INTRODUCTION

As more individuals own and operate Internet enabled devices, and more critical governmental and industrial systems rely on advanced technologies, the issue of cybercrime has become a crucial concern for both the general public and professionals alike. There have been several recent news stories relating to cybercrime. These include relatively low level irritations, such as links to malware on social networking sites (BBC News, 2010), as well as the much more worrying fear that a complex computer worm which is capable of causing disruption to major systems such as transport, emergency and power systems, may have reached the black market and become available to terrorists (Kiley, 2010).

To illustrate the importance of the psychology of cybercrime, a recent case study can be explored. A very high profile cybercrime case occurred in April and May of 2011, where millions of users of the Sony Playstation Network and Sony Online Entertainment had personal details stolen by hackers (BBC News, 2011a). Users of the services had a great deal of personal information taken, including dates of birth, credit card details, names and home addresses. These attacks had a significant effect on Sony itself, with calls for the CEO to resign and a drop in share prices. At the time of writing, it is still unclear as to exactly who completed the attack and why, but this is one area where a deeper understanding of the motives and psychology of hackers, a topic outlined in Chapter 4, could be of assistance to cybercrime investigators as they attempt to identify the culprits. The attacks also led to strong psychological reactions in users. Many considered switching to alternative gaming consoles and networks as their trust in Sony and the Playstation Network had been adversely affected (GamePolitics.com, 2011). Internet users who are the victims of cybercrime can experience strong psychological reactions, even if the crimes occur purely in the virtual world, and these reactions are explored in Chapter 12. It is crucial that these psychological reactions of victims are understood, and not belittled by companies and organisations online, as to do so could result in significant losses as consumers turn to more ‘caring’ or considerate rivals. Those customers who did remain with Sony found themselves facing additional worries, as an exploit was found on the website which was set up to allow users to reset their passwords, which would allow hackers to impersonate users (BBC News, 2011b). Chapter 6 considers why online users are at such high risk of identity theft, and the methods by which such risks can be reduced. As with many types of offline crime, it is preferable to prevent cybercrime whenever possible, as to do so avoids unnecessary financial losses and psychological stresses. In this regard, many chapters of this book explore how cybercrimes can be prevented, particularly in relation to information campaigns targeted at internet users. How these campaigns are presented and implemented influences how effective they can be, and
an understanding of psychological principles can help to develop influential and successful campaigns that reduce the risk of victimisation.

While there have been several books on cybercrime published over the past decade (from the early works by Wall, 2001 and Thomas & Loader, 2000 to the more recent works, such as that of Jewkes & Yar, 2010), these primarily focus on technological, sociological or criminological aspects of cybercrime, with limited psychological analysis. Similarly, while several journal articles and book chapters have begun to examine psychological aspects of cybercrime, and some books have been written about the psychology of particular cybercrimes (see for example Chiesa, Ducci & Ciappi, 2009 regarding hackers; Taylor & Quayle, 2003 regarding child pornography; Sheldon & Howitt, 2007 regarding sex offenders) no single central resource was available which would provide the reader with both an overview of the main types of cybercrime, and how forensic psychology could provide insights into the phenomena. The Psychology of Cybercrime: Concepts and Principles attempts to address a gap in the literature for a book that primarily focuses on how principles of forensic psychology could be applied to cybercrime cases.

This book draws on the expertise of the authors in cyberpsychology and online governance. As with the study of cybercrime, cyberpsychology is also a growing area – it has developed from early texts, such as Wallace’s (1999) “The Psychology of the Internet” to the more recent “Oxford Handbook of Internet Psychology” (Joinson, McKenna, Postmes, & Reips, 2007) and “Psychological Aspects of Cyberspace” (Barak, 2008). There are also a number of peer-reviewed journals in the area, including Cyberpsychology, Behaviour and Social Networking (formerly Cyberpsychology and Behaviour), Computers in Human Behaviour and The Journal of Computer Mediated Communication, along with an increasing number of specialist international conferences. While some of the theories, models and research in conventional psychology can be directly applied to cyberpsychology, this is not always the case, and as such this provides a basis for the argument that cyberpsychology could be considered to be a qualitatively new area within psychology (Kirwan, 2010). Human behaviour online cannot be explained simply by examining offline behaviour and extrapolating from this to predict how people will behave on the Internet. Similarly, the study of forensic cyberpsychology requires particular focus in order to determine how similar online crime is to its offline counterpart.

This Psychology of Cybercrime is designed as a source for researchers and practitioners in the disciplines of criminology, cyberpsychology and forensic psychology, though it is also likely to be of significant interest to many who work in the field of information technology and other related disciplines. The Psychology of Cybercrime applies the theories of forensic psychology directly to cybercrime. Where research has been completed about a specific cybercrime, the key findings are presented with appropriate critical analysis. If there is limited psychological research about the specific cybercrime, the literature from similar offline crimes (such as in the case of terrorism) is examined and an exploration of how this literature can be applied to the online world is presented.

The Psychology of Cybercrime is not limited to documenting offenders and their behaviours. Consideration is given to the effects on victims, legal and governance issues, punishment and preventative measures. The chapters are organised to address specific categories of cybercrime and include case studies that provide examples to which the theory can be applied. Key definitions are provided and, as might be expected in a field as dynamic as cybercrime, suggestions for further research and areas for further development are proposed. In many cases, practical suggestions for methods of tackling the problems are discussed.

The text is divided into four sections. The first section provides the reader with a foundational review of the key disciplines. Chapter 1 sets the scene for remainder of the book by providing the contextual
background to cybercrime. The nature of online crime or cybercrime and the ways in which society is responding to it is explored. The legal response to cybercrime is reviewed as is the field of online governance. Chapter 2 considers how forensic psychology can aid in the examination of cybercrime. The role of a forensic psychologist is discussed as is their current involvement in cybercrime, and how this involvement might be further expanded. Chapter 3 discusses the various theories of crime which form an important part of criminological literature. Different theories address the issue of crime at various levels, ranging from societal, through community and socialisation influence theories, to the most specific level, individual theories. The goal is to determine which theories are most suitable for further investigation and apply best to cybercriminal cases.

The second section identifies internet specific crimes, or offences that could not exist without the use of computers. Chapter 4 looks at the subject of hacking; the motivations of hackers, the value of psychological profiling in hacking cases, the punishment of hackers and the prevention of hacking attacks. Chapter 5 examines the phenomenon of ‘malware’, or malicious software. The distinctions between hackers and virus writers are considered as are the differing approaches to dealing with these distinct problems.

The third section discusses crimes that can occur without computers, but have become more prevalent or easier because of technology – crimes such as music, video and software piracy, child pornography and paedophilia, terrorism, identity theft and fraud. These chapters include a section identifying the similarities and differences between online and offline offenders in these categories. Chapter 6 deals with one of the most commonly experienced types of cybercrime; identity theft and fraud. Common types of online identity theft and fraud are examined as are the reasons why systems and individuals find themselves vulnerable to such attacks. Internet child pornography is considered in Chapter 7. This difficult and sensitive topic is gaining greater attention from society and the media, as parents and caregivers become more aware of the risks to their children and law enforcement agencies become more aware of the techniques and strategies used by offenders. Chapter 8 continues with the related area of child predation on the internet. The psychology of child predators is considered, including an overview of some of the main theories of paedophilic behaviour and an overview of the risk factors of online predation. Chapter 9 looks at cyberbullying and cyberstalking. Case studies are provided, along with definitions of both activities. Prevalence rates of the phenomena are provided, as are descriptions of some of the techniques used during cyberbullying and cyberstalking attacks. Chapter 10 deals with piracy, illegal file sharing and copyright infringement. Consideration is given to the whether those involved in piracy and online copyright infringement activities see themselves as criminals, as well as examining how offenders justify their actions and how they can be dissuaded from such acts. Chapter 11 deals with the subject of cyberterrorism. This is a subject that has gained considerable interest from both researchers and media. The psychology of terrorism is examined, including investigations of the personalities and psychiatric health of terrorists, and it will be examined as to whether or not the findings relating to ‘traditional’ terrorists can also be applied to online terrorist activity.

The final section of the book considers crimes that take place within virtual worlds, such as the theft of virtual property, or an assault on a person’s avatar. These chapters question the nature of these offences, and the suitability of ‘real-life’ punishments for online offences. Chapter 12 deals with crimes that occur in online virtual worlds. Several cases are described and an attempt made to establish if these ‘virtual crimes’ could or should be considered criminal events. The effects of the crimes on the victims will also be considered, and the necessity for policing virtual worlds will be discussed. Chapter 13 attempts to look at how governments and law makers are dealing with the question of cybercrime. As technology
provides new ways for us to interact as citizens as well as consumers how will technology transform service delivery, governance and civic participation. If citizens as well as criminals are moving online how will the institutions of government move online?

SECTION 1: INTRODUCTION

This introductory section provides the reader with a foundational review of the key disciplines involved in the study of the psychology of cybercrime. These include definitions of cybercrime, descriptions of the discipline of forensic psychology and explanations of theories of crime as they relate to cybercrime.

Chapter 1: Creating the Ground Rules: How can Cybercrimes be Defined and Governed?

The objective of this chapter is to set the scene for remainder of the book. The core of the Psychology of Cybercrime seeks to address both the theory of crime and the question of forensic psychology’s contribution to the understanding of cybercrime. Specific examples of online crime such as hacking, malware, identity theft, child pornography and cyberbullying are dealt with in some detail in later chapters. This chapter seeks to first define the nature of online crime or cybercrime and look at the ways in which society is responding to it. The nature of the response is multi-faceted. Governments attempt to respond with law, corporations with policies and procedures, suppliers with terms and conditions, users with peer pressure, technologists with code. The chapter then looks at how international laws have evolved through what are referred to a ‘soft law’ and seeks to draw lessons for the evolution of laws for the internet. The question of how ideas of governance have evolved and how some of the theoretical work in this field may offer guidance for the governance of the internet is also considered.

Chapter 2: Can Forensic Psychology Contribute to Solving the Problem of Cybercrime?

This chapter considers if forensic psychology can aid in the detection, prevention and governance of online crimes. Forensic psychology to date has generally focused on violent, sexual and juvenile offences, but most of its theory and practice can also be applied to other offences, such as cybercrime. Chapter Two aims to investigate if forensic psychology can be useful in solving the problem of cybercrime, and briefly considers to what extent it has been applied to these crimes so far. Definitions of forensic psychology are discussed, and the primary responsibilities and activities of forensic psychologists are described. How each of these responsibilities and activities may be applied to cybercrime cases is examined and a determination made as to what extent forensic psychology has been involved in cybercrime cases to date. Suggestions are made for how to promote the benefits of forensic psychology in cybercrime cases, and finally proposals for future research and potential trends are discussed.

Chapter 3: Can Theories of Crime be Applied to Cybercriminal Acts?

Theories of crime are an important part of criminological literature. Different theories address the issue of crime at various levels, ranging from societal, through community and socialisation influence theories,
to the most specific level, individual theories. The aim of most of the theories of crime is to explain why crime occurs and who is most likely to engage in criminal acts, and as such they are an important element of developing a thorough understanding of the psychology of cybercrime. Many of the high level theories of crime are mainly sociological, geographical or political in scope, whereas theories of crime that consider socialisation and individual differences are those which are most suited to psychological discussion. While it must be remembered that there has been little empirical examination of how these theories specifically relate to cybercrime, some theories show potential for explaining the nature of the phenomenon. This chapter aims to determine which theories are most suitable for further investigation and applicability to cybercriminal cases.

SECTION 2: INTERNET-SPECIFIC CRIMES

This section identifies internet specific crimes, or offences that could not exist without the use of computers. These include hacking and malware development.

Chapter 4: Is the Research to Date on Hackers Sufficient to Gain a Complete Understanding of the Psychology Involved?

This chapter aims to determine if we have discovered all that we need to about the psychology and motivations of hackers. Hackers are the cybercriminals who have engaged the imagination of the general public the most. They are also those who have elicited the greatest quantity of psychological academic literature. Despite the vast quantities of literature in this area, it seems that we still do not have a thorough grasp on the mentality of the hacker. The chapter commences with some background information regarding the methods used by hackers, a description of the history of hacking behaviour and terminology, and the legal dimensions of hacking. The chapter goes on to consider the very diverse motives of hackers, as determined by psychological and criminological research. The personalities of computer hackers are examined, with special consideration of how psychological profiling could be used to help in hacking cases. Issues regarding punishment and prevention of hacking attacks are examined, finally the difficulties in carrying out hacker research and potential directions for future research in this area is explored.

Chapter 5: Malware: Can Virus Writers be Psychologically Profiled?

Most computer users are likely to have some exposure to malicious software or malware. This can take the form of spyware, computer viruses, worms or Trojan horses. This chapter looks at how malware developers, and in particular virus writers, can be psychologically profiled. The chapter clarifies the distinctions between different types of malware, and provides a brief history of some of the most famous malware programs which have been developed. Malware producers and hackers are not necessarily the same individuals, although some individuals engage in both behaviours and the terms are sometimes used interchangeably in the media. Malware is prolific, and the known prevalence rates for infection, as well as the quantity of known malware programs are identified. A brief overview of how malware applications are developed and distributed is considered, in light of the use of social psychology in encouraging individuals to download and distribute the programs. Some tentative explanations for the motives of virus writers are put forward, similarities with the psychology of vandalism are explored, in
order to determine if similar theories might explain both phenomena. The chapter also explores methods of reducing and preventing damage done by malware, and the psychological mechanisms that can predict if a computer user is likely to engage in safe online behaviour.

SECTION 3: ONLINE VARIATIONS OF OFFLINE CRIMES

The third section of the book discusses crimes that can occur without computers, but have become more prevalent or easier because of technology. There are several examples of this, including copyright infringement, identity theft, fraud, terrorism, child pornography and the use of the Internet to groom children by sexual predators. This section also examines cyberbullying and cyberstalking, which are considered to be criminal offences by some jurisdictions, or which may include elements of criminal activity, such as threats of physical violence.

Chapter 6: Identity Theft and Online Fraud: What Makes us Vulnerable to Scam Artists Online?

Most individuals have received an email involving some kind of attempt at getting them to part with their money. This chapter describes some of the common types of identity theft and fraud which can occur online, as well as attempting to determine what makes us vulnerable to such attacks. To do this, the chapter examines some aspects of human decision making, as well as identifying the social engineering tactics used by prospective fraudsters. The chapter describes the known prevalence rates and costs of online identity theft and fraud, and compares these types of offences to offline fraud schemes. The methods of attack are described, including phishing, keyloggers, social engineering, advance fee frauds, and other techniques. The psychology of the identity thief and fraudster is examined, based on comparisons to similar offline offenders. The effects on the victim are also considered, including the phenomenon of victim blaming, where others place partial blame on the victim for the criminal event. Possible methods of preventing identity theft and online fraud are considered, along with potential future trends and research.

Chapter 7: Internet Child Pornography: A Stepping Stone to Contact Offences?

Child pornography is a topic which is getting greater attention from society and the media, as parents and caregivers become more aware of the risks to their children and law enforcement agencies become more aware of the techniques and strategies used by offenders. The distribution of child pornography is not a new offence, but rather one which has been facilitated by the introduction of new technologies such as digital photography and the internet. Before the popularity of the internet, public concern and academic interest in child pornography was quite low as it was considered to be a small and specialist issue. However, the proliferation of images of child sexual abuse online has altered public opinion considerably. This chapter considers how online distribution of child pornography is different to offline distribution. It also considers the psychology of the online child pornography offender and considers the difference between these individuals and contact offenders, attempting to determine if online offenders later progress to offend offline as well.
Chapter 8: Online Child Predators: Does Internet Society make Predation Easy?

The internet seems to provide an easier route for child predators to encounter and engage with children and teenagers. This chapter addresses the question of how the internet may facilitate this process. Initially paedophilia is defined, and problems with its diagnosis considered. An attempt is made to quantify the problem of online child predation, and the techniques used by online child predators are described. The psychology of child predators is considered, including an overview of some of the main theories of paedophilic behaviour. The psychology of victims is also considered, with an overview of the risk factors of online predation, along with the psychological effects on victims. Potential solutions are reviewed, including rehabilitation efforts and prevention methods.

Chapter 9: Cyberbullying and Cyberstalking: Are They as Serious as Their Offline Counterparts?

Two of the most personal forms of online attack are cyberbullying and cyberstalking. While this activity is not always considered criminal, some jurisdictions treat cyberbullying acts as offences. This is especially the case when they include direct threats or physical assault. Cyberstalking may also be included in the stalking laws of many jurisdictions. This chapter examines cyberbullying and cyberstalking and questions if they are as severe as their offline counterparts, particularly from a psychological perspective. Case studies of both cyberbullying and cyberstalking are provided, along with definitions of both activities. Known prevalence rates of the phenomena are provided, although as with most types of criminal events, the true prevalence rates of these activities is unknown. Descriptions are provided of some of the techniques used during cyberbullying and cyberstalking attacks, and differences between online and traditional stalking and bullying are considered. The demographic and psychological traits of cyberstalkers and cyberbullies are described, along with the traits of their victims, and the psychological effects of victimisation. Possible solutions for these problems are considered, including both preventative measures and suitable responses. Finally, potential future trends in the area are considered, including the possible use of online gaming and social networking sites for harassment, as well as the underexamined phenomenon of workplace cyberbullying.

Chapter 10: Music, Video and Software Piracy: Do Offenders See Them as Criminal Activities?

Chapter 10 considers the issue of piracy, illegal file sharing and other types of copyright infringement and if those involved in piracy and online copyright infringement activities see themselves as criminals. It also examines how such offenders justify their actions and how they can be dissuaded from such acts. Definitions of key terms in the area are presented, along with some examples of real events relating to illegal file sharing. A description of some of the methods used during illegal file sharing and piracy are provided, along with a historical view of how copyright infringement has developed over time. The known current prevalence rates and costs of offending, and the arguments presented from industry and academia regarding the effects of file sharing on legitimate sales are considered. Similarly, the problem of trying to estimate the true cost of piracy and illegal file sharing is highlighted. The psychology of offenders is considered, and in particular, the phenomenon of the lack of insight of offenders into their own
criminality will be investigated. In particular, the roles of self-control, social learning and justifications in illegal file sharing are analysed. Some potential solutions for these crimes are considered, including the determination of appropriate punishments and the development of suitable educational campaigns.

Chapter 11: Cyberterrorism: Can Terrorist Goals be Achieved using the Internet?

Cyberterrorism has gained considerable interest from both researchers and media, in particular since the attacks on the United States of America on September 11th 2001. Nevertheless, there is a considerable lack of empirical research in the area, with most writings based on theoretical or anecdotal accounts, despite many calls by leaders in the field for more empirically sound methods. This is further complicated by the difficulty in even finding consensus as to what does and does not constitute cyberterrorism. This chapter aims to determine if cyberterrorism is a likely strategy to be used by terrorists, and if so, how it might be used to strike terror into the hearts of citizens. Following some illustrative scenarios of terrorist activity online, some of the conflicting definitions of the subject are considered. The methods used by terrorists online will be outlined, including both an examination of the possibility of using the internet for a large scale attack, and using the internet for more conventional activities such as recruitment and fundraising. The psychology of terrorism is examined, including investigations of the personalities and psychiatric health of terrorists, and it will be examined as to whether or not the findings relating to ‘traditional’ terrorists can also be applied to online terrorist activity. The potential effects of an attack on victims is also considered as is how terrorist activity online can be prevented.

SECTION 4: CRIMES IN VIRTUAL WORLDS

This final section of the book considers crimes that take place within virtual worlds. While not necessarily considered criminal events in the offline world, these ‘crimes’ can still have very serious consequences for the individuals involved.

Chapter 12: Crime in Virtual Worlds: Should Victims Feel Distressed?

The final type of cybercrime to be considered involves crimes that occur in online virtual worlds. While there is considerable literature available on other cybercrimes, as outlined in the previous chapters of this book, relatively little academic literature has been published concerning crime in online virtual worlds. Several cases have come to light concerning specific crimes in these environments, including both property offences (such as theft) and crimes against the person (such as sexual assault). It should be noted that while the term ‘crime’ is used in this chapter to describe these events, they may not necessarily be illegal or criminal events, at least so far as the offline world would consider them to be. This chapter describes these types of virtual crimes, and determines if they could and should be considered criminal events. The effect of the crimes on the victims is also considered, and the necessity for policing virtual worlds discussed. In addition, the online community needs to consider how to deal with virtual offenders – if their offence has real-world consequences, should they be punished offline, or only in the virtual world?
Chapter 13: On-Line Governance

Power is dissipating from traditional government; upwards to supranational institutions and downwards to sub national agencies. Governments are also losing influence with their citizens as power is lost to interest groups, influential individuals and media organizations. Citizens are disengaging with the political process as they perceive their ability to effect change is diminishing. As individuals spend more time online, form relationships and interest groups in virtual worlds, the polis is becoming virtual. This chapter looks at how technology, which has already begun to transform service delivery in the public sector, can also transform consultation and participation. If power and influence has been dissipated from the government, can it be regained by finding new ways to engage online with the citizens on whose behalf it exists to serve?

CONCLUSION

The objective of this book has been to draw together on one place the recent psychological thinking and research on a range of crimes and antisocial behaviours which are becoming more common in our increasingly interconnected lives. There is a case to be made that the very suffix of cyber has been outgrown by the degree to which humanity has been wired. When we made a conscious decision to ‘go online’ or to ‘log in’ to our online lives it made sense to distinguish between the ‘world’ and the ‘cyberworld’ between ‘crime’ and ‘cybercrime’, between ‘laws’ and ‘cyberlaws’. The day is surely coming when such distinctions are no longer useful and we have simply integrated into every aspect of our lives a degree of interconnectedness, group work, or networking. As the technology becomes ubiquitous in our lives and social networking assumes no more novelty than water cooler conversation the use of the prefix cyber will seem quaint.

Until cyber assumes the status of, fax, telegraph, or computer room, it remains a useful way to hold up our online behaviours to the norms and learning of a decade or more of study into the disciplines of psychology, forensics, sociology and law and ask is this different. Do we need new approaches or can we adapt our knowledge to fit this new medium. This book seeks to take the knowledge established in an offline world and measure it for fit against the needs of the online world and offer suggestions where the fit is not exact. Much cybercrime is committed for much the same motives and by much the same people as have always been tempted to criminal activity, although there are some exceptions. Many of the differences relate to the opportunity, access, impact, and range of activities that can be engaged in, although factors such as the anonymity and disinhibition that the Internet affords are also important psychological differences. Psychological study has much to offer in the study of cybercrime, as is evident in the following chapters, and it is important that these insights are evaluated and employed as useful weapons in developing anti-cybercrime strategies.

REFERENCES


**ADDITIONAL READING**

