1 Psychology of cybercrime

Case studies

Jack's computer has been running very slowly for a few days, and eventually he asks his friend to take a look at it for him. His friend downloads the latest version of an antivirus software program, which finds a virus on Jack's computer. Jack remembers downloading an email attachment received from his sister just before the computer began to slow down. When he searches through his sent messages, he discovers that the file has sent itself on to all of his contacts. Jack feels embarrassed having to tell all his contacts that he was the victim of a virus, and that they should all check their computers. He wonders why anyone would create such a malicious file, and what they have to gain from infecting his computer.

Michael has just been arrested. Police officers have found over 10,000 images and videos of child pornography on his computer, which Michael has downloaded from the internet. Michael claims that he hasn't really done any harm as he has never abused a child himself, nor has he ever uploaded any images to the internet.

Chapter overview

This chapter is designed to introduce the reader to forensic psychology. It may be that you are studying cybercrime as part of a wider forensic psychology module or course, in which case you may have already come across many of the concepts in this chapter, and you may prefer to move directly on to the rest of the chapters in this book. However, if you have never studied forensic psychology before, this chapter will provide you with some of the fundamental concepts of the field, especially those that relate to the study of the psychology of cybercrime.

Firstly, a brief description will be provided of forensic psychology, followed by a cursory overview of the different types of cybercrime and their categorisation. Following this the key areas that forensic psychologists specialise in are described, including offender profiling, offender assessment, punishment and rehabilitation, risk assessment, juries, helping victims, crime prevention and police psychology. Finally, an overview will be provided of some of the key theories of crime – the possible reasons why crime exists and why certain individuals

are more likely to become criminals than others. These theories are offered at various levels, from societal to individual, and many of the theories can be applied to cybercriminal acts.

Forensic psychology

Forensic psychology has enjoyed considerable popularity in the media for some time, with films such as *The Silence of the Lambs* and television programmes such as *Cracker* and *Criminal Minds* attracting large audience numbers and introducing many viewers to forensic psychological concepts. However, most of these programmes and films focus on one specific area of forensic psychology – offender profiling. While this is undoubtedly a very interesting topic within the field, and understandably popular among screenwriters and producers, relatively few forensic psychologists engage in offender profiling, and the majority of forensic psychologists actually work in prison settings (British Psychological Society, 2011). Torres *et al.* (2006) indicate that only about 10 per cent of forensic psychologists and psychiatrists have ever worked in offender profiling. Forensic psychology is made up of considerably more areas than offender profiling, and an overview of some of the definitions of forensic psychology provides insight into how diverse this field is.

Brown and Campbell (2010) indicate that even the 'term forensic psychologist is unhelpful and potentially misleading as no one individual can hope to have the breadth and depth of knowledge … Rather we think that there are a family of settings within which forensic psychology is applied and that context is critical to limiting claims of expertise' (p. 1). They argue that there is a lack of consensus as to the definition of forensic psychology. This is evident among the many definitions of forensic psychology that have been offered.

Some definitions, such as that of Blackburn (1996), are quite narrow in focus, suggesting that forensic psychology is 'the provision of psychological information for the purpose of facilitating a legal decision' (p. 7). Others are much broader, such as Wrightsman's (2001) definition of forensic psychology as 'any application of psychological knowledge or methods to a task faced by the legal system' (p. 2). Davies *et al.* (2008) also favour a broad definition, indicating that forensic psychology is a combination of both '*legal psychology* covering the application of psychological knowledge and methods to the process of law and *criminological psychology* dealing with the application of psychological theory and method to the understanding (and reduction) of criminal behaviour' (p. xiii). Nevertheless, Davies *et al.* (2008) do recognise that the use of the term 'forensic psychology' to encompass both legal and criminological psychology has been contentious.

Both Howitt (2009) and Brown and Campbell (2010) favour the broader definitions of forensic psychology, to allow for the inclusion of the work of psychologists who work in a wide variety of forensic-related settings, such as those described below. In this book, a similar stance will be taken, and a broad definition of forensic psychology will be subscribed to, encompassing any way in which psychology can aid in any stage of the criminal justice process.

Summary box 1.1 Forensic psychology definitions

- Many different definitions for 'forensic psychology' have been suggested, varying widely in the scope involved.
- While many of the general public associate forensic psychology with offender profiling, in fact only a small minority of forensic psychologists engage in this activity.
- For the purposes of this book, a broad definition of forensic psychology will be used, to encompass any way in which psychology can aid in the criminal justice process.

Cybercrime: a brief introduction

There are many different types of cybercrime, some of which will be explored in this book. As with crime in general, most types of cybercrime can be divided into 'property crimes' (such as identity theft, fraud and copyright infringement) and 'crimes against the person' (such as cybercrimes involving the sexual abuse of children).

Similarly, cybercrimes can be divided into internet-enabled crimes and internet-specific crimes. Internet-enabled crimes are those types of crimes that can also exist offline (for example, copyright infringement and the distribution of child pornography), but the presence of internet-enabled devices allows for easier and/or faster execution of such offences. Internet-specific crimes are those cybercrimes that do not exist without an online or computer-enabled environment (such as malware distribution and hacking offences such as denial of service attacks on websites). A third type of cybercrime is also possible – specifically 'crimes in virtual worlds' (Power, 2010; Power and Kirwan, 2011). These are events which occur between avatars (or characters) within online virtual worlds, which in offline settings would be considered to be criminal events (such as murder, theft, sexual assault or violence).

As with many other types of crime, cybercrimes vary in severity, method and motive. They also vary in how they are perceived by criminal justice systems around the world – what is considered illegal in one jurisdiction may not break any specific laws in another. In particular, crimes in virtual worlds can be difficult to define from legal perspectives, due to the varying acceptability of different behaviours in various virtual worlds.

Summary box 1.2 Cybercrime

- Cybercrimes can be defined in two main ways.
- They can be 'property crimes' or 'crimes against the person'.
- They can also be 'internet-specific', 'internet-enabled' or a 'crime in a virtual world' (Power, 2010; Power and Kirwan, 2011).
- Laws regarding cybercrimes vary across jurisdictions.

Components of forensic psychology

As mentioned above, forensic psychology involves many different activities and responsibilities, and most forensic psychologists choose to specialise in one or more of these areas. Two of the most common specialisms include offender rehabilitation and offender assessment, where a psychologist will try to determine if the offender is suffering from a psychological abnormality, if they are likely to reoffend and if they can be rehabilitated to reduce the likelihood of reoffending. Other psychologists examine how witnesses and victims can be helped when trying to recall details of an offence, while others attempt to find strategies that will encourage offenders to confess to their crimes, without increasing the risk of 'false confessions'. The detection of deception is another key area of forensic psychology, where specialists try to determine what the most reliable methods are for determining the truthfulness of responses. Some forensic psychologists work with police forces, attempting to reduce stress levels and devise the best methods of police recruitment and training. Others examine the behaviour of juries, trying to determine who makes up the most reliable juries and how members of the jury make decisions about guilt or innocence. The psychology of victims is also considered, and psychologists attempt to determine how victims can be helped within the criminal justice system and how they can reduce their likelihood of being revictimised. Similarly, psychologists can also work within communities in order to help in the development of educational strategies and other interventions that may reduce levels of crime. In this section, an outline will be provided of some of these activities, along with a brief overview of how they have been applied to cybercriminal events.

Offender profiling

Douglas *et al.* (1986) define offender profiling as 'a technique for identifying the major personality and behavioural characteristics of an individual based upon an analysis of the crimes he or she has committed' (p. 405). However, there are many approaches that can be employed during profile development (Ainsworth, 2001). These include:

- *crime scene analysis*. This is used as the basis for the United States Federal Bureau of Investigation's technique.
- *diagnostic evaluation*. This technique relies on clinical judgements of a profiler.
- *investigative psychology*. This technique utilises a statistical approach to profiling (although it should be noted that investigative psychology is generally considered to have a broader remit than profiling alone (Canter and Youngs, 2009).

Due, at least in part, to the popularity of offender profiling among the general population, a significant number of profilers have published descriptions of the cases that they have worked on and the profiles that they have developed (see, for example, Britton, 1997, 2000; Canter, 1995, 2003; Douglas and Olshaker, 1995, 1999, 2000).

Underlying most profiling methods are two key assumptions, as outlined by Alison and Kebbell (2006). These are the 'consistency assumption' and the 'homology assumption'.

- The 'consistency assumption' states that offenders will exhibit similar behaviours throughout all their crimes. So, for example, if someone engages in online fraud using an auction website, the consistency assumption dictates that they would use auction websites for most of their offences. However, there are problems with this assumption – the offender may have to change their method if they are banned from specific auction sites, or if they find that they are not making sufficient money from such a technique.
- The 'homology assumption' suggests that 'similar offence styles have to be associated with similar offender background characteristics' (Alison and Kebbell, 2006, p. 153). So for example, if the offender is generally a conscientious person, then that conscientiousness will be evident in how they complete their crimes. For example, perhaps the same fraudster described above will display a high degree of conscientiousness in managing their fraud, taking care to manage details of their crimes in such a way as to avoid apprehension. The homology assumption predicts that the same offender will also be conscientious in their day-to-day lives, perhaps ensuring a high quality of work in their employment or a carefully maintained filing system for personal documents. Again, there are problems with this assumption – individuals do not always display the same characteristics in different settings. For example, it is likely that you behave quite differently when you are among your classmates than when you are speaking to one of your lecturers. In relation to this, Canter (1995) describes the 'interpersonal coherence' aspect of the interaction between victim and offender, referring to how variations in criminal activity may reflect variations in how the offender deals with people in non-criminal circumstances.

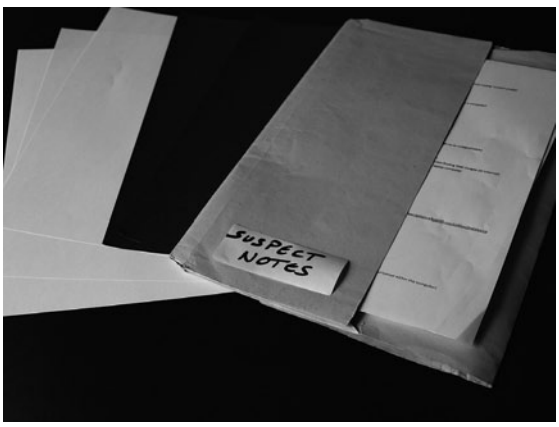

Illustration 1.1 Offender profiling and suspect characteristics. Offender profilers examine evidence from current and previous crime scenes, comparing what is known about the current offences to the behaviours of previously apprehended offenders. This information is used to predict the characteristics of the current offender.

While it should be remembered that it is difficult to verify the effectiveness and utility of offender profiling (Alison and Kebbell, 2006; Alison *et al.*, 2003), there are several studies which have examined how offender profiling might be useful in cybercrime cases. Gudaitis (1998) outlines a need for a multi-dimensional profiling method for assessing cybercriminals, while Nykodym *et al.* (2005) also indicate that offender profiling could be of use when investigating cybercrimes, especially where it is suspected that the offender is an insider in an affected company. Rogers (2003) indicates that offender profiling could be useful in a variety of ways for cybercriminal investigation, including helping the investigators to search hard drives more effectively, narrowing the pool of potential suspects, identifying a motive and determining the characteristics of victims which make them more appealing to offenders.

There is conflicting evidence regarding the consistency assumption in cybercrime cases. Jahankhani and Al-Nemrat (2010) suggest that due to the rapid changes in technology over time, it is possible that cybercriminal behaviour may also undergo rapid changes. Nevertheless, Preuß *et al.* (2007) report the analysis of twelve hacking incidents in Germany, and found that the methods used years ago were still the preferred methods of more contemporary hackers.

One of the key large-scale studies involving offender profiling and cybercrime was the Hackers Profiling Project (Chiesa *et al.*, 2009), which produced a large quantity of information such as demographics, socioeconomic background, social relationships, psychological traits and hacking activities. The results of this study are considered in more detail in Chapter 3. However, it should be noted that this project aimed to create a profile of hackers based on completion of a self-report questionnaire, rather than any attempts to develop a profile of a hacker from their activities and offences alone. Nevertheless, the scale and scope of the Hackers Profiling Project is an important initial step in developing the database of information required to make accurate profiles of offenders in the future.

Summary box 1.3 Offender profiling

- There are three main approaches to offender profiling: crime scene analysis, diagnostic evaluation and investigative psychology (Alison and Kebbell, 2006).
- Most approaches to offender profiling are based on two main assumptions – the 'consistency assumption' and the 'homology assumption'. However, there are flaws with both of these assumptions.
- While the potential benefits of offender profiling for cybercriminal cases have been noted by several authors, limited empirical research has been produced to date.

Psychological disorders and offender assessment

One of the most common activities carried out by practising forensic psychologists involves assessment of offenders. When serious crimes are reported in the news, people often feel that the perpetrator must have some psychological disorder, otherwise they would not have been able to carry out such horrendous acts. It is often the role of the

forensic psychologist to assess whether or not the offender meets the diagnosis for a psychological disorder and to provide a report or expert testimony in court (Gudjonsson and Haward, 1998). However, this role is sometimes complicated by a lack of agreement between psychology and legal systems as to what constitutes a psychological disorder.

While defining abnormal behaviour seems on the surface to be simple, when analysed in depth it is quite difficult to achieve. For example, in most cases if a person cries easily and frequently, we would consider their behaviour to be abnormal. However, if the person has just lost a close friend or family member but they do *not* show signs of psychological distress, then we would also consider their behaviour to be abnormal. As such, one of the key methods of determining abnormality relates to *discomfort* – is the person experiencing distress that continues over a long period of time or is unrelated to their current circumstances?

A second consideration of abnormality involves *dysfunction* – can the person manage their daily life effectively? Are they able to study, work and socialise, and can they maintain interpersonal relationships? It is important to consider the person's potential when doing this – if a student is generally weak at a subject like maths, and gets a poor grade, he or she may still be reaching their potential. However, if a normally strong student who usually gets A or B grades suddenly starts to fail their courses, it may be indicative of a problem.

A third method of defining abnormality involves *deviance*. In this sense, deviance refers to unusual (rather than specifically criminal or antisocial) behaviour. So, if a person experiences a symptom that most members of the population do not (such as violent mood swings or hallucinations), it may indicate a psychological disorder. Nevertheless, deviance alone is insufficient to define abnormality – it is unusual for a student to receive straight As in their exams, but it certainly would not be considered to be abnormal.

Psychological disorders are quite carefully defined, and lists of them (and their corresponding symptoms) can be found in the American Psychiatric Association's *Diagnostic and Statistical Manual* (*DSM*, 2000, 2011). Any offender may be suffering from a psychological disorder, and forensic psychologists will assess the suspect for symptoms of these disorders using a combination of clinical interviews, psychometric tests, clinical history and observations. Most abnormal psychology textbooks base their content on the DSM, but it is important to remember that the concept of *insanity* is a legal one, rather than a psychological term (Huss, 2009). There are many types of psychological disorders, and not all would lead to a diagnosis of insanity from a legal perspective. Indeed, the definitions of insanity have varied over time and jurisdiction, but most relate to understanding of right and wrong, or the control of impulses (see Foucault, 1965; Huss, 2009).

Activity 1.1 Psychological disorders

Using a current textbook on abnormal psychology, or a reputable website on the internet, identify the main signs and symptoms of the following psychological disorders: depression; bipolar disorder; schizophrenia; dissociative disorder; and antisocial personality disorder. How do the concepts of deviance, dysfunction and discomfort help to define these disorders?

There has been very little research to date investigating the link between psychological disorders and cybercriminals. However, it has been suggested that there is a link between Asperger's Syndrome (AS) and hacking behaviours (Hunter, 2009). AS is a disorder on the autistic spectrum, which is characterised by a significant impairment in social interaction skills, a lack of emotional reciprocity and repetitive and strong interests in a limited number of activities (Sue *et al.*, 2005), although there is intact cognitive ability and no delays in early language milestones (Toth and King, 2008). Several hackers have been diagnosed with this disorder, including Gary McKinnon and Owen Walker (Gleeson, 2008). Hunter (2009) indicates that these characteristics could lead AS individuals to spend more time with computers, indicating that 'For a person with Asperger's Syndrome, computers can provide a perfect solitary pastime as well as a refuge from the unpredictability of people' (p. 46). Certainly the focus that individuals with AS have on certain activities would benefit them if they wished to become accomplished hackers. However, care should be taken to remember that not all individuals with AS are hackers. Similarly, not all hackers have AS. As such, while there is substantial anecdotal evidence to suggest a link between hacking and AS, until an empirical study is completed in this area, a strong correlation between the two cannot be assumed.

Summary box 1.4 Psychological disorders and offender assessment

- Forensic psychologists are sometimes required to assess offenders or suspects in order to determine if they have any underlying psychological disorders, or if they meet the definition of insanity in their jurisdiction.
- Insanity is primarily a legal term, rather than a psychological one.
- Abnormal psychological states are often defined in terms of dysfunction, discomfort and deviance.

Punishment, rehabilitation and risk assessment

While it is common for serious offenders to be assessed when they are apprehended and before trial, a forensic psychologist may also be involved in later stages of their experience within the criminal justice system. Forensic psychologists often help to devise appropriate rehabilitation strategies and interventions and may be asked to assess the offender's risk of further offending behaviours, should the perpetrator be released. Such risk assessments can play an important part in the determination of early release suitability.

Legal systems often have a variety of punishments available, of which certain subsets are deemed to be suitable for various offences. If the offence is minor, the perpetrator may face a relatively light punishment (such as a fine for a parking offence). More serious crimes are associated with more severe punishments, such as imprisonment, community service, probation and in some jurisdictions corporal and capital punishment. Similarly, different punishments may have different aims, including deterrence,

rehabilitation, restitution or incapacitation (preventing the offender from committing further acts by 'incapacitating' them – perhaps by imprisonment or preventing them from accessing certain equipment or people).

Deterrence can be 'general' or 'specific'. Specific deterrence is aimed at the individual offender, in the hope that they will not reoffend, while general deterrence is aimed at society as a whole, in the hope that by punishing the individual, other members of society will be deterred from criminal acts. Both types of deterrence have been used in cybercrime cases. Smith (2004) discussed the case of Simon Vallor, who spent eight months in prison for writing computer viruses. Vallor stated that he '… would never try to create a virus again … Going to prison was terrible. It was the worst time of my life' (Smith, 2004, p. 6). In this instance, specific deterrence seems to have been achieved, although Smith also suggests that general deterrence is less effective in hacking cases, as many hackers feel that convictions can be difficult to obtain, and punishments only occur in rare cases. General deterrence has also been utilised in copyright infringement cases, where a relatively small number of individuals have received severe punishments for the illegal distribution of material such as songs, videos and software, although it again appears that this tactic has limited effectiveness in deterring most users from these activities.

It could be suggested that in an ideal world, all offenders should be fully rehabilitated so that they are no longer a danger to society and will not reoffend. In practice, unfortunately, this is unlikely to occur, although forensic psychologists attempt to determine the best strategies for working with offenders to reduce their risk. Rehabilitation programmes vary greatly – some of the most common ones involve substance abuse rehabilitation programmes that attempt to discourage offenders from committing property offences in order to feed drug habits. However, rehabilitation programmes are also provided for violent offenders, sex offenders and juvenile offenders, among many others. The type of rehabilitation provided depends on both the type of crime which has occurred and the psychology of the specific offender – not all offenders are suitable for rehabilitation, and psychologists and psychiatrists assess offenders to determine if they are suitable for, and will benefit from, rehabilitation programmes. Specific rehabilitation programmes have been suggested for individuals who commit child-related online offences, such as the distribution of child pornography, and these are discussed in more detail in Chapter 6. All rehabilitation programmes need to be carefully carried out, with suitable evaluations and controls, in order to determine their effectiveness.

The aim of restitution is to compensate the victim for the damage done by the offender's actions. For this reason, restitution is best suited to property offences, such as theft and vandalism. One example of the use of restitution involved Jammie Thomas-Rasset (BBC News Online, 25 January 2010), who was fined almost two million dollars in 2009 for sharing songs over the internet (although this fine was later reduced). In restitution cases, damages can be awarded to the victim (such as the music industry) in order to compensate them for any losses incurred. It is also possible that restitution may be a suitable tactic for crimes that occur in virtual worlds. However, restitution is less appropriate for other offences, such as distribution of child pornography.

The goal of incapacitation is to prevent the offender from committing any more crimes. Punishments which aim for this goal include imprisonment, where the offender is prevented from carrying out more crimes because of their incarceration. For cybercriminals, incarceration can take other forms, such as in the case of computer hacker Kevin Mitnick. When he was arrested he was held without bail, as US Magistrate Venetta Tassopulos ruled '… that when armed with a keyboard he posed a danger to the community' (Littman, 1996, as cited by MacKinnon, 1997, p. 17). Mitnick's access to telephones was also severely restricted. In modern society it is very difficult to restrict internet access completely, especially with the advent of internet-enabled mobile technologies such as smartphones. However, variations of such penalties have been considered for cybercriminals. It has been suggested that those who repeatedly download pirated music, videos or games should have their internet connection speed reduced to the extent that it would prohibit further downloading.

Activity 1.2 Punishment

Discuss the relative merits of deterrence, rehabilitation, restitution and incapacitation as punishments for cybercriminal acts. Consider specific cybercrimes (such as copyright infringement, child-related online offences, hacking, cyberterrorism, etc.). Develop a set of guidelines for one or more types of cybercrime which could be used by a court to determine an appropriate punishment for offenders.

A related responsibility of some forensic psychologists involves risk assessment. In these cases, the psychologist is asked to determine what the probability is of the offender committing further crimes, often for the benefit of parole boards who use the psychologist's report during their decision-making process. Predicting future criminal behaviour is extremely hard, even with the benefit of hindsight. A criminal may be considered to be at high risk of further offending, and so would not be released, but it could not be known with certainty if they would have offended again if they had returned to society. Similarly, an offender who is considered to be at low risk of reoffending and who is released may still reoffend, but avoid detection. When making such assessments, parole boards consider the type of criminal activity involved. For some types of property-related offences it may be preferable to err on the side of releasing the offender, as the consequences of an inaccurate assessment are relatively low. However, if the offender is an online child predator, it may be preferable to err on the side of continuing incarceration, as the consequences of releasing an offender who is still a danger to society are so great.

Summary box 1.5 Punishment, rehabilitation and risk assessment

- Forensic psychologists may be required to develop and implement appropriate rehabilitation strategies for offenders.