to critical infrastructure posed by individuals and organised groups with political or religious motivations; the latest malware threats arising from bots, kernel-mode software, and ransomware and risks associated with new payment systems including RFID-enabled

[1] Earlier published in the Australian and New Zealand Journal of Criminology (Publication Date: 01-DEC-07). Reprinted by permission of Australian Academic Press Pty. Ltd. COPYRIGHT 2007 Australian Academic Press Pty. Ltd.

[2] Principal Criminologist; Manager, Global, Economic and Electronic Crime Program, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601, Australia. Email: Russell.Smith@aic.gov.au

[3] "The views expressed are those of the author alone and not the Australian Government".

credit cards, to name a few. There will be, without doubt, a need for a second edition in the near future.

For policy makers and lawyers, the level of legislative and case law analysis is somewhat limited, although to do justice to this would require a different kind of book. Some further discussion of global normative initiatives could have been included, such as the Council of Europe's Convention on Cybercrime of 1 July 2004, and the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems of 1 March 2006. In addition, the work undertaken on behalf of the OECD and G8 countries, as well as the United Nations Working Group on Internet Governance deserve some mention, as do the recent attempts at improving mutual assistance in cross-border investigations by police. The second edition will also need to examine recent legislation designed to deal with spam, which has been introduced in a number of countries, and the new computer misuse provisions enacted in various jurisdictions including the United Kingdom (where the Police and Justice Act 2006 amended certain provisions of the Computer Misuse Act 1990 to deal with emerging cyberthreats). It is important that students and other readers be made aware of the efforts being made around the world to respond effectively to cybercrime on a number of fronts.

Perhaps the most important initiative in responding to cybercrime lies in the use of public and private sector partnerships. An example is the work undertaken by the International Centre for Missing and Exploited Children to combat online child abuse and child pornography. Under this joint initiative, Microsoft and the International Centre (http.//www.icmec.org/) have established links with over 30 financial institutions worldwide, including credit card companies, to develop a system that will monitor and report online commercial transactions involving crimes against children.

Students of quantitative criminology may also find the book lacking in critical analysis of the, admittedly, poor statistical information on cybercrime which currently exists globally. Majid Yar acknowledges this deficit but could have explored in greater depth the reasons why cybercrime statistics are so poor around the world at present. Not only do cybercrimes traverse traditional criminal offence categories with alacrity, thus making official crime statistics of little use, but the victimisation surveys that do exist are often superficial or promoted by those without sufficient distance from the outcomes they are seeking to achieve. A case in point, discussed in the book, is the assessment of financial loss attributed to online piracy, which a number of industry groups compile each year and which are often methodologically flawed and superficial in quantifying losses occasioned due to music and film piracy carried out online. A well chosen case study would illustrate the inadequacies of such calculations clearly. The problems of defining and quantifying the various categories of identity-related crime are also substantial, and could have been explored in greater depth. Cybercrime presents some wonderful examples of criminological debates, which students could be asked to unpack and to analyse. However, to do so they need to be alerted to the imprecise information and lack of analysis that currently pervades much of the academic cybercrime discourse.

The most intractable issue concerns the terminology used to describe cybercrime, which has parallels with the 80-year-old debate surrounding the meaning of white collar crime. Majid Yar provides a good introduction to the many and conflicting terms currently used to describe the phenomenon, but fails to provide an effective solution. Arguably the debate over whether information and communications technologies are

crime enablers or crime enhancers needs to be resolved, as does the question of how we should classify crimes in which ICT is incidental to the illegality. Theft of laptops may be a simple example to present as a type of crime that falls outside the definition of cybercrime, but what of online tax fraud in a world in which the vast majority of taxpayers now lodge official documents electronically? If they happen to be fraudulent, does this make the whole transaction one of cybercrime? What needs to be determined is the point at which the use of ICT becomes so important that we can no longer consider the conduct to fall within the concept of traditional crime, but one carried out in cyberspace.

The discussion of theory could also have been more extensive, particularly in a student text designed for courses in which theories of crime occupy such a large proportion of teaching time. Some attempt is made to explain how new forms of online criminality are constructed and how they come to be accepted as criminal. Theories based around ecological and individual approaches are also mentioned. There is, however, much that could be gained from exploring other approaches which might help to explain crimes that take place exclusively in cyberspace, such as the creation and dissemination of malware, or abuse of online gaming technologies. Asking students to consider the reasons why individuals may seek to exploit virtual multiplayer online games (e.g. Second Life) could provide an excellent platform for understanding more mundane forms of cybercrime such as cyberstalking or online scams.

Nonetheless, the description of the many aspects of cybercrime which are addressed is clear and largely up to date with good examples given and the work of most recognised scholars cited. Chapter 8 on cyberliberties was particularly well written and provided an excellent introduction to the debate concerning the over-reliance which many governments are placing on ICT for surveillance and control of their citizens in the 21st century, often without any evidence that this will bear fruit in terms of reduced deviance.

The book is largely free from factual errors (note that the National High Tech Crime Unit in the United Kingdom (p. 10) now forms part of the Serious Organised Crime Agency), although some references have mistakes (e.g. Forde & Patterson and Ogilvie each should be to publications in Trends and Issues in [Crime and] Criminal Justice). There are relatively few typographical and spelling errors (e.g. Advance[s] Fee p. 155).

On the whole, the book will be greatly appreciated by students of cybercrime around the world. It provides a sound and concise introduction to the field and gives a platform for further research and debate. The challenge for Majid Yar in the second edition will be to keep pace, not so much with new forms of cybercrime as they emerge, but with the burgeoning growth in policy debate, government reports, legislation and technical solutions to the problem.