

1

The Challenge of Digital Crime

Robin Bryant

In this chapter we examine the challenges arising from the growth of digital crime, particularly the problems faced by investigators. The interaction between technological change and criminality is well recognised for crime in general, but certain aspects of digital crime mark a significant shift both in the ways in which crime is enacted, and the consequent investigative response. This chapter explores some of the more general technological and social factors that have accompanied and possibly contributed to these changes. The remaining chapters consider particular aspects in more detail.

1.1 Technology and crime

Throughout history, general technological developments have continually created new opportunities for criminal activity, which in turn have driven the development of new technologies. Both the pre-modern and modern eras provide clear examples of such interactions. For example, in the 12th century, the techniques employed for counterfeiting currency closely matched the technological development of reliable methods to produce genuine currency. Similarly, bank robbers in the early 20th

century soon began to use motor cars to speed their getaway, a scenario portrayed frequently in early Hollywood gangster movies such as *White Heat*. More recently, criminals employ advanced technology in their attempts to access internet-based banking systems in order to launder the proceeds of criminal enterprises.

The burgeoning development of a wide range of new technologies provides an ever expanding range of options for the creative mind. Some of the terminology relating to these technologies and their applications are shown in figure 1.1; no doubt digital crime investigators will already be familiar with the meanings of many of the terms shown.

Just as technology is utilised by many people for legitimate reasons, so it will be by those intent on committing crime. In this sense, little has changed; *plus ça change, plus c'est la même chose*. However, in the late modern age, crime that specifically exploits digital technologies (what we term in this book 'digital crime') has a number of possibly novel characteristics, and we explore these below.

1.1.1 Spatial and temporal differences

It perhaps now a cliché to observe that digital crime respects no international or legislative boundaries. However, it is undoubtedly true that much digital crime (particularly crime associated with the internet) is not anchored in time and space in quite the same sense as more conventional crime. Whereas the 1950s con artist inviting passers-by to 'Find the Lady' (pick out the Queen of Hearts from a row of three face-down playing cards) in London's Petticoat Lane would need to make direct personal contact to carry out the fraud, an eBay fraudster is not so constrained. Likewise, some crimes (such as installing a 'Trojan horse' virus) may be enacted in seconds, but the effect may not be felt until days, months or years later. Vatis (2005) goes so far as to claim that cybercrime in particular represents

[...] the most fundamental challenge for law enforcement in the 21st century. By its very nature, the cyber environment is borderless, affords easy anonymity and methods of concealment and provides new tools to engage in criminal activity.

For digital crime, temporal differences are also significant, particularly in relation to the rapidity of interactions, such as receiving reward and gratification. The probable motivation for a person to illegally download the mp3 version of

1.1 TECHNOLOGY AND CRIME

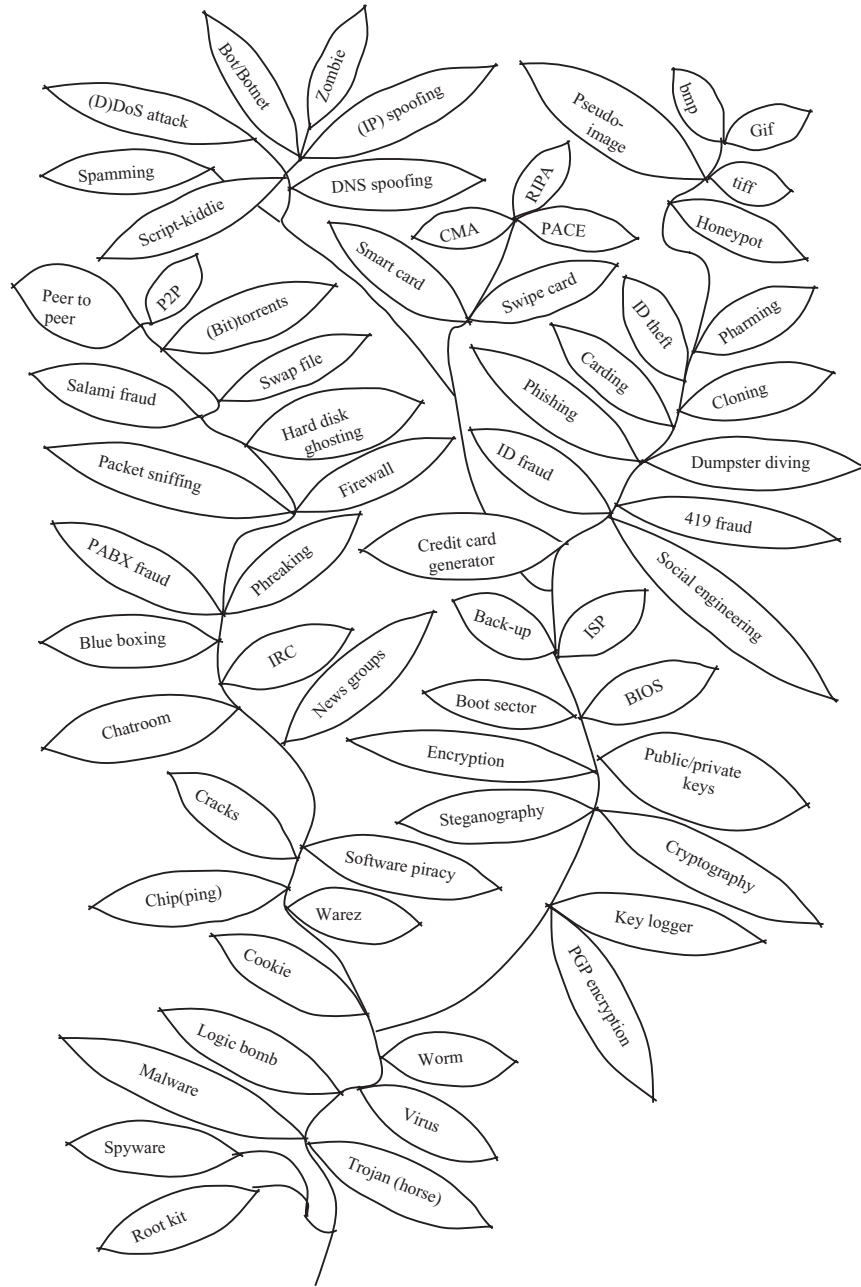


Figure 1.1 Digital terminologies (Sarah Bryant)

copyrighted music is not solely because it is relatively free of charge, but also because it is immediately available.

Access to information is no longer so constrained by time and space. It is far more difficult, largely as a result of the internet, for groups, organisations, authorities and official bodies to control access to certain forms of information, many of which may be considered to be sensitive or even dangerous. Once Pandora's digital Box is opened it is almost impossible to track down and remove any information released. On reflection, this should not be surprising, given the



Figure 1.2 A typical hypertext version of the 'Anarchist's Cookbook'.

origins of the internet as a network designed to withstand attack. Contrast two documents produced in the 1970s: the so-called 'Green Book' produced by members of the Provisional IRA (to help train their recruits in the use of lethal weapons and quasi-military tactics) with the notorious 'Anarchist's Cookbook', a text still circulating on the internet which details, inter alia, the manufacture of improvised explosive devices.

Most of the 'military' content of the Green Book was strictly controlled and 'analogue' in nature (presumably mainly photocopied and distributed on paper), and has not apparently been released into the public domain. However, the Anarchist's Cookbook and similar documents (such as the Terrorist's Handbook) have been developed and expanded by a number of contributors working independently and anonymously (now as part of a wider project termed the 'Jolly Roger Cookbook') and are readily available to anyone through the internet. In 1999 David Copeland (not believed to be a member of any terrorist organisation) used information contained in the Terrorist's Handbook to construct nail bombs which he used to attack people in a gay bar in Soho in London, and then passers-by in Brick Lane and Brixton, both multi-cultural areas of London (BBC, 2000).

1.1.2 Economies of scale

Second, digital crime often exploits the ability of ICT to disseminate information widely, repeatedly and cheaply. As a result, what we might term the 'sucker quotient' for digital crime can be much lower than for conventional crime; for digital crime the investment of time and effort may be low, but the activity may still nonetheless provide high returns for the criminal. Our 1950s con artist is counting on quite a few people from those hundreds passing by to be gullible enough to take part in the con; the sucker quotient has to be relatively high for the con to yield sufficient results. On the other hand, a phisher can send tens of thousands of fake emails relatively easily, and even if only one victim responds, the resulting user account details may be used subsequently to commit identity theft and fraud, potentially very lucrative crimes. In a somewhat similar way, the pattern of rewards from other digital crimes follows the related principle of many victims and small losses. As Wall (2004, p. 20) suggests

Where once a robber might have had to put together a team of individuals [...] in order to steal £1 million from a bank, new technologies are powerful enough (in principle at least) to enable one individual to rob one million people of £1 each.

1.1.3 Anonymity

Third, digital crime, particularly if it is conducted over the internet, provides a much greater scope for anonymity, through either secrecy or by presenting a false identity (DiMarco, 2003). A paedophile may brazenly assume a faked identity (perhaps as another young person) in an attempt to groom a potential victim in an online chatroom. In comparison, grooming in the pre-internet era necessitated the paedophile gaining the trust of the child and family by an often slow and (for the paedophile) risky face-to-face process.

1.1.4 Virtual worlds

Fourth, the virtual nature of some digital crime (Brenner, 2001) is an important explanatory and defining factor. In a very loose sense this refers to the sense of unreality or even 'de-individualisation' (akin to Zimbardo's concept of 'deindividuation') with an attendant loss of sense of self-accountability and self-awareness pervading a person's actions in the digital world, particularly online. This sense of unreality may in turn lead to disinhibition (Suler, 2004). For example, many people make no attempt to conceal the fact that they have committed the theft of intellectual property online (using peer-to-peer programs (P2P) to download copyrighted music), but they would otherwise consider themselves to be entirely law-abiding citizens (Yar, 2007).

1.1.5 Legislative lag

Fifth, digital crime (particularly cybercrime) is perceived to suffer from an increased propensity to 'legislative lag'; a longer period of time seems to elapse between innovations in criminal enterprise and the response of the state and law enforcement agencies. This is probably an illusion; digital crime develops and changes very rapidly, but it may take years for legislation to be enacted, by which time the crime may well have mutated or developed to assume a different form. In consequence, it may seem that many digital crimes are in effect beyond the reach of law, and indeed this may be the case; at least some digital crimes cannot be addressed under contemporaneous legislation. This is a complex area, discussed more fully in later chapters, but it is interesting to

note at this stage that the UK government does not share the view that specific e-related legislation is always necessary, or that there is necessarily a problem of legislative lag:

The Government is committed to ensuring that actions should be legal or illegal according to their merits, rather than the medium used, i.e. what is illegal offline should be illegal online and vice versa. As such, all legislation criminalises offences regardless of the means used to commit the offence.

Where there is a need to revise legislation to take account of new criminal techniques we seek to do so. We liaise regularly with the prosecution and law enforcement authorities to ensure the criminal law remains fit for purpose, but are not aware of significant legislative gaps that hinder the agencies (Home Office, 2006).

1.1.6 Horizontal and vertical hierarchies

Using an analogy with the four kinds of mapping employed in mathematical set theory, we can conceptualise the main forms of human communication as falling into one or more categories, as illustrated in Table 1.1.

Table 1.1 Mapping forms of communication

Form of communication (mapping)	Hierarchy	Example
One-to-one	Predominantly horizontal (across)	Person to person, e.g. by speaking or writing a letter
One-to-many	Predominantly vertical (downwards)	One person addressing a group, e.g. making a speech to a group of people
Many-to-one	Predominantly vertical (upwards)	A group of people addressing one person, e.g. a written petition to a politician
Many-to-many	Predominantly horizontal (across)	Groups of people communicating with others, e.g. a 'Facebook' entry on the internet

It is in the many-to-many forms of communication that we have probably witnessed the most significant change as a result of digital forms of data storage and communication. As Dupont (2004) notes, the advent of the internet in particular has led to the ‘decline of vertical hierarchical social structures and the concomitant rise of horizontal networks’. That is, in the past, the flow of some forms of information tended to be ‘top down’ and hence under the control of those occupying a higher position in a hierarchy. This applied as much to knowledge concerning criminal matters as it did to more socially acceptable forms of information.

Horizontal structures, particularly single horizontal planes from a much larger vertical hierarchical pyramid, also tend to be less efficient in terms of opportunities for communication. Communication is often limited to a relatively small group of people within the horizontal plane, leaving a silent and unempowered majority; a scenario that may be familiar to employees within large organisations. There are other examples; incarceration in prison is sometimes an opportunity for criminals to share information concerning criminal techniques, such as improved ways to commit a burglary (Gill, 2007). However, given the nature of the information concerned it was by necessity limited to a small circle, (and be largely verbal in nature) and would as a consequence spread only slowly.

If we accept that the internet has led to an increase in horizontal communication, that is amongst peers with little or no control exercised by authorities, then this will also be reflected in new opportunities to share information and techniques amongst those interested, or intent upon, criminal activities. There is some patchy evidence that this may be happening. For example, it is alleged that the notorious US-based ‘Shadowcrew’ online community (located around the now closed website

Shadowcrew
 For Those Who Wish To Play In The Shadows!

SSN and DOB, Credit Reports and other lookups
 Credit Cards with CVV and CVV2
 and other information only from Zo0mer

FAQ Search Memberlist Usergroups Register
 Profile Log in to check your private messages Log in

The time now is Thu Jul 01, 2004 12:53 pm
 Shadowcrew Forum Index

Forum	Topics	Posts	Views	Last Post
Global Forum All topics from all forums	3247	27187		Thu Jul 1 2004 12:53 pm
Discussion Forums				
The Lounge Anything goes in this forum. Take your battles and personal matters into the lounge. Moderators: Shado , Suthe	622	4996		Thu Jul 1 2004 12:53 pm
Identification Technical discussion on Novelty Identification, 2nd ID, Passports, and the like. Moderators: p0th0 , p0rta0	956	4362		Thu Jul 1 2004 12:53 pm
Cyberspace Discussion about online anonymity tools and programs in general. Moderators: p0rta0 , p0rta0	224	1255		Thu Jul 1 2004 12:53 pm
Credit and Checks Discussion concerning credit cards, credit bureaus, credit reports, and credit services. Moderators: p0rta0 , Suthe	957	5839		Thu Jul 1 2004 12:53 pm

Figure 1.3 Excerpt from the ‘Shadowcrew’ website in 2004

www.shadowcrew.com) shared and traded information concerning stolen credit card numbers and ATM skimmers, and it is claimed that these activities resulted in the loss of \$4 million, (United States of America v. Mantovani and others, 2004). At its height it is alleged that the Shadowcrew community consisted of over 4000 members (United States of America v. Mantovani and others, 2004).

1.1.7 Investigative challenges

Finally, by its very nature digital crime can give rise to a number of specific detection and investigative challenges. For example, the use of steganography to hide child pornographic images can pose the kind of technical and legislative problems inconceivable just two decades or so ago. Steganography is the process of hiding one object within another. It predates the digital era; Allied PoWs concealed messages in letters written to loved ones, using barely visible dots (amongst other means). However, interest in steganographic techniques has received an added impetus for two main reasons; its use to hide electronic information (such as a child pornographic image within an innocent-looking holiday snap) and the wide availability of software to assist the process. Note that steganography is not simply cryptography in a different guise: in the use of cryptography for example, it is obvious that a change has been made to the original information, with steganography it is not.

There are well-documented cases of the use of steganography by criminals, such as the sharing or selling of child pornography. For example, in 2002 an international police investigation ('Operation Twins', led by the UK's NHTCU and involving Europol, the Canadian RCMP and police forces from Norway and Germany) uncovered an extensive paedophile ring whose members frequently employed steganography to hide child pornographic images. Less well substantiated is the claim that the technique is also used by terrorists. Gabrielle Weimann, a senior fellow at the United States Institute of Peace and Professor of Communication at Haifa University claimed in March 2004 that:

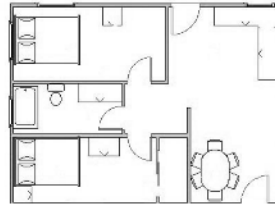
Hamas activists in the Middle East, for example, use chat rooms to plan operations and operatives exchange e-mail to coordinate actions across Gaza, the West Bank, Lebanon, and Israel. Instructions in the form of maps, photographs, directions, and technical details of how to use explosives are often disguised by means of steganography. (Weimann, 2004)

Undoubtedly, the use of steganography presents a serious challenge to digital investigators (McBride *et al.*, 2005), and for a number of reasons. For example,

An 'innocent' (non-incriminating) image



A plan, required by the recipient for undertaking an attack

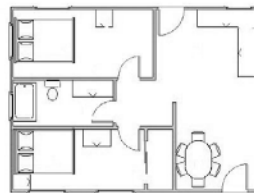


The two images are combined using steganography and a key



This combined image is sent openly to the recipient

The recipient separates the two images, using steganography and the key.



The plan is retrieved.

Figure 1.4 Concealing images by steganography

by deliberate intent, steganographic versions of illegal images are impossible to identify simply by sight, and sophisticated techniques are necessary for both identifying the existence of a file changed through steganography and in recovering the original in a manner that would withstand legal scrutiny (steganalysis). Often the hidden file is password protected and forms of cryptography can also be used as part of the steganographic process, adding another level of difficulty for the investigator.

1.2 Analogue and digital

In popular culture we are often said to live in a ‘digital world’, presumably a reference to those information and communication technologies (the internet, the mobile phone), consumer and entertainment products (DVD, satellite TV) which exploit the advantages of storing and transmitting data represented in a *digital* form. The term digital used in this context probably arose from the word digit, referring to the fingers, particularly when used in counting (*digitus* is Latin for a finger or toe). Increasingly, digital has come to mean the representation of information (in its most fundamental form) as a number of states, usually two states, but sometimes three or more. Two-state systems are sometimes termed as binary, referring to states such as ‘1’ and ‘0’ or ‘on’ and ‘off’. This is not a new idea; the reliability of such systems is exploited in Morse code which uses a two-state representation of dots and dashes, (although intervals of four different lengths are used to help decode messages). According to the *Oxford English Dictionary* (2007) the more modern sense of the word ‘digital’ first came into use in 1984.

Digital technology is often contrasted with precursor analogue (or analog) technologies. Analogue technology represents information in a form that is analogous to the quantity or quality itself. Perhaps the classic example of this is the difference between analogue watches (using the movement of hands to represent the time), and digital watches which use only numbers. We can draw an analogy between position and time for the hands of an analogue watch; the hands move through space at a rate proportional to the lapse of time. In this way, an analogue watch attempts to replicate the phenomenon of time itself by a direct copying; the smooth movement of the hands representing time as a continuous variable. Digital watches use a more abstract representation instead, identifying points in time such as 10:23, with the passage of time itself not represented visually. The time will then appear to suddenly move on, to 10:24, 10:25 and so on; time is represented as if it is a discrete variable.

Music and other sounds may also be stored by analogue or digital means. A comparison of earlier analogue methods (the acetate or vinyl record) and later

digital approaches (the CD) provides a further illustration of some key differences between analogue and digital representations. Consider two copies of the Beatles' Sgt Pepper album, one a vinyl LP, the other a CD. On the vinyl disc the spiral groove is visible (just), with its variable peaks, troughs and gradients; complex shapes that are analogous to the sounds produced when the disc is played. On the other hand, the sound on a CD is represented as digital data; physically this consists of only a series of simple 'pits' and 'lands'; a two-state representation (invisible to the unaided human eye).

Sound recordings

The line represents the groove on a vinyl record, as seen from above, for a mono record.



Figure 1.5 A representation of a groove on a vinyl record

The wider the sideways displacement of the groove, the louder and deeper the sound. Higher pitched sounds are carried by tightly packed oscillations. For a stereo recording, the width of the groove itself varies too, allowing the stylus to move up and down as well as from side to side.

The diagram below shows the simple way in which information is represented digitally as 'pits' and 'lands', as seen from above.

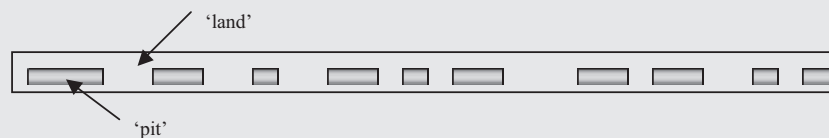


Figure 1.6 A representation of part of a digital track on a CD

The dark areas are the pits (depressions) in the plastic surface. All the pits are the same depth; only the distance between them varies. The lands are

the regions in between the pits. A laser moves along the track as the CD is read. The distance between successive pit-land transitions is the significant information in the signal.

Which format is likely to be illegally shared on the internet? The answer is obvious: the digital version, largely because the numerical representation of the pattern of pits and lands is far easier to reproduce than the precise and complex patterns engraved into the vinyl. The digital version also readily lends itself to conversion to other formats such as mp3, and to sharing through peer-to-peer networks. Crucially, because of the way that information is represented in a digital signal, there is no loss of quality when copying or sharing: the ten thousandth copy sounds exactly the same as the original.

The robustness of digital data also has significant advantages for data transmission. As the signal is composed of just two or more states, each relatively easily distinguishable from the other, it will remain clear and readable, almost regardless of the amount of distortion inadvertently introduced. As an example consider the developments in satellite TV broadcasting in the last decade or so. In the past, the satellite signal was essentially analogue in nature, and frequently subject to some distortion due to incorrectly aligned dishes, problems at the transmission end or weather conditions. Therefore, for the viewer, the picture might have been near perfect, or fuzzy with ‘sparklies’, or so fuzzy that there was almost no picture at all; the distortion in the signal created a proportionally distorted sound and picture. However, digital satellite signals (now the norm, at least for European and North American distributors) can still be ‘read’ accurately even if the signal is distorted, and the picture remains near-perfect. This is a slight simplification, as signal compression may produce a ‘blocky’ picture as the signal becomes more distorted, and of course complete picture loss is inevitable if the signal is so severely distorted that the states become indistinguishable. For the same underlying reason, messages in Morse code may remain clear, even if the signal has been transmitted over thousands of miles, as the code contains only six elements that are relatively easy to distinguish.

The storage of information in digital form also facilitates the integration of devices and systems. Whereas in the past a personal phone could not play music, and a tape deck was not an answering machine, now the distinction between the functionality of digital devices (particularly those designed for the consumer market) is increasingly blurred, and deliberately so. A mobile phone might well also function as a GPS device and a DVD player might also be able to show digital photographs. Some refrigerators even have IP addresses on the internet.

The differences between analogue and digital means of storage and reproduction may appear to be largely technical in nature but these differences are important when attempting to understand the nature of digital crime. For example, the increased availability and distribution of hardcore adult pornography have been greatly facilitated by the use of digital media. In the 1970s and 1980s, VHS tapes of hardcore pornography originating from countries where its production and trade were legal could only be distributed to other countries to a limited extent, partly due to technical difficulties in producing multiple copies. A VHS tape copied 'serially' (that is, making copies of copies) is virtually unwatchable after at most three or four copies, due to compounded errors in reproduction. However, digital formats can be serially copied without any loss of information, so production of such material is now far easier, and can be carried out successfully on a smaller scale.

Not only do these changes in forms of distribution affect crime but they also influence legislative and regulatory responses; indeed the censors' apparently more liberal views may be to some extent a pragmatic response to the widespread availability of hardcore pornography through digital media, resulting in desensitisation. In the case of adult pornography, the British Board of Film Classification (BBFC) now allows most forms of adult hardcore pornography (images of aroused genitalia and ejaculation) to be sold from licensed sex shops in the UK. However, the BBFC's decision (as a result of a High Court decision) must also be viewed against the wider context of changes of attitude to censorship.

Finally, digital data occupies far less physical space than its analogue equivalents. For example, a novel of 125 000 words would probably cover about 500 paper pages, but could be stored digitally in a volume much smaller than a pinhead, occupying about 1.25 Mb in digital terms. Similarly, 128 000 such novels could be stored on a single 160 Gb PC hard drive. The digital storage 'space' required can be reduced still further through the use of encoding and compression techniques. For example, an average CD audio track occupies between 50 to 60 Mb, but can be compressed to about four Mb when encoded in mp3 format, and for most listeners there will be no noticeable loss of quality.

1.3 The growth of digital technologies

The telephone was the first mass-market two-way communication device. The first public telephone exchange (serving only eight subscribers) was opened in 1879 (BT, 2007), but it was not until the mid 1970s that more than 50 per cent of the households in England and Wales had their own landline telephone. And from the

1.3 THE GROWTH OF DIGITAL TECHNOLOGIES

15

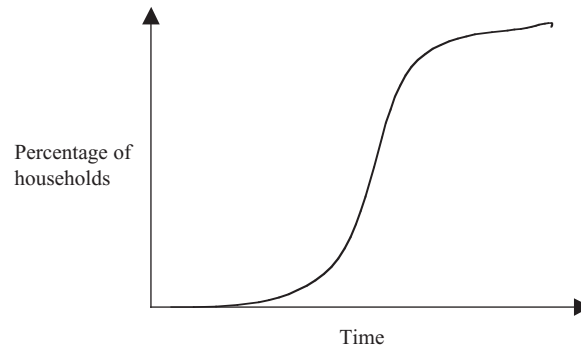


Figure 1.7 Market penetration of new products

1922 inception of regular radio broadcasting by the BBC, it took almost 30 years for radio to become a regular presence in almost every home. Most new consumer devices follow a characteristic 'S' shape of take-up, as illustrated in Figure 1.7.

In the early years of a new device (e.g. the 'wireless' radio) take-up is relatively slow (the lag phase) but then gains pace before slowing again; at this stage market penetration may approach (or even exceed) 100 per cent for some items.

This 'S' shaped pattern of consumer behaviour has also been observed for many new (digital) technology devices but with a noticeable difference: the 'S' shape is often much more foreshortened with a more rapid acceleration towards market adoption. For example, it was estimated that in 2006, 57 per cent of households in Great Britain had an internet connection with 73 per cent of these being broadband, compared with just nine per cent in 1998 (National Statistics Online, 2006).

Not only has there been an exponential growth in the numbers of digital devices in circulation and the number of digital services utilised; the processing power of digital devices has increased dramatically. Moore's Law, originally formulated in the mid 1960s observed that the number of transistors in an integrated circuit doubled every two years, but that the real cost remained constant year after year, (Intel, 2007). In popular use Moore's Law has now assumed a more general meaning, and is often used (perhaps erroneously) to make the case that processing power doubles every 18 months to two years. Certainly, technological advances have given rise to cheap and widely-available computing power in a wide variety of forms. The consequences of such rapid technological change (and its implications for crime) are difficult to predict, but are likely nonetheless to be real and manifest.

For example, the cost of many digital devices has decreased significantly in the last decade or so, as illustrated by the Table 1.2. The power and functionality of these devices has also increased.

Table 1.2 The changing costs of digital devices

Device	Cost in 1997	Cost in 2007
Mid-range desktop PC	£1200	£400 ¹
Basic DVD player	£275	£14.98 ²
'Entry level' mp3 player	£180 ³	£14.99 ⁴

¹ Ebuyer, <http://www.ebuyer.com/UK/store/5/cat/Home-PCs>

² Tesco, Bush 2051ND DVD Player, <http://direct.tesco.com/q/R.100-1141.aspx>

³ The first portable mp3 players appeared in 1998.

⁴ Play.com, Inovix IMP-15 256MB MP3 / WMA Player, <http://www.play.com/Product.aspx?r=ELEC&title=1063434&source=9710>

At the present time, the cost of digital devices is still falling and their functionality and power is increasing; it may seem paradoxical that a convergence of technologies is coinciding with increased specialisation. For example, even an 'entry level' PC will play a music collection, and many mobile phones will also take photographs, however it becomes more of a challenge for the average person to make simple repairs to his or her own car. Digital services are also increasingly being 'bundled' together (Ofcom, 2007) leading to a greater convergence and take-up of digital television, broadband and VoIP.

At the same time, digital devices are tending to become smaller whilst remaining consistent with practical use, referred to in the past as miniaturisation. For example, mobile phones were the size of a house brick until the 1990s and a DVD player is likely to be slimmer and much lighter than its equivalent predecessor, the VCR (partly because it has far fewer moving parts). As we see in section 1.6 below, these reductions in size have implications for digital crime.

The growth in digital technologies and their widespread and rapid adoption (including information communication technologies) have obviously provided new opportunities to commit crime; these crimes and the investigative response are the subjects of most of this book. However, microprocessors and storage memory in many devices (other than the usual locations such as PCs and PDAs) also provide new opportunities for investigators; additional forms of evidence, and more sophisticated investigative methods and means for law enforcement. For example, many new cars (particularly the higher specification models) come equipped with GPS navigation devices which store data relating to locations and times (and some of this information will not be apparent to the average user). This information may be used as intelligence in an investigation or be used as evidence in court. It may seem ironic that although a driver using a GPS system may feel more independent, the device can also be used by others to track movements retrospectively; this could be seen as a loss of independence as well

as a possible invasion of privacy. Of less obvious interest to the investigator (and less well known to the public) is the fact that some modern washing machines are equipped with ROM that may contain residual information concerning time of use; this could be important, for example, in an investigation into an alleged rape. In essence, whenever a digital device contains memory it is of potential interest to an investigator.

1.4 Key features of digital crime

In popular discourse, in crime investigation and within the academic community, a number of terms are used relating to the advent of new (or 'retooled') forms of criminality associated with the growth of digital technologies (see Section 1.3 above). These terms include 'new technology crime', 'cybercrime' and 'high



Figure 1.8 Digital crime terminologies

(or 'hi') tech crime'. In addition, the prefixes 'e' and 'cyber' also tend to be attached to existing labels to indicate new and 'digitised' versions of existing crime phenomena.

Wall (2004) argues the need for accurate terminology when describing these new forms of crime. It is debatable therefore, whether we really need yet another term, such as 'digital crime' to describe some of these phenomena. However, digital crime is more than cybercrime (Wall, 2005, 2007 (Chapter 2)), e-crime (cited by Morris, 2004), netcrime, new technology crime, online crime, high tech crime. The term 'digital crime' embraces most of these, but also includes other forms of crime, such as music and video piracy, which have grown and developed largely as a consequence of the growth of digital technologies and the opportunities for criminal enterprise that we examined in the preceding section. As Kshetri (2005, p. 555) notes: 'Crimes target sources of value, and for this reason, digitization of value is tightly linked with digitization of crime'.

Cybercrime

More recently, the term 'cybercrime' has taken on a more defined meaning, and this is reflected in a growing literature on the subject. Cybercrime is increasingly being defined as that crime which occurs in a networked environment (such as the internet), and which is peculiar to these environments.

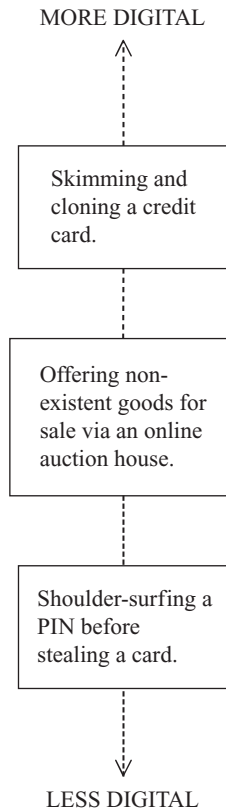
The term cybercrime usually embraces the following criminal activities:

- computer hacking and cracking;
- developing and/or spreading malicious code (e.g. virus, Trojans);
- spamming;
- network intrusion;
- software piracy; and
- network-based or network-enabled crimes such as phishing, identity theft, IPR crimes (e.g. illegal filesharing), distribution of child pornography.

However, we acknowledge that such a wide meaning for digital crime results in a somewhat tautological or 'catch all' definition. In this sense we are closer

1.4 KEY FEATURES OF DIGITAL CRIME

19

**Figure 1.9** The digital spectrum

to Grabosky (2007, p. 2) who uses the term ‘electronic crime’ to describe ‘a wide range of crimes committed with the aid of digital technology’, but, like ourselves, also acknowledges that this is a ‘label of convenience’. Wall (2005) proposes the application of an ‘elimination test’ to a crime – that is, if we ignore the digital features of a crime, has a crime still been committed (or has the crime been ‘eliminated’)? Wall goes on to suggest that crimes can be placed along a spectrum depending on the extent of digital involvement; some crimes may involve only incidental use of a computer, whilst other crimes, such as phishing, could not be committed without computers and computer technology. It is the crimes at this latter end of the spectrum that we might conceptualise as digital in nature, if not form. Figure 1.9 shows some examples of crimes and their positions along this spectrum.

Consider a street thief who first observes an unwary user input their PIN at an ATM, and then steals the card and later withdraws cash; this is not a crime that appears to be particularly digital, and it is therefore placed at the less digital end of the spectrum. On the other hand, skimming the magnetic stripe of a credit card, cloning the card, and then using it to make transactions is clearly a crime unique to the digital era, and would appear to be placed at the more digital end of the spectrum.

However, many crimes are more likely to have a digital aspect rather than to uniquely exploit digital technologies. An example would be a fraud enacted via an online auction house such as eBay (see Figure 1.8 above); this type of fraud belongs to the long and dishonourable tradition of separating the gullible from their money, and there would appear to be little that is ‘post – or even late – modern’ about it. However, the fraudster may well have undertaken planning for the fraud involving the internet; setting up temporary and difficult to trace email accounts and surfing the internet for images, descriptions and prices. Furthermore, he or she may well have falsified his or her own ‘satisfaction rating’ to inspire confidence in sellers, and then bid on his or her own fake auction, using a ‘shell’ account to up the price. These are all activities which exploit the advantages of digital technologies, but nonetheless arise from a conventional and classic form of crime.

1.5 Growth and development of digital crime

As we noted in the introduction to this chapter, changes in technology (particularly forms of information communication) almost always provide new opportunities for crime. However, although there may be new opportunities and ample evidence of individuals exploiting these opportunities for illegal gain, it will not necessarily lead to an overall increase in criminal activity. An important question therefore, is how much of this new crime is simply a displacement or reconfiguration of previous criminal activity? Or has there been a genuine increase in overall levels? This is a complex issue; as an illustration, consider the impact of digital technologies on copyrighted music and video and intellectual property rights crime.

In the 1960s it was just about possible to copy music using consumer-level equipment, but the process was technically demanding and far from reliable; reel-to-reel tape machines were expensive and the process involved using a microphone to record from the radio or a vinyl record onto a tape. The whole approach was thoroughly analogue in nature, and normally produced only a single taped

copy of listenable quality. Though (to our knowledge) no academic research has been undertaken on this particular issue, home taping of copyrighted music by amateur enthusiasts seems not to have been considered a problem in the 1960s, and certainly not by the companies that may potentially have been affected.

Home taping of film images (largely 8 mm film stock) was (if anything) at an even earlier stage of development than taping music in the 1960s. There were no consumer VHS or Betamax recorders available to copy from TV, and most piracy at this time consisted of copying film (often pornography) for private distribution, and was limited to those with access to specialist equipment.

In the 1970s and 80s, with the advent of relatively inexpensive audio cassette players with a record button, home taping of copyrighted popular music became widespread, and came to be perceived as problematic, particularly by the record producing industries. For example, in the early 1980s the British Phonographic Industry (BPI) organisation launched their 'Home Taping is Killing Music' campaign. At about the same time, organised counterfeiting of music for criminal profit became widespread; commercially-produced copyrighted music (on tape or vinyl) was copied (in parallel and in series) onto tapes for selling on.

The first Betamax video player for the consumer market was introduced in the mid 1970s, but it could not make recordings (and cost over \$2000). By the mid 1980s VHS had won the video format 'war' and video players and recorders became widely available. Inevitably these were used to make taped copies of commercially produced videos. One UK company even marketed a 'double-decker' VHS machine; tapes could be copied without the need for a second VHS deck. Despite its clear potential for making pirate copies, the House of Lords judgement (*CBS Songs Ltd and Others v Amstrad Consumer Electronics Plc and Another*, [1987] 2 WLR 1191) held that the company could not be held responsible for the misuse of the machine. Copy protection such as Macrovision was introduced, but so too were forms of circumvention (the 'signal cleaners' advertised in satellite, video and TV magazines).

Music CDs were introduced to the market in the early 1980s but it was not until CD recorders became widely available (initially as 'stand alone', then normally as part of a PC) that CD copying began in earnest. Before the internet became a widespread means of digital communication, this copying was usually 'physical', from one CD to another. Copies of commercial CDs were made by the owner of the CD as so-called 'back ups', or for passing or selling to another person. In most cases, the distribution of these copies was limited to a relatively small circle of friends, family and acquaintances. There were relatively few instances of organised physical piracy of CDs using specialised

equipment to make numerous pirated CDs, but this began to increase in the late 1980s.

As in earlier decades, the digital piracy of visual media in the 1980s lagged behind music piracy. This was largely because video had not yet been digitalised to the same extent as music, and remained in analogue VHS format until the late 1990s. DVDs for the popular market became available in the late 1990s. Initially, DVDs were difficult to copy because of copy protection (usually employing the Content Scrambling System or CSS) and the huge volumes of data involved. For example, the 1999 commercial DVD of the Disney film 'A Bug's Life' was over 4 Gb in size (not including 'extras') but blank recordable DVDs for the public market were limited at the time to 3.95 Gb.

In the late 1990s 'personal digital piracy' emerged as a phenomenon, as distinct from earlier forms of organised physical piracy of cassette tapes and CDs, (Enders Analysis, 2003). Initially this was through usenet internet groups but latterly through Napster, now BitTorrent and P2P (peer-to-peer) successors, and involved the sharing of the mp3 versions of copyrighted music, and more latterly film and software. No physical piracy was required. This digital (or cyber) piracy became possible for a number of reasons:

- The increased speed of the internet through the rapid take-up of broadband, allowing much faster bit rates.
- A reduction in file size, using compression techniques with no major loss in auditory or visual quality. For example, the mpeg4 ('divx' or 'avi') version of the film 'Shaun of the Dead' is about one-tenth of the size of the original DVD; approximately 750 Mb compared to 7.63 Gb.
- A further reduction in file size, using software designed to 'strip out' extras such as alternative soundtracks and subtitling.
- The circumvention of copy protection, using programs such as DeCSS which became widely and freely available through the internet.

Both personal and physical digital piracy ('illegal filesharing' and 'commercial music piracy' or 'counterfeiting' respectively) are now considered to be serious problems by the companies and organisations involved. For example, the BPI claims that 'Illegal peer-to-peer filesharing has already had an enormous effect on British music sales; with an estimated £1.1bn in revenue lost in the last three

years as a direct result' (BPI, 2007). However, as Wall (2007) and others note, the nature of online crime makes it difficult to accurately quantify statistics of this kind, and some industry-based organisations may have a particular interest in emphasising the seriousness of the problem.

1.6 A new criminology?

Many digital crimes can be understood and 'explained' in conventional criminological terms. For example, the miniaturisation of digital devices makes them more likely to be a target of crime, and their attractiveness to criminals can be understood, at least in part, through Clarke's familiar crime-reduction 'CRAVED' model (Clarke, 1999), as Table 1.3 illustrates.

However, what proportion of digital crime is actually new (in the sense of new forms of criminality) and how much is simply a modern manifestation of old (in some cases, ancient) and existing forms of crime? This issue has stimulated a lively academic debate, and as we alluded to earlier, is sometimes referred to as the '*plus ça change*' question, (from the French phrase '*plus ça change, plus c'est la même chose*' which may be translated as 'the more things change, the more they stay the same'.) For example, Hollinger (writing in 1997 on published research from 1976) noted that many of the early examples of 'computer abuse' were

Table 1.3 The CRAVED model and mobile phones

	Mobile phones pre 1990s (e.g. car phone)	Mobile phones 2007
Concealable	Typically up to 30 cm in length and hence not easily concealable	Easily concealable due to small size
Removable	Often fixed in some way inside a car	Rarely fixed, easily removable
Available	Rare	In many countries approaching or even over 100% market penetration
Valuable	Very expensive	A wide range of value
Enjoyable	Largely limited to business or other professional uses	Wide degree of functionality, added capability including mp3 playing, etc.
Disposable	Limited market for stolen mobiles	Vibrant market for second-hand mobiles, unofficial 'unchipping' services on offer

instead ‘simply older forms of deviance and crime ‘retooled’ for the computer age’ (Hollinger, 1997). Others argue that we are witnessing distinctly different and new forms of criminal behaviour, some of which can be attributed to the new ways in which we communicate and interact with one another. If there are distinctly new forms of criminal behaviour do we need matching new criminological theories? For example, David Wall outlines six commonly understood features of traditional criminal activity but concludes that ‘In contrast, cybercrimes would appear to exhibit nearly the opposite characteristics’ (Wall, 2005, p. 87).

Questions

Robin Bryant & Sarah Bryant

1. What activities illustrate the relationship between crime and technology in pre-modern eras?
2. What is ‘deindividualisation’ and how might this explain some online criminal behaviour?
3. ‘Internet and other new digital crimes pose a challenge to those traditional criminological theories that emphasise the importance of place and time’. In what ways do we have to adjust our ways of thinking about crime and policing with the advent of information and communication technologies?
4. ‘We should seek to distinguish between “true” cyber crime (i.e. dishonest or malicious acts which would not exist outside of an online environment, or at least not in the same kind of form or with anything like the same impact), and crime which is simply “e-enabled” (i.e. a criminal act known to the world before the advent of the worldwide web, but which is now increasingly perpetrated over the Internet)’. (Burden & Palmer, 2003, p. 222).
5. How far is this distinction still valid?

References

BBC (2000) Nailbomber set out to ‘terrorise’. BBC News [Online]. Available at: <http://news.bbc.co.uk/1/hi/uk/782876.stm> (Accessed: Oct 9 2007).

REFERENCES

25

- BPI (2007) Online music and the UK record industry. [Online]. Available at: http://www.bpi.co.uk/index.asp?Page=news/apu/news_content_file_825.shtml (Accessed: Oct 9 2007).
- Brenner, S. (2001) Is there such a thing as virtual crime?. *Californian Criminal Law Review* **4**(1).
- BT (2007) The historical development of BT. [Online]. Available at: <http://www.btplc.com/Thegroup/BTsHistory/History.htm> (Accessed: Oct 9 2007).
- Burden, K., Palmer, C. (2003) Internet crime – cybercrime – a new breed of criminal? *Computer Law and Security Report* **222** **19**(2):222–227.
- Clarke, R.V. (1999), Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods. (Police Research Series Paper 112) [Online]. Available at: <http://www.homeoffice.gov.uk/rds/prgpdfs/fprs112.pdf> (Accessed: Oct 9 2007).
- DiMarco, H. (2003) The electronic cloak: secret sexual deviancy in cybersociety. In: Jewkes, Y. (ed.) *Dot.cons: Crime, Deviance and Identity on the Internet*. Cullompton: Willan Publishing.
- Dupont, B. (2004) Security in the Age of Networks. *Policing & Society* **14**(1):76–91.
- Enders Analysis (2003) Piracy Will it kill the music industry? [Online]. Available at: [http://www.endersanalysis.com/enders/documents/Piracy%20ES%20\(Ref%202003-12\).pdf](http://www.endersanalysis.com/enders/documents/Piracy%20ES%20(Ref%202003-12).pdf) (Accessed: Oct 9 2007).
- Gill, M. (2007) *Modus operandi of a thief conducted amongst 13 convicted British burglars*. Perpetuity Research and Consultancy International Ltd on behalf of Halifax General Insurance Ltd.
- Grabosky, P. (2007) *Electronic Crime*. New Jersey: Pearson Education Inc.
- Hollinger, R. (1997) Introduction. In: Hollinger, R. (ed.) *Crime, Deviance and the Computer*. The International Library of Criminology, Criminal Justice and Penology. Aldershot: Dartmouth.
- Home Office (2006) Memorandum by the Government (Home Office and the Department of Trade and Industry). House of Lords Select Committee on Science and Technology, 29 November 2006 [Online]. Available at: <http://www.parliament.the-stationery-office.com/pa/ld200607/ldselect/ldsctech/999/6112902.htm>. (Accessed: Oct 9 2007).
- Intel Corporation (2007) Moore's Law. [Online]. Available at: <http://www.intel.com/technology/mooreslaw/> (Accessed: Oct 9 2007).
- Kshetri, N. (2005) Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management* **11**:541–562.
- McBride, B., Peterson, G. and Gustafson, S. (2005) A new blind method for detecting novel steganography. *Digital Investigation* **2**(1):50–70.
- Morris, S. (2004) The future of netcrime now: Part 1 – threats and challenges. (Home Office Online Report 62/04). [Online]. Available at: <http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf> (Accessed: Oct 9 2007).
- National Statistics Online (2006) Internet Access. [Online]. Available at <http://www.statistics.gov.uk/CCI/nugget.asp?ID=8&Pos=1&ColRank=2&Rank=704> (Accessed: Oct 9 2007).

- Ofcom (2007) Communications Market Report (23 August 2007) [Online]. Available at: http://www.ofcom.org.uk/research/cm/cmr07/cm07_print/cm07_1.pdf (Accessed: Oct 9 2007).
- Suler, J. (2004) The Online Disinhibition Effect. [Online]. Available at: <http://www.rider.edu/~suler/psycyber/disinhibit.html> (Accessed: Oct 9 2007).
- United States of America v. Mantovani and others (2004) [Online]. Available at: <http://www.usdoj.gov/usao/nj/press/files/pdf/files/firewallindct1028.pdf#search=%22firewallindct1028.pdf%22> (Accessed: Oct 9 2007).
- Vatis, M. (2005) statement to the Senate Judiciary Committee, Criminal Justice Oversight Subcommittee and House Judiciary Committee, Crime Subcommittee Washington, D.C. February 29, 2000, [Online]. Available at: <http://www.usdoj.gov/criminal/cybercrime/vatis.htm> (Accessed: 9 Oct 2007).
- Wall, D. (2004) What are Cybercrimes? *Criminal Justice Matters* **58** Winter 2004/05: 20–21.
- Wall, D. (2005) The internet as a conduit for criminals. In: Pattavina, A. (ed.) *Information Technology and the Criminal Justice System*. London: Sage Publications, pp. 77–98.
- Wall, D. (2007) *Cybercrime*. Cambridge: Polity Press
- Weimann, G. (2004) How modern terrorism uses the internet. [Online]. Available at: <http://www.usip.org/pubs/specialreports/sr116.pdf> (Accessed: Oct 9 2007)
- Yar, M. (2007) Teenage kirks or virtual villainy? Internet piracy, moral entrepreneurship, and the social construction of a crime problem. In: Jewkes, Y. (ed.) *Crime Online*. Cullompton: Willan Publishing.