1

CYBERCRIME AND THE INTERNET

An Introduction

Overview

Chapter 1 examines the following issues:

- how cybercrime is perceived and discussed in society, politics and the media;
- the kinds of questions that criminologists ask about cybercrime;
- the emergence and growth of the Internet, the role it plays in a wide range of everyday activities, and how this growth creates new opportunities for offending;
- how cybercrime can best be defined and classified;
- whether and to what extent cybercrime can be considered a 'new' or 'novel' form of criminal activity;
- the extent of cybercriminal activities, and the problems associated with accurately measuring them;
- the challenges that cybercrime presents for criminal justice systems and for criminological explanation.

key terms

Anonymity
Crime
Cybercrime
Cyberspace
Deviance
e-commerce
Globalization
Hacking
Hidden crime
Information society
Internet
Moral panic
Official statistics
Piracy
Policing
Pornography
Recording of crime
Reporting of crime
Representations of crime
Social inclusion and social exclusion
Stalking
Surveillance
Surveys of crime and victimization
Transnational crime and policing
Viruses

1.1 Perceptions of cybercrime

4 May 2000. A computer 'worm' called the 'Love Bug' rapidly infects computers worldwide. It uses infected machines to email itself to other users, corrupting files on computers as it goes. Within hours, millions of computers are affected, including those of UK and US government agencies. The damage caused by the 'Love Bug' is placed at between $7 billion and $10 billion. The prime suspect is Onel de Guzman, 24-year-old college dropout from the Philippines. In August 2000 all charges against de Guzman are dropped – the Philippines simply doesn't have laws that cover computer hacking under which he could be tried and convicted.

(Philippsohn, 2001: 61; Furnell, 2002: 159–61)

11 February 2003. FBI Director Robert Mueller tells the US Senate that 'cyberterrorism' is a growing threat to US national security. He claims that Al-Qaeda and other terrorist groups are 'increasingly computer savvy' and will, in future, have ever greater opportunities to strike by targeting critical computer systems using electronic tools.

(USDS, 2003)

4 February 2004. Graham Coutts, a 35-year-old musician from Hove, UK, is convicted of murdering Jane Longhurst, a 31-year-old school teacher. Coutts, who strangled his victim, is reported to have been 'obsessed' with images of violent sexual pornography, which he had viewed on the Internet just hours before the murder. In the wake of the trial, UK and US government officials announce that they will investigate ways of eradicating such 'evil' sites from the Internet.

(BBC News, 9 March 2004)

> *August 2011*. As urban disturbances spread across numerous English cities, politicians and mass media claim that new social media had been used by participants as a means of disseminating information about incidents in real time, and utilised as a means of social coordination to facilitate rioting and to better evade the police. The UK Prime Minister, David Cameron, suggests that banning 'troublemakers' from using such media may be desirable in the interests of public order.
>
> (Halliday, 2011)

The above are just a few instances of what appears to be an explosion of crime and criminality related to the growth of new forms of electronic communication. Since the mid-1990s, the Internet has grown to become a fact of life for people worldwide, especially those living in the Western industrialized world. Its relentless expansion, it is claimed, is in the process of transforming the spheres of business, work, consumption, leisure and politics (Castells, 2002). The Internet is seen as part of the globalization process that is supposedly sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a 'shrinking' world. We are now said to be in the midst of a 'new industrial revolution', one that will lead us into a new kind of society, an 'information age' (Webster, 2003). Yet awareness of, and enthusiasm for, these changes have been tempered by fears that the Internet brings with it new threats and dangers to our well-being and security. 'Cyberspace', the realm of computerized interactions and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities. Two decades or so on from the Internet's first appearance in popular consciousness, we can see that the intervening years have been replete with fears about its 'darker', criminal dimensions. Businesses cite threats to economic performance and stability, ranging from vandalism to 'e-fraud' and 'piracy'; governments talk of 'cyberwarfare' and 'cyberterror', especially in the wake of the September 11, 2001 (9/11) attacks in New York; parents fear for their children's online safety, as they are told of perverts and paedophiles stalking the Internet's 'chat rooms' and social networking sites looking for victims; hardly a computer user exists who has not been subjected to attack by 'viruses' and other forms of malicious software; the defenders of democratic rights and freedoms see a threat from the state itself, convinced that the Internet furnishes a tool for surveillance and control of citizens, an electronic web with which 'Big Brother' can watch us all. The development of the Internet and related communication technologies therefore appears to present an array of new challenges to individual and collective safety, social order and stability, economic prosperity and political liberty.

Our awareness of the Internet's criminal dimensions has certainly been cultivated and heightened by mass media representations. The news media have played their part in identifying and intensifying public concerns, and hardly a day goes by without some new report of an internet-related threat. Dowland et al. (1999: 723–4) surveyed two 'quality' UK newspapers over a two-and-a-half-year

period, and found that, on average, stories about computer-related crime appeared twice a week in each throughout the period. In a more recent overview of media coverage, Levi (2008: 373) notes the way in which cybercrime 'is used as titillating entertainment which generates fear at the power of technology beyond the control of respectable society'. In addition to the print media, we must also consider broadcast media (television, radio) and the Internet itself (which now constitutes a major source of cybercrime reportage). Popular fiction has also picked-up on the Internet's more problematic dimensions, with films such as *Hackers* and *The Net* sharpening the sense that our safety may be under threat from irresponsible individuals and unscrupulous authorities (Webber and Vass, 2010). Perhaps such representations, and the concerns they inform and incite, should not altogether surprise us. After all, while the Internet itself may be new, history shows us that times of rapid social, economic and technological change are often accompanied by heightened cultural anxieties (even 'panics') about threats to our familiar and ordered ways of life (Goode and Ben-Yehuda, 1994). Thomas and Loader (2000a: 8) suggest that social transformation wrought by internet technologies 'makes the future appear insecure and unpredictable', yielding a public and political overreaction. Such 'moral panics', fuelled by the media, lead to an excessive and unjustified belief that particular individuals, groups or events present an urgent threat to society (Critcher, 2003). Yar (2012a) suggests that representations of the Internet in the popular imagination have increasingly come to be characterized by a 'cyber-dystopian' outlook, one that portrays the social effects of new technologies in overwhelmingly negative terms. Internet-related instances of panics include those over the effects of pornography in the mid-1990s, and more recently over threats to child safety from paedophiles (Littlewood, 2003; Cassell and Cramer, 2008). The proliferation of such anxieties is perhaps best viewed as a consequence in part of the rapid shifts and reconstructions in the midst of which we currently find ourselves. This is not to suggest, however, that the dangers posed by cybercrime can simply be dismissed as wholly unfounded. Nor is it to suggest that such widespread reactions ought to be simply ignored by criminologists. Media representations, both factual and fictional, constitute an important criminological research topic in their own right; their careful examination enables us to uncover how the problem of cybercrime is being constructed and defined, and how this shapes social and political responses to it (Taylor, 2000; Vegh, 2002). Yet the weight of such representations can also serve to obscure the realities of criminal activity and its impacts, hindering rather than facilitating a balanced understanding.

1.2 Cybercrime: questions and answers

For criminologists, making sense of cybercrime consequently presents a significant challenge, as it requires us to take, as best we can, a more sober and balanced view,

sifting fact from fantasy and myth from reality. The very existence of this book is testimony to the author's belief that such an examination is both possible and worthwhile. Indeed, numerous scholars have already made considerable strides in this direction. By using a combination of theoretical analysis and empirical investigation they have attempted to get a handle on a range of pressing questions:

- Just what might be meant by 'cybercrimes'?
- What is the actual scope and scale of such crimes?
- How might such crimes be both like and unlike the 'terrestrial' crimes with which we are more familiar?
- Who are the 'cybercriminals'?
- What are the causes and motivations behind their offending?
- What are the experiences of the *victims* of such crimes?
- What distinctive challenges do such crimes present for criminal justice and law enforcement?
- How are policy-makers, legislators, police, courts, business organizations and others responding?
- How are such responses shaped by popular perceptions of computer crime and computer criminals?
- How is cybercrime shaping the future development and use of the Internet itself?

There now exists a considerable literature addressing such issues, drawn from a wide range of disciplines including criminology, sociology, law and socio-legal studies, political science, political economy, cultural and media studies, science and technology studies, business and management, and computing. The ever-expanding range of such material, along with its dispersal across different disciplinary boundaries, makes it difficult for the newcomer to find an accessible route into current debates. This difficulty is exacerbated by the fact that cybercrime refers not so much to a single, distinctive kind of criminal activity, but more to a diverse *range* of illegal and illicit activities that share in common the unique electronic environment ('cyberspace') in which they take place. Consequently, different academic contributions tend to focus on some selected aspects of the cybercrime problem, to the detriment or neglect of others. Hence the purpose of the present volume, which is conceived as a thorough and up-to-date introduction to the range of issues, questions and debates about cybercrime that have come to characterize it as a field of study. Out of necessity, I draw upon theoretical and empirical contributions from different areas of scholarship, but with the main focus falling upon criminology and sociology, the two areas that comprise my own primary fields of expertise. The following chapters will furnish a critical introduction to a variety of substantive issues. Many of them focus on recognizably different kinds of cybercriminal activity, such as 'piracy', 'hacking', 'e-fraud', 'cyberstalking' and 'cyberterrorism'; each is examined and analysed in light of the social, political, economic and cultural context in which it takes

shape. Other chapters consider debates of a more general nature, addressing, for example, the tensions apparent between internet security and policing, on the one hand, and individual rights, freedoms and liberties, on the other. Given the range of issues to be covered, their treatment cannot be exhaustive. Hence each chapter contains guidance for further, more in-depth reading, which can be found both in conventional print form and online.

However, before we can move on to these more detailed examinations, there are a number of important issues of background and context that must be outlined, and some important conceptual issues that must be tackled. Hence the remainder of this chapter will situate cybercrime in relation to the growth and development of the Internet, and ask questions about how we might best classify cybercriminal activities, and why it is that cybercrime might need to be viewed as qualitatively different from other kinds of criminal and illicit activity.

1.3 A brief history and analysis of the Internet

An examination of cybercrime ought to begin with the Internet, for the simple reason that without the latter, the former could and would not exist. It is the Internet that provides the crucial electronically generated environment in which cybercrime takes place. Moreover, the Internet should not be viewed as simply a piece of technology, a kind of 'blank slate' that exists apart from the people who use it. Rather, it needs to be seen as a set of *social practices* – the Internet takes the form that it does because people use it in particular ways and for particular purposes (Snyder, 2001). 'What' people do with the Net, and 'how' they typically go about it, are crucial for understanding what kind of phenomenon the Internet actually is. Indeed, it is the kinds of social uses to which we put the Internet that create the possibilities of criminal and deviant activity. To give one example, if people didn't use the Internet for shopping, then there would be no opportunities for credit card crimes that exploit users' financial information. Similarly, it is *because* we use the Internet for electronic communication with friends and colleagues that the 'Love Bug' worm, which targeted the email systems we use for that purpose, could cause billions of dollars in damage.

The Internet, as its name suggests, is in essence a computer network; or, to be more precise, a 'network of networks' (Castells, 2002). A network links computers together, enabling communication and information exchange between them. Many such networks of information and communication technology (ICT) have been in existence for decades – those of financial markets, the military, government departments, business organizations, universities and so on. The Internet provides the means to link up the many and diverse networks already in existence, creating from them a single network that enables communication between any and all 'nodes' (e.g. individual computers) within it.

The origins of the Internet can be traced to the development of a network, the Advanced Research Projects Agency Network (ARPANET), sponsored by the US

military in the 1960s. The aim was to establish a means by which the secure and resilient communication and coordination of military activities could be made possible. In the political and strategic context of the 'Cold War', with the ever-present threat of nuclear confrontations, such a network was seen as a way to ensure that critical communications could be sustained, even if particular 'points' within the computer infrastructure were damaged by attack. The ARPANET's technology would allow communications to be broken up into 'packets' that could then be sent via a range of different routes to their destinations, where they could be reassembled into their original form. Even if some of the intermediate points within the network failed, they could simply be bypassed in favour of an alternate route, ensuring that messages reached their intended recipients. The creation of the network entailed the development not only of the appropriate computer hardware, but also of 'protocols', the codes and rules that would allow different computers to 'understand' each other. This development got under way in the late 1960s, and by 1969 the ARPANET was up and running, initially linking together a handful of university research communities with government agencies.

From the early 1970s further innovations appeared, such as electronic mail applications, which expanded the possibilities for communication. Other networks, paralleling the ARPANET, were established such as the UK's JANET (Joint Academic Network) and the US's NSFNET (belonging to the American National Science Foundation). By using common communication protocols, these networks could be connected together, forming an inter-net, a network of networks. A major impetus for the emergence of the Internet as we now know it was given when, in 1990, the US authorities released the ARPANET to civilian control, under the auspices of the National Science Foundation. The same year, 1990, saw the development of a web browser (basically an information-sharing application) by researchers at the CERN physics laboratory in Switzerland. Dubbed the 'World Wide Web' (www), this software was subsequently elaborated by other programmers, allowing more sophisticated forms of information exchange such as the sharing of images as well as text. The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet Explorer the following year. These browsers made Internet access possible from personal computers (PCs). In the mid-1990s, numerous commercial internet service providers (ISPs) entered the market, offering connection to the Internet for anyone with a computer and access to a conventional telephone line. These connection services, while popular, were slow and offered a very limited capacity for transmitting data. They have since been supplanted by much faster 'broadband' connections as well as services offering data connections to mobile devices such as phones. Since the commercialization of the Internet in the mid-1990s, its growth has been incredibly rapid. Between 1994 and 1999 the number of countries connected to the Internet increased from 83 to 226 (Furnell, 2002: 7). In December 1995 there were an estimated 16 million Internet users worldwide; by May 2002, this figure had risen to over 580 million, almost 10 per cent of the world's total population (NUA, 2003). As of March 2012, the total number of Internet users

had reached an estimated 2.28 billion, comprising some 32.7 per cent of the global population (IWS, 2012). However, it is crucial to bear in mind that, despite this phenomenal growth, access to the Internet remains highly uneven both between countries and regions, and within individual nations. The technical capacity enabling internet access (PCs, software, reliable telecommunications grids) is unevenly distributed: for example, more than 70 per cent of households in Europe have internet access, while the comparable figure for the African continent is less than 6 per cent (ITU, 2012). Similarly, while Europe boasts 200 broadband internet connections for every 1,000 people, in Africa there is only one such connection per 1,000 people (ITU, 2009: 5). Unequal access also follows existing lines of social exclusion within individual countries – factors such as employment, income, education, ethnicity and disability are reflected in the patterns of internet use (Castells, 2002: 208–23; Miller, 2011: 97–105). These inequalities are criminologically important, as they tell us something about the likely social characteristics of both potential cybercriminal offenders and their potential victims (a point I shall return to later in the chapter).

It is further worth considering not only what kinds of people are online, where, and in what numbers, but also *what they do* in online environments. As noted earlier, the range of social practices that people legitimately engage in will create distinctive opportunities for offending – what criminologists call 'opportunity structures' arising from people's online 'routine activities' (Grabosky, 2001; Newman and Clarke, 2003). Therefore one of the most important areas of internet usage relates to its applications in electronic business, or 'e-commerce'. Businesses increasingly use the Internet as a routine part of their activities, ranging from research and development, to production, distribution, marketing and sales. These uses create a range of criminal opportunities: for example, the theft of trade secrets and sensitive strategic information (Jackson, 2000), the disruption of online selling systems, and the fraudulent use of credit cards to obtain goods and services (Grabosky and Smith, 2001; Smith, 2010). The increasing prevalence of online banking and similar financial services likewise generates opportunities for financial crimes that exploit systems for identity authentication (Gupta et al., 2011). Similarly, the Internet is increasingly being mobilized by a range of actors for political purposes – governments use it to inform and consult citizens, political parties use it to recruit supporters, pressure groups use it to organize campaigns and raise funds, and so on. Consequently, we see the emergence of cybercrimes that are political in nature; these range from the sabotage and defacement of official websites, and the use of the Internet to instigate 'hate' campaigns by far-right extremists, to the activities of 'terrorist' groups aiming to recruit members and raise funds (Denning, 1999: 228–31; Whine, 2000; Denning, 2010). Another important area of internet activity relates to leisure and cultural consumption. People in increasing numbers are turning to the Internet to access everything from music and movies to celebrity gossip and online video gaming. Yet again, the demand for such goods creates opportunities exploited by the criminally inclined – these range from the distribution of

obscene imagery, to the trade in 'pirate' audio and video recordings and computer software (Akdeniz, 2000; McCourt and Burkart, 2003; Yar, 2005). A further notable feature of the contemporary internet is the huge public uptake of new social media platforms (such as Facebook, Twitter and the like) which generate new patterns of vulnerability to misuse and abuse (Yar, 2012b). These examples suggest that illegitimate online activities must be viewed not in isolation, but as deeply inter-connected with their legitimate counterparts.

1.4 Defining and classifying cybercrime

A major problem for the study of cybercrime is the absence of a consistent current definition, even among those law enforcement agencies charged with tackling it (NOP/NHTCU, 2002: 3). As Wall (2001a: 2) notes, the term 'has no specific referent in law', yet it is often used in political, criminal justice, media, public and academic discussions. I have already suggested that instead of trying to grasp cybercrime as a single phenomenon, it might be better to view the term as signifying a *range* of illicit activities whose 'common denominator' is the central role played by networks of ICT in their commission. A working definition along these lines is offered by Thomas and Loader (2000a: 3) who conceptualize cybercrime as those 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks'. Thomas and Loader's definition contains an important distinction that warrants further reflection, namely that between *crime* (acts explicitly prohibited by law, and hence illegal) and *deviance* (acts that breach informal social norms and rules and hence considered undesirable or objectionable). Some analysts of cybercrime focus their attention on the former, those activities that attract the sanctions of criminal law (see, for example, Akdeniz et al., 2000). Others, however, take a broader view, including within discussions of cybercrime some acts which may not necessarily be illegal, but which large sections of a society might deem to be deviant. A prime example of this latter kind of activity would be sexually explicit speech and imagery online (see, for example, DiMarco, 2003). Given that the primary focus of this book is crime rather than deviance, discussions will be directed in the main toward those internet-related activities that carry formal legal sanctions. However, it is important to bear in mind that crime and deviance cannot always be strictly separated in criminological inquiry. For example, the widespread perception that a particular activity is deviant may fuel moves for its formal prohibition through the introduction of new laws. Alternatively, while particular activities may be illegal, large sections of the population may not necessarily see them as deviant or problematic, thereby challenging and undermining attempts to outlaw them (one such instance, discussed in Chapter 4 is that of 'piracy'). Such dynamics, in which boundaries between the criminal and the deviant are socially negotiated, are a recurrent feature of contemporary developments around the Internet.

Starting with an understanding of cybercrime as 'computer-mediated activities that are illegal', it is possible to further classify such crime along a number of different lines. One commonplace approach is to distinguish between 'computer-assisted crimes' (those crimes that pre-date the Internet, but which take on a new life in cyberspace, e.g. fraud, theft, money laundering, sexual harassment, hate speech, pornography) and 'computer-focused crimes' (those crimes that have emerged in tandem with the establishment of the Internet, and could not exist apart from it, e.g. hacking, viral attacks, website defacement) (Furnell, 2002: 22; Lilley, 2002: 24). On this classification, the main way in which cybercrime can be subdivided is according to the role played by the technology, that is, whether the Internet plays a merely 'contingent' role in the crime (it could be done without it, using other means), or if it is absolutely 'necessary' (without the Internet, no such crime could exist). This kind of classification is adopted by policing bodies such as the UK's National Hi-Tech Crime Unit, which distinguishes between 'old crimes, new tools' and 'new crimes, new tools' (NHTCU, 2004).

While the above distinction is helpful, it may be rather limited for criminological purposes, as it focuses on the *technology* at the expense of the relationships between offenders and their targets or victims. One alternative is to use existing categories drawn from criminal law into which their cyber-counterparts can be placed. Thus, Wall (2001a: 3–7) sub-divides cybercrime into four established legal categories:

1 Cyber-*trespass* – crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.
2 Cyber-*deceptions* and *thefts* – stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. 'piracy').
3 Cyber-*pornography* – breaching laws on obscenity and decency.
4 Cyber-*violence* – doing psychological harm to or inciting physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking.

Such classification can be seen to sub-divide cybercrime according to the object or target of the offence: the first two categories comprise 'crimes against property', the third covers 'crimes against morality', and the fourth relates to 'crimes against the person'. To these we may also wish to add 'crimes against the state', those activities that breach laws protecting the integrity of the nation and its infrastructure (e.g. terrorism, espionage and disclosure of official secrets). Such a classification is helpful, as it allows us to relate cybercrime to existing conceptions of prohibited and harmful acts.

1.5 What's 'new' about cybercrime?

The classification outlined thus far, while indispensable, may not by itself illuminate all the relevant characteristics of cybercrime. By relating such crime to

familiar types of offending behaviour, it stresses those aspects of cybercrime that are continuous with 'terrestrial' crimes. Consequently, it does little in the way of isolating what might be qualitatively *different* or *new* about such offences and their commission, when considered from a broader, non-legal viewpoint. This question of the 'novelty' of cybercrime is an important one for criminologists. Some argue that cybercrime is pretty much the same as 'old-fashioned' non-virtual crime, and just uses some new tools that are helpful for the offender; what Grabosky (2001) dubs 'old wine in new bottles'. Others, however, insist that it represents a new form of crime that is radically different from the kinds of 'real world' crimes that predate it. Among this latter group, many criminologists (especially those with a sociological orientation) focus their search for novelty upon the social-structural features of the environment ('cyberspace') in which such crimes occur. It is widely held that this environment has a profound impact upon how social interactions can take place (both licit and illicit), and so transforms the potential scope and scale of offending, inexorably altering the relationships between offenders and victims, and the potential for criminal justice systems to offer satisfactory solutions or resolutions (Capeller, 2001). Particular attention is given to the ways in which the establishment of cyberspace variously 'transcends', 'explodes', 'compresses' or 'collapses' the constraints of space and time that limit interactions in the 'real world'. Borrowing from sociological accounts of globalization as 'time–space compression' (Harvey, 1989), theorists of the Internet suggest that cyberspace makes possible near-instantaneous encounters and interactions between spatially distant actors, creating possibilities for ever-new forms of association and exchange (Shields, 1996). Criminologically, this seems to render us vulnerable to an array of potential predators who can reach us almost instantaneously, untroubled by the normal barriers of physical distance. Moreover, the ability of the potential offender to target individuals and property is seemingly amplified by the Internet – computer-mediated communication (CMC) enables a single individual to reach, interact with, and affect thousands of individuals at the same time. Therefore the technology acts as a 'force multiplier' enabling individuals with minimal resources to generate potentially huge negative effects (mass distribution of email 'scams' and distribution of viruses being two examples). In addition, great emphasis is placed on how the Internet enables the manipulation and reinvention of social identity – cyberspace interactions give individuals the capacity to reinvent themselves, adopting new virtual personae potentially far removed from their 'real world' identities (Poster, 1990; Turkle, 1995; Boellstorff, 2010). From a criminological perspective, this is viewed as a powerful tool for the unscrupulous to perpetrate offences while maintaining anonymity through disguise (Snyder, 2001: 252; Joseph, 2003: 116–18), and a formidable challenge to those seeking to track down offenders.

From the above, we can conclude that it is the novel social-interactional features of the cyberspace environment (primarily the collapse of space–time barriers, many-to-many connectivity, and the anonymity and changeability of

online identity) that make possible new forms and patterns of illicit activity. It is this difference from the 'terrestrial world' of conventional crimes that makes cybercrime distinctive and original.

1.6 How many crimes? Assessing the scale of internet offences

Gaining a realistic measure of the scope and scale of cybercriminal activities presents considerable challenges. Some of these problems are well known to criminologists. 'Official statistics' on crime, for example, have been critiqued as 'social constructions' that do not necessarily provide us with an 'objective' picture of the true, underlying levels and patterns of offending (Maguire, 2002). There are a number of reasons for this. First, such statistics depend upon crimes having been *reported* to the police or other official agencies. Studies, however, show that a large proportion of offences simply remain unreported for a wide variety of reasons: victims may be unaware that an offence has been committed; they may consider the offence insufficiently 'serious' to warrant contacting the authorities; they may feel that there is little likelihood of a satisfactory resolution (such as the apprehension of the offender or the return of their property). Second, even if an offence is reported, it may not be *recorded* by the police or other agencies, again, for a variety of reasons. For example, political priorities may lead police to prioritize some crimes as the expense of others (Coleman and Moynihan, 1996); police perceptions of 'seriousness' will affect whether they deem tackling an offence as a worthwhile use of their time and resources; police may have disincentives to record certain types of crime, where they feel that there is little likelihood of a successful investigatory outcome, as a large number of unresolved offences might cultivate the impression that police are failing to maintain 'law and order'. In addition, decisions about whether or not to record a reported offence may depend upon police judgements about the person(s) doing the reporting, such as their perceived status, reliability or trustworthiness. Third, serious problems are evident when we attempt to establish longitudinal measures of crime, that is, the charting of crime trends (decreases and increases) over time. The ways in which crime recording classifies and groups offences are subject to change, making direct comparison over the years difficult. Moreover, it must be remembered that crime is a legal construct (Lacey, 2002: 266–7) – what happens to be illegal is subject to its inclusion in criminal law. Laws change over time – new categories of offence are created, thereby making previously permissible behaviour illegal; conversely, previously prohibited behaviour may be decriminalized or legalized, removing it from the domain of criminal activity. Consequently, year-on-year measures of crime rarely compare 'like with like', making it difficult to derive reliable conclusions about whether or not particular types of crime (or crime in general) are on the increase or decrease.

These familiar problems with measuring crime are, if anything, exacerbated in relation to cybercrime (Wall, 2007: 19–20). For example, the relatively hidden nature of Internet crimes may lead to them going unnoticed. Unfamiliarity with laws covering computer-related crimes may lead victims to be unaware that a particular activity is in fact illegal (Dowland et al., 1999: 715, 721; Wall, 2001a: 8). The very limited allocation of police resources and expertise to tackling computer crime may result in the relevant authorities being unknown or inaccessible to victims for reporting purposes. The extent to which the Internet enables offenders to remain anonymous may lead victims (and police) to conclude that there is little likelihood of a perpetrator being identified (e.g. the chance of being prosecuted for computer hacking in the USA is placed at 1 in 10,000 (Bequai, 1999: 16)). The inherently global nature of the Internet (where victim and offender may be located in different countries, with different laws relating to computer crime) renders effective police action particularly difficult and time-consuming, leading such offences to be sidelined in favour of more manageable 'local' problems (Wall, 2001b: 177; Wall, 2007: 160). Such factors suggest that there may in fact be a massive under-reporting and under-recording of internet-related crimes, and a correspondingly massive (and by definition unknown) 'dark figure' of cybercrime. The problems for charting cybercrime trends over time are also heightened by rapid innovations in internet and computer-related law. Recent years have seen the introduction of many new sanctions into criminal law to cover computer-related offences. These have taken the form of national legislation (such as the UK's Computer Misuse Act (1990) and the US Computer Abuse and Fraud Act (1986), No Electronic Theft Act (1997 and the Identity Theft Enforcement and Restitution Act (2007)) and a range of criminal sanctions incorporated into national laws as a result of international agreements, treaties and directives (such as the 1994 TRIPS (Trade-Related Aspects of Intellectual Property Rights) agreement under the WTO (World Trade Organization), the Council of Europe Convention of Cybercrime (2004), and the provisions of EU law). Such innovations have meant that the range of internet activities covered by criminal law has been constantly shifting, making trend data about cybercrime as a whole difficult to construct.

One way in which the shortcomings of official crime measures have been addressed is through the development of crime and victimization surveys. These have aimed to uncover those crimes that remain unreported and unrecorded by official statistics, thereby giving a more complete and accurate picture of the scope and patterns of offending (Maguire, 2002: 348–58). Such surveys are particularly important for generating knowledge about cybercrime, since there is by and large little officially collected and collated data specifically relating to Internet crimes. However, we should not conclude that such alternative measures wholly overcome the problems previously identified in relation to official statistics. For example, no reporting is possible where victims are unaware that an offence has been committed; those surveyed may have a different understanding of what counts as an offence from those administering the survey;

and they may be unwilling to report an offence even when disclosure is made on an anonymous basis. The problems in relation to cybercrime surveys are, once again, further heightened. First, such surveys as exist tend to be highly selective, focusing mainly upon business and/or public sector organizations, to the exclusion of individual citizens (prime examples include the annual computer crime survey undertaken in the USA by the Computer Security Institute (CSI) on behalf of the FBI, and similar surveys conducted in the UK by the polling organization NOP on behalf of the National Hi-Tech Crime Unit). Moreover, as Wall (2001a: 7–8) notes, there is no consistent methodology or classification across such surveys, making comparison and aggregation of data difficult (see also Fafinski et al., 2010). Finally, there are serious problems relating to under-reporting, as many organizations may prefer not to acknowledge victimization because of: (1) fear of embarrassment; (2) loss of public or customer confidence (as in the case of breaches relating to supposedly secure e-shopping and e-banking facilities); and (3) because of potential legal liabilities (e.g. under legislation relating to data protection, which places organizations under a legal duty to safeguard confidential information relating to citizens and customers) (Furnell, 2002: 28, 51). All of the above should lead us to treat statistics about cybercrime, be they official or otherwise, with considerable caution. One of the most basic challenges for both criminology and criminal justice in relation to cybercrime is the need to develop basic, robust measures of the problem itself.

Despite the difficulties outlined above, it would be mistaken to simply ignore the available statistical measures, limited and partial as they might be. If we wish to glean *some* insight into the nature and extent of the 'cybercrime problem' we must make use of such data as are available – a case of relatively weak data being better than absolutely no data at all. So long as we not do 'reify' these measures, taking them to be incontrovertible facts, they can still serve a useful purpose in giving us some preliminary indication of the problem. Indeed, in so far as such data are taken seriously by the various actors who discourse publicly upon cybercrime and take legislative, policing and security decisions on its basis, we need to give these figures due consideration. Subsequent chapters will give more detailed attention to the 'facts and figures' as they relate to different types of cybercriminal activity (such as hacking, viruses, e-fraud, piracy, and so on). For the moment, we can reflect on some 'headline' figures that have appeared in high-profile reports on cybercrime, as these give us an indication of why internet crime has become the object of concerted concern for a range of public and private actors:

- A survey distributed to more than 5,000 public and private sector organizations in the USA revealed that in the preceding 12 months, 67.1 per cent had been targeted by malicious software, 38.9 per cent had been targeted by 'phising' attacks, and 28.9 per cent had their networks infected by 'bots'. The total financial losses incurred from these incidents were estimated at over $200 million (CSI, 2011: 15).

- According to the 2011 Global Economic Crime Survey, cybercrime is now one of the 'top four economic crimes', alongside asset misappropriation, accounting fraud, and bribery and corruption; 48 per cent of the 3,877 respondents assessed the risk from cybercrime to be rising (PWC, 2011: 9,29).
- A 2009 study claimed that computer crime costs businesses at least $1 trillion per annum, but cautioned that that actual figure is likely to be considerably higher due to under-reporting of cybercrimes (Voigt, 2011).
- US 'copyright industries' claim annual losses due to 'piracy' (of goods such as music, films and computer software) to the order of $58 billion (Siwek, 2007).
- In 2009 alone, it is estimated that more than 1.5 million new pieces of malicious software (such as viruses and Trojans) appeared (Benzmüller and Berkenkopf, 2010: 4).
- Online credit card fraud is estimated to cost UK consumers some £290 million per annum (Smith, 2010: 282).

Figures such as those above furnish an important context for understanding why the media, politicians, law enforcement agencies and business organizations have come to be increasingly exercised by the cybercrime threat. Cybercrime can be viewed as an integral component of those globalized risks that are increasingly coming to define 'contemporary landscapes of crime, order and control' (Loader and Sparks, 2002). Moreover, if we bear in mind estimates that as little as 5 per cent of such crimes may actually be reported to the authorities (Furnell, 2002: 190), then the problems posed by cybercrime may well figure among the most urgent of the early twenty-first century.

1.7 Challenges for criminology, criminal justice and policing

The proliferation of cybercriminal activity poses new challenges not just for criminal justice and crime control, but also for criminology as a discipline. The specific character of such challenges will be considered in more detail in subsequent chapters, but we can identify here some general dimensions.

1.7.1 The challenge for policing and criminal justice

From the discussion thus far it is clear that the Internet has distinctive features that shape the crimes which take place in cyberspace. These features pose difficulties for tackling crime when approached by the established structures and processes of criminal justice systems. Not least among these is that policing has historically followed the organization of political, social and economic life within national territories. Moreover, crime control agencies such as the police traditionally operate within local boundaries, focusing attention and

resources on crimes occurring within their 'patch' (Lenk, 1997: 129; Wall, 2007: 160). Yet cybercrime, given the global nature of the Internet, is an inherently de-territorialized phenomenon. Crimes in cyberspace bring together offenders, victims and targets that may well be physically situated in different countries and continents, and so the offence spans national territories and boundaries. While there are ongoing attempts to strengthen transnational policing through agencies such as Europol and INTERPOL (Bowling and Foster, 2002: 1005–9), these are largely focused upon sharing intelligence related to large-scale 'organized crime'. A more focused transnational initiative is the EU high-tech crime agency European Network and Information Security Agency (ENISA), established in 2004; yet its role is not directly investigatory, but restricted to coordinating investigations into cybercrime by police in member countries (Best, 2003).

Further problems arise when we consider the constraints of limited resources and insufficient expertise. For example, the UK's National Hi-Tech Crime Unit (NHTCU) was established in 2001, comprising 80 dedicated officers and with a budget of £25 million; however, this amounted to less than 0.1 per cent of the total number of police, and less than 0.5 per cent over the overall expenditure on 'reduction of crime' (Home Office, 2002a; Wales, 2001: 6). Moreover, by 2009 the NHTCU had been absorbed into the newly established Serious and Organised Crime Agency (SOCA), and was subsequently displaced by the Police Central e-crime Unit (PCeU) (see discussion of these and other related developments in Chapter 9). The lack of organizational stability and continuity in the field of cybercrime policing may itself disrupt efforts to effectively tackle the problem of online crime. ENISA, the EU agency, labours under similar budgetary constraints. It was established with an annual allocation of just £17 million (€24.3 million) to coordinate transnational investigations spanning the 25 member countries (Best, 2003); by 2012, this budget had been cut to a mere £6.8 million (€8.5 million) (ENISA, 2012). A lack of appropriate expertise also presents barriers to the effective policing of cybercrime. Investigating such crimes will often require specialized technical knowledge and skills, and there is at present little indication that police have the appropriate training and competence (Bequai, 1999: 17). Moreover, research indicates that many police do not view the investigation of computer-related crime as falling within the normal parameters of their responsibilities, undermining attempts to put such policing on a systematic footing (Hyde, 1999: 9).

The difficulties are further intensified once we consider the problem posed by different legal regimes across national territories. The move toward an international harmonization of internet law has already been noted. Yet such developments are in a relatively early stage. Examination of Internet law reveals that many countries lack the legislative frameworks necessary to effectively address internet-related crimes (Sinrod and Reilly, 2000: 2). Attempts to legislatively tackle cybercrime may also run foul of existing national laws. For example, the US introduction of the Communication Decency Act in 1996, aimed at curbing

'offensive' and 'indecent' images on the Internet, was partly overturned as some of its provisions were held to breach constitutional guarantees relating to freedom of speech and expression (Biegel, 2003: 129–36). Even where appropriate legal measures have been put in place, many countries (especially in the 'developing world') simply lack the resources needed to enforce them (Drahos and Braithwaite, 2002). In countries facing urgent economic problems, with states that may be attempting to impose order under conditions of considerable social and political instability, the enforcement of internet laws will likely come very low down on the list of priorities, if it appears at all.

1.7.2 Challenges for criminology

The discipline of criminology has been concerned throughout its history with attempts to uncover the underlying causes behind law-breaking behaviour. Thus, theories of crime purport to locate the forces that propel or incline people toward transgressing society's rules and prohibitions. Such explanations have, inevitably, been based upon data relating to criminal activity in 'real-world' settings and situations. The emergence of the Internet poses challenges to existing criminological perspectives in so far as it exhibits structural and social features that diverge considerably from conventional 'terrestrial' settings. It is by no means clear whether and to what extent established theories are compatible with the realm of cyberspace and the crimes that occur within it. Two such challenges for criminology are now considered:

1 *The problem of 'where':* Many criminological perspectives are based, implicitly or explicitly, upon 'ecological' assumptions. That is to say, they view crimes as occurring within particular places that have important defining social, cultural and material characteristics. It is in the distinctive features of such local environments that the causes of the crime are supposedly to be found. Recent decades have seen the development of influential criminologies that focus upon the spatial organization of lived environments, and explain patterns and distributions of offending in terms of the ways in which such environments are configured. So, for example, 'routine activity' approaches focus on how potential offenders are able to converge in space and time with potential targets, thereby creating the conditions in which offending is able to take place (Cohen and Felson, 1979; Felson, 1998). Such thinking has also inspired a range of crime mapping, measurement and prevention programmes, again focused on identifying 'criminogenic' environments and localities whose crime-inducing characteristics can then be removed (Fyfe, 2001). However, such approaches run into difficulties when we consider cybercrimes. The environment in which such crimes take place, cyberspace, cannot be divided into distinctive spatial locations in any straightforward manner, in the way we can distinguish in the 'real world' between neighbourhoods and districts,

urban and suburban, the city and the country and so on. Rather, cyberspace can been viewed as basically 'anti-spatial' (Mitchell, 1995: 8), an environment in which there is 'zero distance' between all points (Stalder, 1998), so that identifying locations with distinctive crime-inducing characteristics becomes well-nigh impossible (Yar, 2005). The inability to answer the question of 'where' crimes take place in cyberspace indicates that criminological perspectives based on spatial distinctions may be of limited use.

2 *The problem of 'who':* Criminological theories have also sought to understand why it is that some individuals engage in law-breaking behaviour while others do not. Official statistics indicate that offending is not only spatially but also socially located; the profile of offenders shows a preponderance of those with certain shared characteristics. One such characteristic has been the over-representation among known offenders of those from socially, economically, culturally and educationally marginalized backgrounds. Consequently the fact of 'deprivation' (whether 'relative' or 'absolute') has come to be causally linked to offending behaviour (Lea and Young, 1984; Hagan and Peterson, 1994; Finer and Nellis, 1998). Such inferences have not enjoyed universal acceptance, as Marxist and other 'critical' criminologists have claimed that the association of socio-economic marginality with criminal activity is more a product of the iniquitous class-based prejudices of the criminal justice system than of any real concentration of offending among particular social groups. However, much mainstream criminology gives considerable credibility to the view that the 'crime problem' is one predominantly centred upon those who suffer 'social exclusion' (although controversy continues to rage between those on the 'Left' who find the causes of such exclusion in economic structures and processes (Wilson, 1996), and those on the 'Right' who attribute it to the individual's 'fecklessness' and irresponsibility (Murray, 1984)). Wherever we stand on the ultimate origins of exclusion, the relationship between marginality and offending is an established feature of criminological explanation. When we come to consider cybercrime, however, this correspondence appears to break down. It was noted earlier that the capacity to access and make full use of the Internet is unevenly distributed across society, with those in the most marginal positions enjoying least access. Conversely, the skills and resources required to commission offences in cyberspace are concentrated among the relatively 'privileged': those enjoying higher levels of employment, income and education. Consequently, the social patterns of Internet criminality may well turn out to be rather different from those typically identified in the 'terrestrial' world, with cyber-offenders being 'fairly atypical in terms of traditional criminological expectations' (Wall, 2001a: 8–9). If this is the case, then recourse to concepts such as 'marginality' and 'exclusion' to explain the origins of offending behaviour, so prevalent in relation to 'real-world' criminology, might be of extremely limited value when attempting to explain the genesis of cybercrimes.

The foregoing discussion suggests that criminology, as much as criminal justice, faces challenges from the emergence of cybercrime. Rather than simply being able to transpose an existing 'stock' of empirical assumptions and explanatory concepts onto cyberspace, the appearance of Internet crimes might require considerable theoretical innovation. Criminology itself may need to start looking for some 'new tools' for these 'new crimes'.

1.8 Summary

Over the past two decades, cybercrime has become an increasingly widely debated topic across many walks of life. Our understandings of cybercrime are simultaneously informed and obscured by political and media discussions of the problem. It is clear that the rapid growth of the Internet has created unprecedented new opportunities for offending. These developments present serious challenges for law and criminal justice, as it struggles to adapt to crimes that no longer take place in the terrestrial world but in the virtual environment of cyberspace, which span the globe through the Internet's instantaneous communication, and afford offenders new possibilities for anonymity, deception and disguise. Society's increasing dependence on networks of computer technology renders us ever-more vulnerable to the failure and exploitation of those systems. Equally, the emergence of cybercrime poses difficult questions for criminologists and sociologists of crime and deviance. Such academic disciplines have formed their theories of and explanations for crime on the basis of assumptions (about who, what, where and so on) drawn from offending in the terrestrial world. In so far as the virtual environment of the Internet may be radically different from its terrestrial counterpart, criminology itself is challenged to adapt its perspectives in order to come to grips with cybercrime, or to develop new concepts and vocabularies which might better fit with the online world that we increasingly inhabit.

Study questions

- How does public discourse represent the problem of cybercrime?
- What kind of questions does the emergence of cybercrime invite us to ask?
- How great a problem are cybercrimes when set alongside those terrestrial crimes with which we are more familiar?
- What is new or different about cybercrime?
- What kinds of cybercrimes do everyday users of the Internet encounter?
- Who are the 'cybercriminals'? Are they the 'usual suspects' of criminal justice and criminology?
- How might the growth of cybercrimes shape the ways in which the Internet develops in the future?

Further reading

A valuable introduction to a range of cybercrime issues and debates can be found in David S. Wall's *Cybercrime* (2007). For a detailed discussion of a wide variety of cybercrime problems, by a range of leading scholars in the field, see Yvonne Jewkes and Majid Yar's (eds) *Handbook of Internet Crime* (2010). The growth of the Internet and its central place in the development of the 'information society' are explored in Manuel Castells' ground-breaking *The Information Age: Economy, Society and Culture: Vol. 3, End of Millennium* (1998) as well as his *The Internet Galaxy: Reflections on the Internet, Business, and Society* (2002). A wide-ranging and accessible introduction to the Internet, digital media, and their social and cultural implications can be found in Vincent Miller's *Understanding Digital Culture* (2011). For up-to-date and detailed data on the levels and trends in cybercrime, see the Computer Security Institute's annual *Computer Crime and Security Survey*. The debate about whether or not cybercrime is a new or novel phenomenon is conducted in Peter Grabosky's article 'Virtual criminality: Old wine in new bottles?' (2001), and Wanda Capeller's 'Not such a neat net: Some comments on virtual criminality' (2001). Finally, useful discussions about the governance and regulation of the Internet can be found in Brian Loader's (ed.) *The Governance of Cyberspace Cyberspace*: *Politics, Technology and Global Restructuring* (1997), and John Mathiason's *Internet Governance: The New Frontier of Global Institutions* (2009).