THE INTERNATIONAL LIBRARY OF CRIMINOLOGY, CRIMINAL JUSTICE & PENOLOGY

SECOND SERIES

CRIME AND DEVIANCE IN CYBERSPACE

David S. Wall

Crime and Deviance in Cyberspace

Edited by

David S. Wall

University of Leeds, UK

ASHGATE

Published by
Ashgate Publishing Limited
Wey Court East
Union Road
Farnham
Surrey GU9 7PT
England

Ashgate Publishing Company
Suite 420
101 Cherry Street
Burlington, VT 05401-4405
USA

Ashgate website: http://www.ashgate.com

British Library Cataloguing in Publication Data
Crime and deviance in cyberspace. – (International library of criminology, criminal justice and penology. Second series)
1. Computer crimes 2. Computer crimes – Prevention
I. Wall, David, 1956–
364.1'68

Library of Congress Cataloging-in-Publication Data
Crime and deviance in Cyberspace/edited by David S. Wall.
p.cm. – (International library of criminology, criminal justice and penology : second series)
Includes index.
ISBN 978-0-7546-2453-0 (alk. paper)
1. Computer crimes. 2. Deviant behavior. 3. Internet–Social aspects. I. Wall, David, 1956–

HV6773.C74 2009
364.16'8–dc22

20080302797

ISBN: 978-0-7546-2453-0

Printed and bound in Great Britain by
TJ International Ltd, Padstow, Cornwall

Acknowledgements

The editor and publishers wish to thank the following for permission to use copyright material.

Canadian Journal of Sociology for the essay: Kevin D. Haggerty and Amber Gazso (2005), 'Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats', *Canadian Journal of Sociology*, **30**, pp. 169–87.

Copyright Clearance Center for the essay: Bruce Berkowitz and Robert W. Hahn (2003) 'Cybersecurity: Who's Watching the Store?', *Issues in Science & Technology*, **19**, pp. 55–62. Copyright © 2003 Issues in Science and Technology.

Crime and Justice International for the essay: Tony Krone (2005), 'International Police Operations Against Online Child Pornography', *Crime and Justice International*, **21**, pp. 11–20.

Elsevier for the essays: G.T. Marx (2001), 'Technology and Social Control', *International Encyclopedia of the Social and Behavioral Sciences*, pp. 15506–12. Copyright © 2001 Elsevier; Peter Sommer (2004), 'The Future for the Policing of Cybercrime', *Computer Fraud & Security*, **1**, pp. 8–12. Copyright © 2004 Elsevier.

Emerald Group for the essay: Roderic Broadhurst (2006) 'Developments in the Global Law Enforcement of Cyber-crime', *Policing: An International Journal of Police Strategies and Management*, **29**, pp. 408–33. Copyright © 2006 Emerald Group.

Journal of Technology Studies for the essay: Sam McQuade (2006), 'Technology-enabled Crime, Policing and Security', *Journal of Technology Studies*, **32**, pp. 32–42.

Bert-Jaap Koops and Ronald Leenes (2006), 'Identity Theft, Identity Fraud, and/or Identity-related Crime. Definitions Matter', *Datenshutz und Datensicherheit*, **30**, pp. 553–56. Copyright © 2006 Bert-Jaap Koops and Ronald Leenes.

North Carolina Journal of Law and Technology for the essay: Susan W. Brenner (2002), 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships', *North Carolina Journal of Law and Technology*, **4**, pp. 1–50.

Sage Publications for the essays: Majid Yar (2005) 'The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory', *European Journal of Criminology*, **2**, pp. 407–27. Copyright © 2005 Sage Publications; Sheila Brown (2006), 'The Criminology of Hybrids: Rethinking Crime and Law in Technosocial Networks', *Theoretical Criminology*, **10**, pp. 223–44. Copyright © 2006 Sage Publications; Lorine A. Hughes and Gregory J. DeLone (2007), 'Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?',

Social Science Computer Review, **25**, pp. 78–98. Copyright © 2007 Sage Publications; David S. Wall and Matthew Williams (2007), 'Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities', *Criminology and Criminal Justice*, **7**, pp. 391–415. Copyright © 2007 Sage Publications; Helen Nissenbaum (2004), 'Hackers and the Contested Ontology of Cyberspace', *New Media & Society*, **6**, pp. 195–217. Copyright © 2004 Sage Publications; Francesca Philips and Gabrielle Morrissey (2004), 'Cyberstalking and Cyberpredators: A Threat to Safe Sexuality on the Internet', *Convergence*, **10**, pp. 66–79. Copyright © 2004 Sage Publications; Giselinde Kuipers (2006), 'The Social Construction of Digital Danger: Debating, Defusing and Inflating the Moral Dangers of Online Humor and Pornography in the Netherlands and the United States', *New Media & Society*, **8**, pp. 379–400. Copyright © 2006 Sage Publications; Jerry Finn (2004), 'A Survey of Online Harassment at a University Campus', *Journal of Interpersonal Violence*, **19**, pp. 468–83. Copyright © 2004 Sage Publications.

Spiked Journal for the essays: Sandy Starr (2004), 'Can the Law Can Spam? Legislation is a Blunt Instrument with Which to Beat Junk Email', *Spiked*, **April**, pp. 1–4. Copyright © 2004 Spiked; Sandy Starr (2004), 'Can Technology Can Spam? IT Companies Do Battle with Bulk Email', *Spiked*, **May**, pp. 1–5. Copyright © 2004 Spiked.; Barbara Hewson (2003), 'Fetishising Images', *Spiked*, **January**, pp. 1–8. Copyright © 2003 Spiked.

Springer for the essays: David S. Wall (2005), 'Digital Realism and the Governance of Spam as Cybercrime', *European Journal on Criminal Policy and Research*, **10**, pp. 309–35. Copyright © 2005 Springer; Gregor Urbas (2006), 'Cross-National Investigation and Prosecution of Intellectual Property Crimes: The Example of "Operation Buccaneer"', *Crime, Law and Social Change*, **46**, pp. 207–21. Copyright © 2006 Springer; Jonathan Clough (2008), 'Now you See it, Now you Don't: Digital Images and the Meaning of "Possession"', *Criminal Law Forum*, **19**, pp. 205–39. Copyright © 2008 Springer. Ronald V. Clarke (2004), 'Technology, Criminology and Crime Science', *European Journal on Criminal Policy and Research*, **10**, pp. 55–63. Copyright © 2004 Springer; Peter Grabosky (2007), 'Requirements of Prosecution Services to Deal with Cyber Crime', *Crime, Law and Social Change*, **47**, pp. 201–23. Copyright © 2007 Springer.

Taylor and Francis for the essays: Briavel Holcomb, Philip B. Bakelaar and Mark Zizzamia (2003), 'The Internet in the Aftermath of the World Trade Center Attack', *Journal of Urban Technology*, **10**, pp. 111–28. Copyright © 2003 The Society of Urban Technology; Yvonne Jewkes and Carol Andrews (2005), 'Policing the Filth: The Problems of Investigating Online Child Pornography in England and Wales', *Policing and Society*, **15**, pp. 42–62. Copyright © 2005 Taylor & Francis; Benoît Dupont (2004), 'Security in the Age of Networks', *Policing and Society*, **14**, pp. 76–91. Copyright © 2004 Taylor & Francis; Peter Sommer (2004), 'The Future for the Policing of Cybercrime', *Computer Fraud & Security*, **1**, pp. 8–12, 12a. Copyright © 2004 Taylor & Francis.

Wiley-Blackwell for the essay: Jacqueline L. Schneider (2003), 'Hiding in Plain Sight: An Exploration of the Illegal(?) Activities of a Drugs Newsgroup', *Howard Journal of Criminal Justice*, **42**, pp. 374–89. Copyright © 2003 Blackwell.

Every effort has been made to trace all the copyright holders, but if any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangement at the first opportunity.

Preface to the Second Series

The first series of the International Library of Criminology, Criminal Justice and Penology has established itself as a major research resource by bringing together the most significant journal essays in contemporary criminology, criminal justice and penology. The series made available to researchers, teachers and students an extensive range of essays which are indispensable for obtaining an overview of the latest theories and findings in this fast-changing subject. Indeed the rapid growth of interesting scholarly work in the field has created a demand for a second series which, like the first, consists of volumes dealing with criminological schools and theories as well as with approaches to particular areas of crime criminal justice and penology. Each volume is edited by a recognized authority who has selected twenty or so of the best journal essays in the field of their special competence and provided an informative introduction giving a summary of the field and the relevance of the essays chosen. The original pagination is retained for ease of reference.

The difficulties of keeping on top of the steadily growing literature in criminology are complicated by the many disciplines from which its theories and findings are drawn (sociology, law, sociology of law, psychology, psychiatry, philosophy and economics are the most obvious). The development of new specialisms with their own journals (policing, victimology, mediation) as well as the debates between rival schools of thought (feminist criminology, left realism, critical criminology, abolitionism etc.) make it necessary to provide overviews that offer syntheses of the state of the art.

GERALD MARS
Honorary Professor of Anthropology, University College, London, UK

DAVID NELKEN
Distinguished Professor of Sociology, University of Macerata, Italy
Distinguished Research Professor of Law, University of Cardiff, Wales
Honorary Visiting Professor of Law, LSE, London, UK

Introduction

In my Introduction to *Cyberspace Crime*, the predecessor to this volume which covered the cybercrime literature up to 2001 (Wall, 2003), I observed that the Internet had developed way beyond our initial expectations. I also predicted that this trend of transformations in online criminal behaviour would continue as communications and information technologies further converge during the forthcoming decade. Well, almost a decade on, this prediction still holds true, and the trend has continued with some rather remarkable developments. Of course, this does not make the earlier observations any less valid because, like this volume, its predecessor addressed those forms of online offending that were, to varying degrees, the product of available networked technologies. But, by today's technical standards, then available networked technologies such as the dial-up modem and the very early forms of cable broadband now seem antiquated. Since the turn of the millennium, enhancements in Internet provision have considerably increased the rate that the information flows, and we are now discussing norms of 56mb, rather than 56kb per second, in service delivery, which technically (rather than practically) represents a 1000-fold increase in rate of flow. Whilst such improvements help Internet service providers cater for the bandwidth demands of the rapidly growing online population, they have also contributed to a number of distinctive changes in the ways in which we experience crime and deviance in the information age, all of which I hope to reflect in this volume.

The main change since the earlier volume has been the cybercrime wave that we have experienced since about 2002–03 onwards, which was caused by the automation of online crime through infections of multifunctioning malicious software or 'crimeware'. Once this crimeware has infected a computer, then a remote administrator can gain control over the machine and use it for various nefarious purposes. The power of this facility is amplified further when networks of these 'zombie' computers are constructed. These 'botnets' (after r*obot net*work) have, to all intents and purposes, further automated cybercrime. Moreover, by extending the reach of criminals and increasing their access to victims, the individual returns from the crime harvest (such as spam-related frauds) can now be smaller, but larger in aggregate. Not only has this change transformed the nature of online criminal behaviour by reducing the impact of individual victimizations, but it has also increased their geographical reach and span, causing important knock-on effects for criminal justice that are discussed later. New online criminal sub-economies have also emerged as a result of this automation – for example, the botnets themselves are now available for hire and the services of their owners (the bot-herders) are available on a pay-per computer infection basis. What is more, automation has also made the more legitimate online economies all the more criminogenic – for example, the development of online banking systems have stimulated information or identity theft and the development of online (pay per click) advertising systems have similarly become prone to 'click' frauds. These have been augmented, if not facilitated, by the growth in new digital environments for financial transactions (e-auction and banking sites) and social networking (Second Life), plus new interactive shared media sites such as *YouTube*'s video-

sharing service. These new environments also become fora for a range of different types of victimization, such as grooming, harassment and bullying.

The step-change upwards in ill-gotten gains from online criminal activity has meant that online offenders are no longer so eager to be visible. Whereas online offenders used to want to be known, be recognized, be revered and even be feared for their malign achievements, often advertising their expert services in the process, their modern counterparts seek precisely the opposite – total anonymity. It literally pays to be invisible today, and virtual stealth is becoming the name of the game. Towards this end there has been a discernible shift away from the use of spam as the means for delivering crimeware, towards the use of 'drive-by-downloads' from legitimate, but infected, www sites. This type of crimeware is now 'intelligent' enough to evade 'capture' by proprietary security software and then uninstall itself once its mission has been accomplished. Furthermore, attacks are becoming increasingly personalized as information about occupation, gender, age and area of residence is sorted, using analytical software to profile individuals into potential victim groups. These are some of the directions in which criminal behaviour online is currently heading at the time of writing. They are identifiable trends that contrast the positions at the beginning and end of this seven- or eight-year snapshot of the literature, and, of course, some of these changes are still too new to have yet been written about. Before exploring the contents of this volume let us first reflect upon what cybercrimes are and why we should be concerned about them.

What are Cybercrimes?

'Cyber-terrorism', 'information warfare', 'phishing', 'spams', 'denial of service attacks', 'hacktivism', 'hate crime', 'identity thefts', 'online gambling', plus the criminal exploitation of a new generation of pornographic peccadilloes, comprise the new language that describes the criminal and harmful behaviours that are conspiring to degrade the overall quality of life online and beyond. In so doing they pose significant threats to public safety that are tempering commercial and governmental ambitions to develop the information society.

Although 'cybercrime' is now an immensely topical and newsworthy subject, little contemporary information is known about its occurrence other than through news reportage. And although few commentators would now deny that cybercrimes exist there is still little overall consensus on what they actually are. Furthermore, whilst we do know more about them than we did previously, we still lack reliable sources of information and knowledge to counter the effects of misinformation as well as the various Internet mythologies that have arisen around cybercrimes: that the Internet is unsafe and pathologically criminogenic; that no-one is safe from the super-hacker; that cyber-criminals go unpunished; that the Internet corrupts and so on. Each of these mythologies can be challenged, yet persist as part of the cultural construction of cybercrime to obscure the emergence of more pressing matters of Internet security (Wall, 2008).

Without reliable information, misunderstandings about the Internet and cybercrime will perpetuate and weaken criminal justice policy on cybercrime. Particularly confusing is the tendency of reporters to regard almost any offence that involves a computer as a 'cybercrime'. This is not helped by conflicting media messages, which, on the one hand, demonize the Internet as a place where youngsters are groomed by paedophiles and upstanding citizens robbed of their identity, while, on the other hand, simultaneously depict it as a wonderland for enhanced

citizenship through improved personal, commercial and governmental communications. Furthermore, this malaise is not assisted by various academic and government endeavours to alternatively conceptualize similar issues either as 'virtual crime' (Brenner, 2001), 'cyberspace crime' (Wall, 2003), 'cybercrime' (Wall, 2007; Yar, 2006), 'net-crime' (Morris, 2004), 'hi-tech crime' (NCIS, 2002:s. 8) 'computer crime' (Walden, 2003), 'hypercrime' (McGuire, 2007) often using different quite different yardsticks.

As I have mentioned elsewhere, including in the previous Introduction (Wall, 2003, 2007), whatever its merits and demerits, the term 'cybercrime' has now entered the public parlance and we are stuck with it. The term cybercrime is now far too deeply entrenched in our vocabulary and culture to change. At best we can demystify it and seek to explain it to the public and other groups with a voice in cybercrime to encourage common understanding. To this end, I argue that the term has a greater meaning if it is understood in terms of the *transformation* of criminal or harmful acts by networked computing technologies, rather than the specific acts themselves (see, further, Wall, 2007). So, by applying a simple 'transformation test' to simply think about what would happen to the behaviour if the Internet were to be removed from it, three different types of 'transformed' cyber-criminal behaviour emerge as points on a spectrum that accommodate many of the previous attempts at conceptualization. This method also accommodates any major changes in, or convergences of, technology.

At the near end of the spectrum to established legal concepts of crime is the first generation of cybercrimes. These are behaviours that are often called cybercrimes, but are in fact 'traditional' crimes in which a computer has been used peripherally – usually as a method of networked communication or source of information to assist with the organization of a crime. They would include such offences as fraud within discrete computing systems or the seeking of information about potential victims and/or about how to harm them. In such cases, if the Internet is removed from the activity, the harmful behaviour will persist because offenders will simply revert to using other forms of easily available communication or information sources. Towards the middle of the spectrum are the second generation of 'hybrid' cybercrimes. These are 'traditional' crimes for which network technology has created entirely new opportunities across a globalized span. They would include offending behaviour that takes place across systems, such as global frauds and deceptions, and also the global trade in illegal pornographic materials. Take away the Internet in this case and the behaviour may continue by other means, but without the Internet-added benefits and therefore not with such great prevalence across such a wide span of jurisdictions and cultures. At the far end, however, lie the 'true' cybercrimes which are solely the product of opportunities created by the Internet and which can only be perpetrated within the digital environs of cyberspace. They include, amongst others, intellectual property piracy, spamming, phishing and, if we take away the Internet, they and the other true cybercrimes vanish.

Phishing is a particularly interesting example of a true cybercrime because it illustrates the rapid evolution of the practice in response to attempts to prevent it. Most of us will have some personal experience of phishing, because we have all at some time received bogus messages purporting to be from our banks that encourage us to log on to their websites to allegedly 'reaffirm' the personal information they hold about us. The sites are convincing, but fake, and by responding to these requests we unsuspectingly give away valuable personal information that can subsequently be used to defraud us. Some idea of the volume of identify theft cases can be obtained from CIFAS, the UK's fraud prevention service, whose statistics reveal 77 593

cases of identity fraud reported to them in 2007 (CIFAS, 2007). Many of these identity frauds were the product of online identity theft. Interestingly, these statistics represent a fall of –3.46 per cent on 2006, which suggests that online prevention measures are becoming effective. However, as recipients of phishing e-mails gradually become wise to the scams, phishing has evolved. First, it evolved into pharming (DNS cache poisoning) which automatically switched the e-mail recipient to the fake www upon opening the email. Then, once users became aware of the risks from banking e-mails, phishing became 'SMiShing' with offenders sending out computer-generated SMS (cellphone) texts to encourage recipients either to log on to a fake www site, or to call a telephone number purporting to be the security department of their bank. Even more recently, SMiShing has evolved into 'vishing' which exploits VOIP (voice over Internet protocol).

The main challenge that phishing poses for the criminal justice processes is that the offence is individually minor and tends only to be serious in aggregate and only then when the stolen information is actually used against the owner. Indeed, the theft of data is still not a criminal offence in all jurisdictions. Even when a fraud does take place using stolen information, usually in the form of credit card misuse or unauthorized account take-over, the police may be reluctant to investigate the case because the losses may be too small, or the problem may be global rather than local, or the local police may think that it is the province of the banks, or the banks may prefer no police contact in order to keep the knowledge of the scams out of the public domain. Identity theft therefore creates a range of fairly new issues for both law enforcement and lawyers representing victims, especially when a defrauded individual seeks to restore his or her reputation to what it once was. Usually, lost reputations are measured in terms of their (financial) credit rating, but, in the worst-case scenario, the stolen identity details may have been used to gain access to, for example, a paedophile site, which significantly complicates the process of restoring a previously good reputation (Sigsworth, 2008).

The three-level distinction made earlier between traditional crime using computers, hybrid and true cybercrimes are important because the first two tend already to be the subject of existing laws, and existing professional experience can be applied to law enforcement practice. Any legal problems arising therefore tend to relate more to legal procedures than substantive law. The final group, however, are solely the product of the Internet, and methods of resolving the problems that they give rise to may not be so easily found.

It is also equally important, of course, to look at substantive common features in online criminal behaviours. The following categories not only describe common behavioural features, but also link them to existing bodies of law and some, albeit limited, experience in the justice processes (Wall, 2007):

- *Computer integrity crimes.* These assault the integrity of network access mechanisms –hacking and cracking, cyber-vandalism, spying, denial of service, viruses and so on. (**Note**: I have previously referred to this group of activities as 'cyber-trespass', but the nature of the activity has now become much broader.).
- *Computer-assisted crimes.* These use networked computers to engage with victims with the intention of dishonestly acquiring cash, goods or services – 'phishing', advanced fee frauds and so on.
- *Computer content crimes.* These relate to the illegal content on networked computer systems and include the trade and distribution of pornographic materials as well as the

dissemination of hate-crime materials. (**Note**: I have previously referred separately to violent and sexually-explicit content, but the explosion of social networking and blogging has made it harder to disaggregate the two.)

Although these categorizations are useful for locating law and expertise, it is nevertheless the case that the specific informational, networked and global characteristics of cybercrimes can conspire to impede the traditional investigative process – despite the existence of applicable bodies of law backed up by international harmonization and police coordination treaties such as the Council of Europe's Convention on Cybercrimes (ETS. 185). On the one hand there is the curious phenomenon of over-reporting cybercrime because of the way in which it is either wrongly conceptualized, or because of misinterpretations of data automatically collected from propriety security software which represent breaches of scientific rules rather than infringements of law. On the other hand there is also the ever-present problem of under-reporting of actual victimizations, as described earlier in the example of phishing. Either the dangers posed by cybercrimes are not always immediately evident to potential (or actual) victims, or they are not regarded as serious, or they are genuinely not serious but possess a latent danger in their being precursors to more serious crimes.

Alternatively, the cybercrime component may not always be seen to be the focus of the offence – which could also lead to under-reporting. 'Computer integrity' cybercrimes can simply be preparatory acts that pave the way for more serious offending. Identity theft from computers, for example, only becomes serious when the information is used against the owner. Similarly, hackers or crackers may use crimeware (Trojans, worms and viruses) to install 'back doors' which are later used to facilitate other crimes, possibly by bot-herders who have compiled bot-nets of infected addresses (see, further, Wall, 2007). Computer-assisted cybercrimes, such as Internet scams perpetrated by fraudsters in collusion with spammers, tend to be relatively minor in individual outcome, but serious by nature of their volume. Computer content crimes, on the other hand, mainly tend to be informational and while they are often extremely personal and/or politically offensive they are not necessarily illegal. But they could contribute subsequently to the incitement of violence or prejudicial actions against others.

Even when the circumstances of a cybercrime are serious enough to get reported and the report has been accepted for investigation there are still a number of problems that can further frustrate the investigative process. Simply put, the informational, networked and globalized qualities of cybercrimes cause them to fall outside the traditional local, even national, operational purview of police. They clearly differ from the regular police crime diet, which is one reason why they can evade the criminal justice gaze. On the few occasions when cybercrimes may be familiar to the routine police diet (for example, some types of fraud), the computing misuse component of the offending is often dropped in favour of a charge for the offence the computer was used to commit. For the most part, however, cybercrimes tend to be too individually small in impact (*de minimis*) to warrant the expenditure of finite police resources in the public interest. Also, because they fall outside routine police activities, the police accrue little professional experience in dealing with them. This becomes additionally problematic when disparities in legal coding across jurisdictions add to the frustration of local law-enforcement initiatives. The big question is how might these challenges be addressed?

This brief deconstruction illustrates that not only does the term 'cybercrime' already have a general linguistic agency, but, when understood in terms of the mediating and transformative impacts of networked technology on the criminal and harmful behaviours it describes, it can also have some common meaning and, indeed, also give meaning to the findings of other research done within the area of networked computer technology. Looking to the future, such conceptual preparation is important as we gradually learn more about the impact that networked technologies are having on online criminal behaviour and victims. To assist us in this task, more research is already being commissioned by the funding councils and government bodies (see, for example, Morris, 2004), and the inclusion of questions about Internet victimization in various national crime surveys will hopefully yield useful empirical data that will challenge some of the misinformation that has accrued during the past decade. Furthermore, there are proposals to introduce the routine recording of computer crime (Hyde-Bales, Morris and Charlton, 2004). Improved conceptual clarity, combined with improved quality of data and professional experience, will further assist the analysis.

Why Should Cybercrimes be an Issue?

Cybercrimes present us with a number of criminal justice-related issues to resolve. Not only is there arguably enough law in most jurisdictions, but there is also quite a lot of policing activity already going on, although not necessarily by the public police. What this observation and the tensions outlined earlier suggest is that problems exist in the way in which cybercrime is currently being conceptualized and understood. First, cybercrime is not a unitary concept and most of the harmful acts regularly referred to as cybercrime are in fact conventional crimes in law for which there are new networked and global opportunities, and furthermore there are distinctly different types. Second, because true cybercrimes are informational, global and networked, they tend to fall outside the law and experience of the criminal justice systems. Third, this second fact is confused by a common misunderstanding of the concept of cybercrime which has been distorted by its conceptual origins in social-science (cyberpunk) fiction. In other words, we expect cybercrime to be dramatic and directly harmful, if not brutal to the point that planes fall out of the sky – but it isn't! The routine experience of cybercrime to date is that it is individually invidious, but collectively insidious. Nevertheless, news reporting relentlessly continues to dramatize the novel event so that one occurrence, or even an observation that it can potentially happen, can provoke much media coverage and shape public opinion. The upshot is that the public expect the public police to respond to their fears – fears which are often exaggerated and even unfounded, and create a reassurance gap between what the public expect of the police and what they can provide (see Wall, 2008). In this rather long-winded (or long-worded) way I am saying that cybercrimes do exist, but not as we expect to see them, and that it is very important to get right the basis upon which criminal justice policy is made.

All this means that the main cybercrime challenge in the twenty-first century is to formulate effective responsive strategies that take into account the different perspectives which the different actors in the field of cybercrime bring to the subject, rather than see it in simplistic binary terms of being either right or wrong. Such strategies require policy that accepts the different, but real, experiences of the business community and the individual user, but also of law enforcement. It is also crucial to base such a policy on realistic expectations of what

the public police can and cannot do. This includes accepting that not all policing lies with the police because the policing function is also to be found within other nodal and networked structures of order.

In an ideal world the governance of online behaviour should be designed to assist and strengthen the Internet's natural inclination to police itself, keeping levels of intervention relevant while installing appropriate structures of accountability. Remember that the same networked technologies which create criminal opportunity can be harnessed to police cybercrime and also (theoretically) monitor the policing of cybercrime. Also remember that the bodies which currently police the Internet include the many other nodes in the networked model of Internet policing such as Internet users, digital environment managers, ISPs, corporate security and non-governmental organizations. Without a robust framework of accountability that also includes the non-public policing agencies there arises the uncomfortable prospect of overpolicing, using technology – which is all the more worrying if the basis of this exercise is the application of scientific, rather than legal, rules. We therefore need to be clear about where we set the balance between the need to maintain order online and the need to enforce law. Until this balance has been achieved, the cybercrime 'reassurance gap' will not be closed. An equally important consideration in seeking such a balance is to ensure that the fundamental open-ended principles of the Internet are preserved so that the individual users decide what to receive and the information which flows along the wires is free and not censored. We are so dependent on networked technologies these days that we just cannot afford to throw the virtual baby out with the virtual bathwater.

About this Volume

The aim of this collection is to provide an interesting, if not provocative, selection of contemporary thinking on cybercrimes and their regulation to advance understanding of the subject. The essays selected not only introduce new viewpoints, but also a critical edge supported by new empirical research that is beginning to challenge and surpass the hitherto journalistically-driven news stories that were once the sole source of information about cybercrimes.

The essays are organized into five Parts and are discussed within their individual sections below.

Developments in Thinking about Cybercrimes

I have argued earlier and elsewhere (Wall, 2007) that, whilst most of the offending frequently referred to as cybercrime has roots in traditional criminal behaviour, we can identify certain forms of informational, networked and globalized behaviours as cybercrimes. These were referred to earlier as 'hybrid' and 'true' cybercrimes. The essays in Part I independently discuss aspects of this issue. In Chapter 1 Majid Yar explores the way in which discussions about cybercrime focus on the apparent novelty of the topic to analyse cybercrime through the lens of routine activity theory. Yar concludes that, whilst some conceptual similarities between 'traditional' and cybercrime may be observed, there remain some important differences – differences that support the proposition that cybercrime represents a new and distinctive form

of crime. Sheila Brown (Chapter 2) takes a slightly different approach in her analysis of cybercrime by arguing that we need to move away from thinking about binaries of behaviours. Instead, she suggests that we need to think more in terms of a criminology of hybrids that maps out techno-social networks in terms of the meanings given to them by the participants, and also to think more broadly.

Changes in the Organization of Crime Online

One thing that has become very apparent about cybercrime during the past decade has been the difference(s) in the organization of cybercrimes when compared to more traditional forms of crime. The organization of cybercrimes changes with available technology and has become networked and nodal. Yet, traditional understandings of crime and its organization are so deeply embedded within the criminal justice psyche that many, mostly but not exclusively lay commentators look for and assume that traditional structures of crime exist when they do not. In Chapter 3 Susan Brenner considers whether or not the advantages that criminal organizations offer for real-world criminals can translate to cybercrime and, if so, whether we can actually anticipate the emergence of cybercrime mafias or cybercrime cartels. Her conclusion is that such forms of hierarchical organization are the product of specific terrestrial events and conditions and are, therefore, unlikely to be replicated in cyberspace. However, this does not mean that cybercrime is unorganized, but, rather, that the organization of cybercrime takes on different, more ephemeral forms. Such forms are described in David Wall's essay on the construction of spamming and its associated economy (Chapter 4). Also to be found in this essay is a discussion about how spam, as a 'true' cybercrime, might best be regulated. This discussion is also subsequently developed in two short essays by Sandy Starr (Chapters 5 and 6) in which he considers whether spamming should be treated as a crime (as it is in law) or simply as a nuisance that can be eradicated by using technological, rather than legal, solutions.

A key driver behind the cybercrime waves of the early 2000s, as identified earlier, was crimeware (malicious software) delivered to users by spams and drive-by downloads when they visit compromised www sites. In Chapter 7 Lorine Hughes and Gregory DeLone usefully describe the trojans and viruses that constitute crimeware and discuss whether or not these 'unique forms of cybercrime' in fact warrant the general concern expressed over them, or whether the threat has been exaggerated. They conclude that much greater attention needs to be paid to the role that computer users play in the spread of malicious software and also to the handful of repeat offenders who contribute disproportionately to the problem.

Another driver of cybercrime currently raising concern is the emergence of new digital environments as sites of victimization. Internet auction sites, such as eBay, have long been identified as providing opportunities for fraud. But since the turn of the new millennium we have also seen the rise in the popularity of virtual worlds and social networking sites and the subsequent convergence of the two with the likes of Second Life. The attraction of such sites is the freedom that their participants have to express themselves. Yet concerns that such sites also create new criminal opportunities have long been expressed. The big task, therefore, is to preserve the participants' freedom of expression while effectively regulating any bad behaviour. As Jack Balkin (2004) argued, constitutionally protected freedoms of expression are insufficiently strong in virtual worlds, and additional legislation and administrative

support is therefore required to uphold free-speech values. However, what happens in the virtual worlds can have very real-world consequences for participants beyond their freedom of expression; thus governments may arguably have a responsibility to regulate those real-world effects in the public interest. In Chapter 8 David Wall and Matt Williams discuss the ways in which online communities can realistically be regulated and policed. They observe that the global and informational span of virtual communities challenges formal attempts to regulate them. But they also demonstrate that the regulation of those communities is already taking place at a number of levels and that most online communities already have their own distinct histories of control and regulation.

The Changing Nature of Cybercrime

Moving from the new environments to the changing nature of cybercrime, the post-millennium literature has taken on a markedly critical stance, with authors questioning some of the received wisdoms about different types of cybercrime: computer integrity crime; computer-assisted crime; and computer content crime.

Computer Integrity Crime

Helen Nissenbaum (Chapter 9) charts the transformation of the ethical hacker from folk hero to miscreant, vandal, criminal and, more recently, terrorist. She argues that this reconstruction of the hacker image has occurred not as the result of a direct and rational public debate about conflicting ideals and interests, but through 'an ontological shift mediated by supportive agents of key societal institutions: legislative bodies, the courts, and the popular media' (p. 189). This observation is important because it shows how dominant interests, either rightly or wrongly, can shape public opinion about cybercrime and offenders. This view is put into perspective by Peter Sommer in his essay placed later in this volume at Chapter 29. Sommer states that the automation of the hacking role by crimeware has meant that, in reality, the (super)hacker myth today is little more than 'an amusing diversion and [no longer] an opportunity to dust down 20-year old clichés about teenage geniuses' (p. 543). As anxiety about the hacker has declined, then concern about the cyberterrorist has grown, especially since the events of 11 September 2001, and Briavel Holcomb, Philip Bakelaar and Mark Zizzamia discuss the various debates about the Internet in the aftermath of the attack on the World Trade Center.

Computer-assisted Crime

Public concern about intellectual property (IP) theft, fanned by organizations representing the creative industries, has also grown in recent years. The public response to intellectual property theft is mixed because so many individuals are involved in downloading it, so bodies that protect IP rights have to work against high levels of public sympathy for the act. In Chapter 11 Greg Urbas charts the fortunes of the highly organized and globally dispersed networked software piracy group DrinkOrDie. He shows that the main regulatory issue is not so much law, but levels of cross-border cooperation and a lack of harmonization of legal concepts. Another computer-assisted cybercrime concern that has arisen since the millennium is identity theft. Bert-Jaap Koops and Ronald Leenes show that although identity theft is

currently perceived as one of the major upcoming crime threats – and not just in cybercrime – there is no commonly accepted definition of what an 'identity theft' is. Koops and Leenes deconstruct understandings of identity theft into component concepts to argue that without conceptual clarity there is no starting-point for policy and research.

Computer Content Crime

A major recent public concern about cybercrime has been the circulation of sexualized child images that involve the sexual abuse of children (child pornography). A large obstacle for law enforcement when dealing with such imagery has been the lack of good practice. In Chapter 13 Tony Krone examines 31 well-publicized police operations to consider their implications for establishing police best practice and to fill the gaps in our understanding of online child pornography. Such information is crucial to inform police responses in emotionally charged environments. Barbara Hewson (Chapter 12) has independently argued that societal responses to child pornography have become culturally constructed to the point that viewing child pornography is now equated with criminal responsibility for rape and ideologically supports the common assertion/assumption that pornography leads to sex crimes, regardless of evidence. It is a development that has negative and worrying implications for liberty and the law. Jonathan Clough's essay (Chapter 15) adds to this discussion by critically assessing the defences put forward in cases involving possession of indecent photographs of children.

In Chapter 16 Francesca Philips and Gabrielle Morrissey continue the theme of responding to online sexual content by looking not at children, which is the common concern, but at the various ways in which adults can be targeted through content manipulation by sexual predators. Philips and Morrissey argue that online sexual harassment can include obscene e-mails, unsolicited porn, spam and the posting of false personal ads advertising the victim's availability for sex, and may escalate to threats of, or actual, sexual violence and death. Yet, little is known about the sexual predation of adults from websites or how those unfortunate enough to be targeted are affected by this particular form of victimization.

Giselinde Kuipers (Chapter 17) further explores the social construction of digital danger in computer content crime by comparing the moral dangers of online humour and pornography in the Netherlands and the United States. She observes that the Dutch part of the Internet considers ethnic humour to be dangerous and that it is therefore is virtually absent in it, but ethnic humour circulates widely on the Anglophone Internet. She also finds that although online pornography is considered dangerous by Dutch Internet users, it is nevertheless felt to be manageable, yet in the United States it has fuelled a moral panic.

Moving on to other forms of informational content crime, Jacqueline Schneider (Chapter 18) investigates the activities of a drugs newsgroup. She discovers that although current laws may support the possible prosecution of members, relatively little attention has been paid to newsgroups with regard to preventing or reducing drug offending. Finally, Jerry Finn's survey of online harassment on a university campus (Chapter 19) shows that sexual-minority students were found to have been disproportionately harassed online by strangers when compared to heterosexual students.