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
Psychology of cybercrime

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, 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.
Psychology of cybercrime

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.
Components of forensic psychology

- Punishment may involve deterrence, restitution, rehabilitation or incapacitation, or a combination of these devices.
- Appropriate punishment types vary according to the offender and the offence involved.
- Psychologists may be required to assess an offender’s risk of recidivism.

Police psychology

Police psychology includes a wide variety of other aspects of psychology, including eyewitness interviewing, suspect interviewing, police training, recruitment procedures and dealing with stress. It can also include topics such as offender profiling, as described above. Many police forces have dedicated cybercrime units (or at least, units which specialise in cybercrime cases alongside related crimes such as fraud). Forensic psychologists can help to identify suitable recruitment and training methods for the police officers who work in these units. However, a key potential support for police investigating cybercriminal cases which could be provided by forensic psychologists involves assistance in dealing with stress, and so this will be the focus of this section.

Stress is a normal part of everyday life for most individuals. At the moment you may be under a certain degree of stress. Perhaps you have to finish an essay for your professor, help your friend to move house, find a solution for a broken printer and manage to pay the rent and bills on time. Individuals vary in their ability to deal well with stress – some feel unable to cope with the smallest of tasks, while others seem to be able to deal with anything that life throws at them. Similarly, police officers can be subject to many kinds of stress (everything from administrative duties to being in life-threatening situations), and they also vary in how well they can deal with these stressors (a stressor is any stimulus which causes stress). Severe stress may result in the police officer experiencing post-traumatic stress disorder (PTSD) or acute stress disorder (ASD). These disorders involve the person having experienced an event involving fear, horror or helplessness, along with additional symptoms such as emotional numbing, heightened autonomic arousal (such as sleep disturbances or startle responses), flashbacks or intrusive memories (American Psychiatric Association, 2000).

Although dedicated cybercrime officers are less likely to be in life-threatening situations than police officers in other units (such as violent crime units), it is still possible that they may develop ASD or PTSD. They may also be at risk of Secondary Traumatic Stress Disorder (STSD), which has been associated with police officers who have been exposed to disturbing images of internet child pornography (Perez et al., 2010). Perez et al. also noted that police personnel who experienced STSD and burnout developed other symptoms, such as higher protectiveness of their family and general distrust.

Thankfully, computer software is available which reduces the requirement of police officers to examine each image of child pornography on a suspect’s data storage devices (such as computer hard drives and universal serial bus (USB) memory sticks).
Psychology of cybercrime

However, as new images are produced and distributed, it may still be necessary for cybercrime officers to examine such images to determine the severity of the abuse in the image, or the identity of the victim or perpetrator. Police psychologists can sometimes provide ‘stress inoculation training’, which helps the officers to deal with the horrendous task of sorting images while protecting their psychological wellbeing. Psychologists can also provide counselling for officers who have been exposed to such images.

Summary box 1.6 Police psychology

- Police psychology considers a number of topics, including police recruitment and training, offender profiling, eyewitness interviewing, suspect interrogation and dealing appropriately with stress.
- Post-traumatic stress disorder and acute stress disorder can occur after an event which caused fear, helplessness or horror. Symptoms include emotional numbness, heightened autonomic arousal, flashbacks and intrusive memories.
- Police officers who investigate cases involving child pornography may be at risk of secondary traumatic stress disorder (STSD) and burnout.
- Police psychologists can provide ‘stress inoculation training’ and/or counselling for police officers affected by cases.

Cybercrime juries

Juries are frequently portrayed in television programmes and films, so most people are familiar with the concept of what being on a jury involves. In real life, the task of jurors can be quite complex – evidence can be ambiguous, difficult to comprehend or unallowable in court, and the jury is required to sort through all the information in order to reach a verdict. One of the main difficulties in relation to cybercrime juries involves the specialist knowledge which may be required. In addition to understanding the legal terminology of the courtroom, the jury must also familiarise itself with the terminology relating to the specific cybercrime – terms such as ‘malware’, ‘social engineering’, ‘phishing’ and ‘advance fee fraud’ may be used, and jurors may not be familiar with them before the trial (definitions for each of these can be found in the relevant chapters of this book). Of course, it is not just cybercrime cases that demand specialist knowledge, and it has been argued that it would be better if juries were composed of experts, rather than lay people, although this claim is controversial (Walker, 2001). This lack of understanding of terminology is compounded by the finding that jurors can have poor recall of important information, especially in complex cases such as fraud (Nathanson, 1995).

Evidence presented in cybercrime cases can be confusing for jurors (Carrier and Spafford, 2004; Rogers, 2003; Smith and Bace, 2003). A specific example of potential confusion in cybercrime jurors is suggested by Carney and Rogers (2004). They indicate that some offenders and their lawyers may utilise the ‘Trojan defence’. 
This defence suggests that the defendant did not intentionally engage in the criminal act, but that they unintentionally installed software on their computer while downloading another file (see ‘Trojan horses’ in Chapter 4), and it was this software which carried out the offence. Carney and Rogers indicate that a good investigator may be able to determine if the defendant intentionally carried out the crime or not, but it may not be easy to convince a judge and jury of this (Casey, 2002; Smith and Bace, 2003). It is also interesting to consider how juries make decisions in cybercrime cases. While there are several models of jury decision making, Hastie’s (1993) cognitive story model is of specific interest here. This model suggests that jurors create a ‘story’ of the crime from the evidence presented, and they compare this to a schema (or script) which they associate with a certain criminal activity. For example, a juror’s schema for a violent assault may involve a lone individual, innocently walking down a street, who is set upon without cause by another individual or group. However, if the case presented in court doesn’t match this schema (perhaps the victim was intoxicated, and insulted the perpetrator), they may be less likely to convict the defendant as they don’t accept the act as criminal. It is important to note that jurors can have different schemas relating to the same offence, and so two individuals, given exactly the same evidence, may differ in their tendencies to acquit or convict. The cognitive story model is particularly interesting for cybercrime cases, where many members of the public may have uncertain schemas relating to the offences involved, which may add to their confusion. The ‘white hat defence’ which is sometimes offered by hackers (the suggestion that they only hacked into a system in order to highlight its vulnerabilities and to report these back to the system administrators) may be a specific example of how an offence does not fit in with a juror’s schema for the crime.

**Summary box 1.7 Cybercrime juries**

- Cybercriminal cases may require juries to familiarise themselves with both legal terminology and terminology relating to the cybercrime itself.
- It has been argued that expert juries may be more appropriate than juries composed of lay people, although this suggestion is not without controversy.

**Victims**

The victims of many crimes experience negative reactions after their victimisation, and victims of cybercrimes are no different. The reactions experienced vary depending on the type of crime experienced and the coping abilities of the victim, but can include ASD or PTSD, a need for retribution, self-blaming for their victimisation and ‘victim blaming’, where other people put some or all of the blame for the crime on the victim themselves.

Self-blaming activity occurs when the victim blames themselves for their actions in the lead-up to the criminal event, in the belief that had they behaved differently, they would not have been victimised. For example, a victim of a malware attack may feel...
that, had they taken more care to update their antivirus software, their computer might still be okay. Similarly, police, friends and family may have little sympathy for the victim, feeling that they should have taken better care of their computer. This ‘self-blaming’ and ‘victim-blaming’ can occur for almost any type of crime, and while it is certain that in some cases victims have left themselves vulnerable to attack, such behaviours often shift the focus of blame from the offender onto the victim. Mendelsohn (1974, as cited by Walklate, 2006) has suggested that there is a spectrum of shared responsibility between the victim and the offender. This theory, and similar ones proposed by other researchers, can be quite controversial, particularly in relation to offline sexual assault cases, but it can provide an interesting model for understanding self- and victim-blaming. It should be noted that in many cases victim-blaming is not meant to be malicious – police officers, family members and friends may feel that by chastising the victim for their negligence the victim may learn from their past mistakes. However, the victim may feel more upset by these actions, as the people that they turned to after the crime appeared unsympathetic.

ASD and PTSD can affect victims of crime (Scarpa et al., 2006; Hoyle and Zedner, 2007), with similar symptoms to those mentioned earlier in this chapter. Thankfully, as most cybercrimes are not life-threatening, incidents of ASD and PTSD in victims of cybercrime would seem to be very rare, although there is anecdotal evidence of some distress which has been experienced by victims of crimes in virtual worlds. This is examined in more detail in Chapter 10, but it is important to note that this area requires a great deal more empirical examination before strong conclusions can be drawn.

Finally, victims may experience a need for retribution – a desire that the perpetrator be punished for their actions. There has been some evidence for this in the families of homicide victims (Haines, 1996), but it can also occur in the victims of other crimes, including cybercrimes. Many people have experienced a situation where they feel that

Illustration 1.2 Self-blaming and victim-blaming. Victims of cybercrime may feel that if they had taken more care to protect their computer, they would not have been victimised. Such self-blaming can occur for almost any type of crime.
they have been wronged in some way, and a desire for revenge can be strong. Again, there is some evidence for this among victims of crimes in virtual worlds, and some case studies are presented in Chapter 10.

**Summary box 1.8 Victims**

- Victims of crimes can experience many consequences, including self-blaming; victim-blaming; acute stress disorder; post-traumatic stress disorder; and a need for retribution.
- There is some anecdotal evidence of crimes in virtual worlds evoking distress and a need for retribution in victims.

**Crime prevention**

While it is unlikely that cybercrime can ever be eradicated, it is possible that some crimes could be prevented. Various approaches could be taken to achieve this. For example, Welsh and Farrington (2004) describe interventions that could be used with at-risk groups in order to prevent them from progressing to criminal behaviour. Unfortunately, at present it is quite difficult to predict who will become a cybercriminal, although research in this area is accumulating. It is likely that if a more complete profile of the various types of cybercriminal could be achieved then interventions similar to those described by Welsh and Farrington could be implemented.

Other approaches suggest that potential victims should be educated in how to protect themselves and their property adequately, thus potentially reducing victimisation (see, for example, Farrell and Pease, 2006). Most cybercrime prevention strategies to date have been of this type, most notably with attempts to improve the safety of children online, although Tynes (2007) indicates that it is important that parents allow their children to experience the benefits of the online world while simultaneously protecting their children. Cybercrime prevention is also enhanced by the use of technology in the protection of users and equipment, such as secure log-ins, antivirus software, firewalls and child protection software (that can limit the websites that children visit and the amount of time spent online).

Forensic psychology can help the success of crime prevention strategies by identifying ways in which users can be encouraged to engage in safer online behaviours. LaRose et al. (2008) discovered that individuals are more likely to engage in safety behaviours if their personal responsibility and the positive outcomes of safe behaviour online are emphasised. Research from other fields in psychology could also be applied to crime prevention strategies, such as strategies for encouraging individuals to lead healthier lifestyles or social psychological research into persuasion techniques.
Summary box 1.9  Crime prevention

- Cybercrime prevention strategies can involve targeted interventions at potential offenders, victim education strategies and the use of technological protection measures.
- Psychologists can aid in prevention strategies by identifying methods of encouraging users to engage in safer online behaviours.

Forensic psychology – conclusion

As can be seen, forensic psychology can contribute to our understanding of cybercrime in many ways. Investigations and prevention of cybercrimes can be supported by drawing on the research and experience which has built up in forensic psychology over the past few decades. Nevertheless, it is also important that the limitations of forensic psychology are clear to investigators and others involved in cybercriminal cases. Media portrayals of offender profiling tend to promote it as more successful and exact than it is in real life, and it is important that any forensic psychologists working in cybercriminal cases honestly inform other professionals of the strengths and limitations of the field, so that unreasonable expectations and subsequent disappointments can be avoided.

Our attention now turns to an important question in forensic psychology – specifically, why do some individuals become criminals, while others do not?

Theories of crime

There has been a great deal of speculation as to why a person engages in criminal behaviour, often with the hope of identifying a method by which such criminality can be avoided or reduced. However, a single explanation for offending remains elusive. Instead, research findings suggest that criminality results from a variety of different causes, occurring at various levels (from societal levels, through community and social influence theories, to specific individual theories). The following pages will consider some of these theories, with particular focus on social influence and individual theories, as these have the greatest background in psychological theory and research. Some of these theories are currently popular, whereas others have fallen out of favour within the criminological community. Nevertheless, it should be remembered that the theories are not necessarily in competition with each other, and any specific criminality may have arisen from a variety of factors from a number of theories. A brief overview of the levels of explanation of crime will be provided, and then specific theories will be examined, including the social construction of crime, biological theories, learning theories, the complex theory of crime suggested by Eysenck, other trait theories of crime, psychoanalytic theories, addiction and arousal, neutralisation theories, labelling theories, geographical theories and finally routine activity theory.

Levels of explanation of crime

Theories of crime can occur at various levels (Howitt, 2009). These include high-level explanations of crime (such as societal theories and community theories) and explanations
Theories of crime

of crime that are targeted at more personal levels, such as socialisation influence theories and individual theories. Specific theories of crime might be contained within one level of crime, whereas others consider several levels in their attempts to explain crimes.

Societal, community, socialisation influence and individual theories

The highest-level theories of crime are societal (or macro-level) theories. Howitt (2009) suggests strain theory as an example of a societal level theory. At the core of this theory is the inability of all members of society to achieve all of society’s goals. For example, it is not possible for all members of society to be wealthy. Those members of society who cannot achieve the goal of wealth through legitimate means may be tempted to become wealthy through criminal or detrimental means, such as theft. The social construction of crime provides a method of applying societal theories to cybercrime, and is examined in more detail below.

The next level of theories of crime involves community theories. Perhaps you know of the ‘good’ and ‘bad’ areas within your community, and it is often a key variable in people’s decisions regarding where to live. Certain areas of cities and towns have higher crime rates than others, and these are generally (but not always) the areas that suffer from economic deprivation. Such geographical distributions of crimes are not confined to within cities – there are often major differences in crime rates between urban and rural areas, and even between countries. Due to the nature of the internet, such geographical distributions are probably not as indicative of cybercrime as they are of other types of crime. However, at an international level, some countries are associated with higher levels of crime than others. This is explored below in the section on geographical theories of crime.

Socialisation influence theories have a strong basis within psychology, particularly the areas of social and developmental psychology. These theories examine how the individual’s family, friends and other contacts (such as teachers) affect their likelihood of becoming an offender. They also examine the effects of other influences, such as media (television, computer games, books, internet and other stimuli), on the person. As such, ‘observational learning’ is a key concept within socialisation influence theories – as humans we learn how to behave in new situations by watching others’ behaviours. Similarly, criminal behaviour is often learnt by observing other criminals in action.

Finally, individual theories examine the specific characteristics of the person to determine their likelihood of offending. Reviewing the theories mentioned so far, it is possible that two individuals, while being brought up within the same society, in the same community and with the same socialisation influences, may differ in their eventual criminality. In these cases, it is possible that some specific set of characteristics may determine if a person goes on to display criminal tendencies. These characteristics may be psychological in nature (such as certain personality or cognitive traits) or they may be biological (such as neurological, neurochemical, physiological or genetic). Several individual theories are considered in this chapter.

Summary box 1.10 Levels of explanation of crime

- Theories of crime attempt to explain why crime exists, and who is most likely to become an offender.
Howitt (2009) suggests that theories of crime can occur at several levels, including societal theories, community theories, socialisation influence theories and individual theories.

Applying theories of crime to cybercrime

There are many different theories of crime, which can be classified at one or more of the four levels of explanation of crime. Here, we will examine some of the most relevant theories of crime in terms of psychological influence and application to cybercrime. Nevertheless, it should be remembered that this is not an exhaustive list of theories, nor can the full complexity of any of the theories be described in detail here. Some key handbooks and collections of classic texts in criminology and forensic psychology (such as Brown and Campbell, 2010; Maguire et al., 2007; Muncie et al., 1996) provide more thorough explanations of each of these theories and should be consulted by the interested reader.

Social construction of crime

Howitt (2009) explains that it is important to consider how crime ‘simply is not a static, universal thing that needs no explanation in itself’ (p. 78). Society determines what is and is not a criminal act, and an event may be defined as criminal or not depending on a particular set of circumstances. For example, if you take another person’s property, it is a criminal act if you do so without their permission, but not if they allow you to take the item. In addition to this, what constitutes a crime varies from jurisdiction to jurisdiction – certain recreational drugs are legally available in some countries, but not in others. The criminality of an action also varies according to the time the act occurs in – consider the prohibition of the distribution of alcoholic drinks in the US during the 1920s. There have been much more recent changes – same-sex sexual activity was decriminalised in Ireland in 1993.

When considering the social construction of crime, cybercrime is a very interesting case. Some cybercrimes were already defined as criminal events due to their similarity to offline counterparts. These types of offences are often considered in the literature to be ‘old wine in new bottles’, as it is thought that the nature of the crime has not changed, but merely the mechanism by which the crime has been carried out. Offences such as the distribution of child pornography online can be included in this categorisation.

However, not all negative online activities could be classified as criminal quite so easily. For example, the distribution of malicious software or virtual assaults on avatars in online virtual worlds do not fit quite as easily within pre-existing laws. In some cases, laws have had to be developed to deal with such acts, while in others, there is still uncertainty as to how such actions should be considered by legal authorities. Chapter 2 examines the legal situation relating to cybercrime in greater detail.

Biological theories of crime

A ‘comparison of the criminal skull with the skulls of normal women reveals the fact that female criminals approximate more to males, both criminal and normal, than to normal
Theories of crime

women, especially in the superciliary arches in the seam of the sutures, in the lower jaw-bones, and in peculiarities of the occipital region’.

(Lombroso and Ferrero, 1895, p. 28)

The above quote may seem bizarre in the modern context, but at the time of writing it was a relatively common belief that criminals could be recognised by their physiological characteristics. Phrenology is a classic example of this theory, and many psychologists and physicians keep a ‘Fowler’s phrenology head’, which attempts to map psychological constructs onto various parts of a person’s head. Lombroso (as cited by Jamel, 2008) suggested that criminal brains would differ in shape from those of non-offenders, specifically that they would be less developed and have certain facial characteristics, such as thick lips, a receding chin, a large jaw and an asymmetrical face. Despite the prevalence of phrenology heads in surgeries and offices, they are generally kept only for decorative purposes, as these theories have long been refuted.

Illustration 1.3 Fowler’s Phrenology Head. This attempted to map psychological characteristics onto certain areas of the head, and it was thought that an individual’s personality could be read by examining the size and shape of the skull. Some of the characteristics that were supposedly mapped could have related to criminality, such as combativeness, destructiveness, integrity and justice.
Although phrenology is not seriously considered to be a useful tool in predicting criminality, other biological factors may provide more insight. For example, damage to certain structures within the brain may result in deficiencies in planning or changes in personality, which may increase the likelihood of criminal activity, although there are problems in determining a causal relationship and, as such, findings in this field should be interpreted with caution (Jamel, 2008). Similarly, it is possible that unusual neural activity levels in certain areas of the brain may be associated with Antisocial Personality Disorder, which is characterised by aggressiveness, irresponsibility and criminal activity (Davey, 2008, pp. 412–18).

Other possible biological theories examine genetics (for example, males commit more crimes than do females), evolutionary explanations (see Ward and Durrant, 2011 for a review) and levels of neurotransmitters and hormones (such as testosterone). Some researchers have indicated that there may be links between genetics, neural structures and antisocial behaviour (see, for example, Raine, 2008), while others have sought to integrate biological correlates of crime with other criminological theories (see, for example, Armstrong and Boutwell, 2012). The possibility of focusing on biological and physiological risk factors early in life as a method of crime prevention is another potential area for exploration (see, for example, Rocque et al., 2012). However, while there is some evidence that most cybercriminals are male (see the specific literature in each of the chapters of this volume), there is little other research examining the biological construction of those who offend online. As such, it is unknown how useful biological theories are in the explanation of cybercrime.

**Learning theories and crime**

As with all other skills and behaviours, criminality is learned by offenders. There are many methods of learning a new skill, and a great deal of psychological literature has examined how this can take place. Sometimes we learn via trial and error – we literally learn from our mistakes. While attempts have been made to predict criminality using a variety of learning theories, operant conditioning and observational learning are probably of the most interest here.

Operant conditioning examines how individuals learn behaviours due to the consequences of actions and events. Much of the early work in operant conditioning was completed by B. F. Skinner, who worked mostly with laboratory animals, such as rats and pigeons. He taught these animals to complete different tasks, such as turning in circles or pecking a sign, by rewarding them with food. In a similar way, humans can learn to adapt their behaviours as a result of the consequences of those actions – we learn that if we put a lot of effort into studying for an exam, we are more likely to receive a high grade than if we did not study. This affects our future behaviours – if we wish to receive a high grade in future exams then we are more likely to study for them. Similarly, criminal actions can have high levels of rewards – there may be financial rewards if we steal a person’s wallet, or we may experience a release of frustration if we act aggressively. However, the criminal act may also result in punishment – perhaps we will be caught, and may face imprisonment or another penalty. Operant conditioning suggests that offenders will continue to engage in acts that are reinforced and rewarded, while avoiding acts that are punished. The offender may consider the
Theories of crime

likelihood of being apprehended and punished, and if they consider that to be of low risk, may choose to engage in the behaviour which is assumed to result in high benefit. In some types of cybercrime, such as copyright infringement, the offender may feel that it is unlikely that they will be punished, especially due to the perceived anonymity provided by the internet. At the same time, the perceived rewards are quite high – the offender can obtain the desired video, music or software for free in a short period of time. Rational choice theory is a popular criminological theory which is based on the principles of operant conditioning. It suggests that the offender weighs up the potential costs and benefits of the crime before deciding whether or not to carry it out.

As mentioned earlier, observational learning relates to how learning occurs through observing how other people behave in similar situations, and later imitating that behaviour. Albert Bandura carried out research in this area and demonstrated that children will imitate violent acts conducted by adults if the adult is reinforced for their violence (Bandura, 1965). Research in forensic psychology suggests that criminal behaviour is also learned from others – individuals have been found to be more likely to become criminals if their parents, siblings or peers are also offenders (see, for example, Farrington et al., 2001; Fergusson et al., 2000; Robins et al., 1975; West and Farrington, 1977). Similarly, such social learning seems to be an indicator of a person engaging in some cybercriminal acts, such as virus developers (see Chapter 4) and copyright infringement (see Chapter 8).

Eysenck’s theory of crime

Eysenck attempted to develop a theory of crime which combined genetics, personality traits and environmental factors, and examined how each of these types of factors, and the interactions between them, might impact on a person’s likelihood of becoming a criminal (Eysenck, 1977, 1987/1996; Eysenck and Eysenck, 1970, 1977). In particular, Eysenck examined extraversion, psychoticism and neuroticism, and suggested that those individuals who had high levels of these three personality traits would be more likely to be involved in criminal behaviour, but that individual differences may occur. Eysenck’s theory is quite complex, and encompasses several levels of theorising, but it has been the target of much criticism due to a lack of support by research findings.

Other trait theories of crime

While Eysenck selected psychoticism, neuroticism and extraversion as the traits which he identified as related to criminal activity, many researchers in forensic psychology have examined other personality and cognitive traits which may be related to offending. These include moral development (see, for example, Palmer and Hollin, 1998; Trevethan and Walker, 1989), empathy (see, for example, Broidy et al., 2003; Jolliffe and Farrington, 2004), intelligence (see, for example, Levine, 2008; Lopez-Leon and Rosner, 2010), self-control (see, for example, Baron, 2003; Conner et al., 2008; Holtfreter et al., 2010; Piquero et al., 2007) and impulsiveness (see, for example, Meier et al., 2008).

There is varying support for each of these traits as a correlate or predictor of criminality – some characteristics demonstrate more reliable results than others.
This may be due in part to the differences between offenders – the psychological profile of a fraudster may be very different to the psychological profile of a murderer. Even within the subset of cybercriminals, there may be a wide diversity of traits between offenders – it is likely that there are major differences between, for example, cyberterrorists and distributors of child pornography. Nevertheless, there are some findings regarding the personality traits of cybercriminals, with hackers being found to generally have poor interpersonal relationships (see Chapter 3) and those who illegally download files often having low levels of self-control (see Chapter 8). Of course, it should be remembered that even within these groups, there can be offenders who are exceptions and do not fit the profile created. However, identification of general traits that may be associated with specific cybercriminal types can be useful in the development of crime prevention strategies and rehabilitation of offenders.

Psychoanalytic theories of crime

Psychoanalytic theories of crime often focus on the unconscious struggle between the id (an unconscious construct that seeks pleasure and destruction) and the ego, which attempts to curtail the id, while guided by the superego (an internalisation of society’s morals and standards). If the superego is not formed properly during childhood, criminal behaviour may occur. However, it has been suggested that psychoanalytic theories do not comprehensively account for criminal activity (Blackburn, 1993), and that crimes which require rational thought and conscious planning, such as white collar crimes, cannot be easily explained by a theory involving unconscious conflict (Kline, 1987). As many cybercrimes require such planning, psychoanalytic theories may not be useful. Nevertheless, there are exceptions, such as online child predators, and De Masi (2007) and Socarides (2004) consider how psychoanalytic theory might explain paedophilic behaviour.

Addiction and arousal theory

Arousal theory suggests that individuals enjoy a certain level of arousal or excitement, and will engage in acts to maintain this level. It helps to explain why some individuals engage in extreme sports, or take part in potentially risky behaviour for enjoyment. McQuade (2006) suggests that arousal theory might be a suitable explanation for cybercrimes such as those of cyberstalkers and hackers, who may experience a psychological thrill from their pursuits.

Similarly, Howitt (2009) considers how criminal behaviour may be an addiction. Firstly, many criminals also have alcohol or substance addictions. Secondly, successful treatments for criminality are often similar to successful treatments for addictions. Finally, Howitt cites research examining joyriders by Kilpatrick (1997) and shoplifters by McGuire (1997) who noted that offenders showed some characteristics of addiction including conflict (knowing that their actions had negative consequences), withdrawal, relapse and tolerance (having to carry out more, or more serious, offences in order to get the same emotional effect). In addition, Howitt suggests that addiction theory may explain why some juvenile offenders persist in their behaviours and become life-long offenders, while most ‘age-out’ (a similar trend has been noted among cybercriminals such as virus developers). However, there is little evidence to support a relationship between addiction or arousal theory and cybercrime.
Neutralisation theory
People frequently hold a relatively narrow definition of crime, which includes serious offences (such as murder, theft and assaults). However, other offences, while still criminal acts, are often not considered to really be crimes by the person. One of the authors (Kirwan) has taught over a dozen groups of students about forensic psychology, and in the first lecture she tests the students to see how they define criminality. At first, the students are asked if they are a criminal. In some cases one or two students will identify themselves as criminals, but in most groups, no-one will consider themselves to be so. The question is then rephrased – the students are provided with a list of activities, and asked if they have ever engaged in any of them. These activities include ‘day-to-day’ offences, such as driving a car over the speed limit, illegally downloading music or videos, drinking or taking other substances before being of legal age to do so, and even ‘borrowing’ something from a friend or workplace without the intention of returning it. The exercise demonstrates to students that the definition of crime is much broader than they might think it is, but it also demonstrates neutralisation theory. The students have convinced themselves that these crimes are excusable, and not really offences, for a variety of reasons (most often, because they do not feel that their actions really harmed anyone).

Neutralisation theory was initially developed by Sykes and Matza (1957), and it describes how offenders might offer explanations for crimes that they would normally consider to be morally unacceptable. Such excuses can include denying responsibility for their actions (perhaps by suggesting that they had to download a television programme from the internet because it wouldn’t be shown locally for several months). Another neutralisation includes denial of injury to the victim – again in the illegal download of the television programme, the offender may suggest that they are not really doing any harm to the makers of the programme. A common neutralisation cited by those who download music illegally is that they are actually helping to launch the career of the musician by spreading the word about their talent. Neutralisations are also common among those who engage in child-related sexual offences; in this case the literature often refers to them as ‘cognitive distortions’ and further information is provided in Chapter 6. Of course, the justifications provided by offenders do not really excuse the criminal behaviours in most cases, but they allow the offender to carry out the act without reducing their self-image – they can maintain a belief that they are a caring, considerate and law-abiding citizen despite their actions.

Activity 1.3 Neutralisations
It is not just offenders who employ neutralisations. Consider the last time that you used neutralisations to explain or excuse your behaviour. Perhaps you postponed completing an essay for class because you ‘deserved a break’? Or maybe you justified an expensive purchase because your friend owned a similar item? Attempt to identify what types of neutralisations might be employed for cybercrimes such as hacking, virus writing and identity theft. Consider Michael’s case study at the start of this chapter, and discuss his use of neutralisations – do they excuse his behaviour? Should he still be prosecuted for downloading child pornography?
Labelling theory
The labels that are applied to people impact both how society treats them, and how the person behaves. If you currently hold the label of ‘student’, you are likely to behave in ways that are in line with that label – you go to classes, read relevant texts, complete coursework and possibly engage in some of the socialising that is commonly associated with student life. Similarly, society will treat you in a certain way because of your ‘student’ label – people will have a stereotypical image of what you do, how you behave and how you spend your time. If you are a psychology student, you may have experienced a common response from a stranger who has just learned about your chosen course of study – ‘Are you analysing me?’ The ‘label’ of ‘psychology student’ elicits a specific response in many members of society that is frequently inaccurate.

Labelling theory suggests that individuals experience a similar response when given the label of ‘criminal’. If they perceive themselves as a criminal, then they may be more likely to engage in further criminal activity. Similarly, society often distrusts those labelled with the term ‘criminal’, and the person may find it harder to find work. For this reason, many police forces attempt to avoid labelling a young person as an ‘offender’ following a relatively minor infringement – it is thought that if the label can be avoided, then it is possible that further offending might also be avoided.

Labelling theory has an interesting application in the case of hackers, where many different labels have been associated with various types of hacking activity as those involved attempt to differentiate themselves from each other on the basis of motive or ability. On the other hand, some cybercriminals do not identify themselves as offenders (see the section on neutralisation theory above), and it may be necessary to educate those involved as to the criminality of their actions. A specific example of this involves copyright infringement, and some agencies have developed short video clips, commonly shown at the start of DVDs, which attempt to highlight the criminality of copyright infringement.

Geographical theories
If you think about the city or county you live in, which areas seem to have the highest rate of crime? In general, crime rates tend to be higher in urban areas than rural ones. The geographical distribution of crime has been of interest to many researchers in criminology, and the Chicago School of Sociology found that young offenders tend to live in certain areas within cities (Bottoms, 2007). Geographical theories of crime also examine crime rates in smaller communities, such as within housing estates, and on a much larger scale, by examining which countries are associated with particularly high or low crime rates.

For cybercriminal activity, it is very difficult to examine local levels of crime. However, some trends do seem to be notable at international levels. Symantec regularly releases security reports (see, for example, Symantec, 2011b), which investigate which countries most cybercrime originates from. Countries such as Brazil, China, Russia and the US can regularly be found within the top ten lists of these reports. This may in part be due to the methods by which Symantec captures the data (Whitney, 2010), but may also be indicative of high rates of cybercriminal activity in these countries due to access to computers or the internet. Greenberg (2007) quotes Bill
Theories of crime

Pennington of White Hat Security, who suggested that young computer graduates in Russia or China may be engaging in cybercrime for financial reasons. This has yet to be tested empirically, and there may be other reasons why these countries, and others worldwide, are the source of cybercriminal activity.

Routine activity theory
The final theory which we will consider is routine activity theory, outlined by Clarke and Felson (1993). This theory suggests that a crime needs three variables to occur at the same time: a motivated offender, a suitable target and an absence of guardians. If, for example, you have a car (a suitable target) which is left unattended and unprotected (an absence of guardians), a crime still will not occur unless a suitably motivated offender also happens to visit the same location. As such, routine activity theory has some overlap with the geographical theories as motivated offenders are more likely to be present in certain areas of cities and countries.

In a similar manner, a computer is more likely to be hacked if it is seen as a suitable target (perhaps it would be useful because of its processing power, or it is particularly desirable because of the organisation that owns it), is unprotected by guardians (say for example, a lack of adequate antivirus software or a firewall) and is noticed by a motivated offender (perhaps a hacker who wishes to obtain information, or to control the computer as part of a botnet – a network of computers that are controlled by a hacker). Routine activity theory can be applied to almost all types of malicious online behaviour, and as such can be very useful in furthering our understanding of how and why a specific cybercrime occurs.

Summary box 1.11 Theories of crime
- The social construction of crime suggests that society determines what is and what is not a criminal event, and this can change across cultures and history.
- Biological theories of crime include phrenology, neural activity levels, neural structures, genetics, neurochemicals, hormones and evolutionary theories.
- Learning theories of crime include operant conditioning and observational learning.
- Eysenck suggested a theory of crime which considered genetics, environmental variables and personality traits, but it has been criticised due to a lack of support by research.
- Trait theories attempt to determine if certain cognitive or personality traits can be associated with criminality.
- Psychoanalytic theories suggest that criminality occurs because of an inadequately developed superego.
- Arousal theory suggests that criminal activity fills a need for a certain level of arousal in a person which may be met by extreme sports or other potentially risky behaviours in other individuals.
- It is also possible that criminal behaviour is addictive.
- Neutralisation theory describes how individuals might offer explanations for their criminal behaviour in order to maintain a positive self-image.
Labelling theory examines how individuals might engage in certain behaviours, or be treated a certain way by society, depending on the 'criminal' label which has been assigned to them.

Geographical theories examine how crime is distributed at various levels. Some information about the international distribution of cybercrime is available.

Routine activity theory was outlined by Clarke and Felson (1993). It suggests that criminal events require three variables to occur simultaneously: a motivated offender, a suitable target and an absence of guardians.

Conclusion

It is certain that forensic psychology can add a great deal to our understanding of cybercrime, and the chapters that follow describe research that has been carried out in specific types of cybercrime. Theories of crime can help to explain why cybercrime occurs, although some are of greater use than others, and few have been empirically investigated with a particular focus on cybercrime. It should be remembered that psychological research into cybercrime is still at a relatively early stage and, in many cases, very little empirical work has been completed. It is important that more researchers focus on the psychology of cybercrime so that gaps in current knowledge can be filled and hence forensic psychology can be of greater assistance to cybercrime investigators. Forensic psychology holds huge potential for a variety of areas, including offender rehabilitation, victimology, offender profiling and crime reduction strategies, as well as benefiting juries and police officers in cybercrime cases.

Essay questions

(1) Forensic psychology is often portrayed in the media as mainly involving offender profiling. Describe the other key roles of forensic psychologists, and consider the accuracy of the media portrayal of forensic psychologists.

(2) Compare and contrast statistical and clinical offender profiling.

(3) No single theory of crime can explain why an individual engages in criminal acts, but in combination they can be a powerful predictor of criminality. Discuss.

(4) Different theories of crime are useful for different types of criminality. Consider in light of at least three types of cybercrime.

(5) Crime reduction strategies should focus on society rather than individual criminals. Discuss.

Additional reading

Dozens of excellent texts are available on the topic of forensic psychology, but the following are particularly useful if you’d like to understand the area in more detail:
Additional reading


Websites

The website www.forensicpsychology.net has a number of useful links relating to several areas of forensic psychology, including crime scene investigations, mental health, capital punishment and cognitive science.

The British Psychological Society’s Division of Forensic Psychology website includes information about forensic psychology as a career path, along with details of journals and upcoming events. Visit http://dfp.bps.org.uk/dfp/dfp_home.cfm for more information.

Similarly, Division 41 of the American Psychological Association is the American Psychology-Law Society, with more useful information on careers, publications and events: www.ap-ls.org.