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

ABSTRACT

The objective of this chapter is to set the scene for the remainder of the book. The core of this book 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. Before exploring these subjects it is necessary to set out some context.

The first section of this chapter seeks to 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 second section looks at how international laws have evolved through what are referred to as 'soft law' and seeks to draw lessons for the evolution of laws for the internet. The final section looks at the more general area of governance and also looks at 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.

BACKGROUND

Definitions

Online crime takes many forms and a distinction should be made between activities such as; the theft of goods online which is clearly a crime, private law issues such as disputes between buyers and sellers of online goods, and issues of anti social behavior or harassment. Certain activities, such as spamming, hacking and cracking can, depending on severity, target and context, fit into any one of the three categories listed.

The variety of activities and intents has meant that the term cybercrime has come to encompass a range of activities and has not yet achieved a single agreed definition. Definitions include, "*crime committed using a computer and the internet to*

DOI: 10.4018/978-1-61350-350-8.ch001

steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs", which is used by Princeton University (n.d.). It has also been defined in the New World Encyclopedia (n.d.) as *"a term used broadly to describe activity in which computers or computer networks are the tool, target, or place of criminal activity. Cybercrime takes a number of forms including identity theft, internet fraud, violation of copyright laws through file sharing, hacking, computer viruses, denial of service attacks, and spam"*. The IT security company Symantec (n.d.) defines two categories of cybercrime, *"Type I, examples of this type of cybercrime include but are not limited to phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud. Type II cybercrime includes, but is not limited to activities such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities"*. More succinct definitions include, "*crimes perpetrated over the internet, typically having to do with online fraud"* (PC Mag Encyclopedia, n.d.) or *"crime committed using the Internet, for example stealing someone's personal information or introducing harmful programs into someone's computer"*. (Macmillan Dictionary, n.d.)

Some of these definitions are clearly more specific than others and thus more useful in the framing of any legal position on the subject. However the more common understanding of cybercrime as being any activity occurring online which has intended negative consequences for others is more suitable to our purpose of an exploration of the field. This chapter takes a broad definition of the term cybercrime and assumes it to cover a wide range of activities which may vary from those which are clearly breaches of criminal law to those which could more accurately be described as private law issues. Types of crime can be categorized as internet enabled crimes, internet specific crimes and new crimes committed in a virtual world.

Types of Crime

Technology and crime have a long association, each advance in technology that provides an opportunity to be exploited for gain is matched by advances in the technology of detection. The Internet simply provides a new medium. Two categories of online crime have been observed for many years and a third, with the advent of online virtual environments, is a more recent development. The first category is composed of those crimes which existed offline but are now greatly facilitated by the Internet. These include misuse of credit cards, information theft, defamation, blackmail, obscenity, hate sites, money laundering, and copyright infringement. In the main, comprehensive national laws exist to deal with these issues in offline environments. With the exception of the cross border nature of the online version of these activities enabled by the internet existing legal frameworks are capable of dealing with them.

The second category is made up of crimes that had not existed before the arrival of networked computing and more specifically the proliferation of the internet. These include, hacking, cyber vandalism, dissemination of viruses, denial of service attacks, and domain name hijacking. National laws have been introduced in many jurisdictions in an attempt to combat these crimes (for example, an overview of the UK law in this area is available at JISC Legal www.jisclegal.ac.uk).

A third category comes into play when individuals are acting through their online avatars (representations of the user in the form of a three-dimensional model, from the Sanskrit 'avatara' meaning incarnation) or alternate personas. Do these individuals or their avatars constitute a new public, and present new issues of governance, both in cyberspace and of cyberspace? Harassing another individual through their online representation may be criminal or at the very least antisocial. There is, however, no doubt that these activities have lead to very real crimes offline.