PART I

Introduction

1

Cybercrime

1. The evolution of cybercrime

> It is known of all men that the radical change in transportation of persons and goods effected by the introduction of the automobile, the speed with which it moves, and the ease with which evil-minded persons can avoid capture, have greatly encouraged and increased crimes.[1]

What could be said of the automobile in the 1920s is equally apposite of digital technology today. It is trite, but nonetheless true, to say that we live in a digital age. The proliferation of digital technology, and the convergence of computing and communication devices, has transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to these developments. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes.

The magic of digital cameras and sharing photos on the Internet is exploited by child pornographers. The convenience of electronic banking and online sales provides fertile ground for fraud. Electronic communication such as email and SMS may be used to stalk and harass. The ease with which digital media may be shared has led to an explosion in copyright infringement. Our increasing dependence on computers and digital networks makes the technology itself a tempting target; either for the gaining of information or as a means of causing disruption and damage.

The idea of a separate category of 'computer crime' arose at about the same time that computers became more mainstream. As early as the 1960s there were reports of computer manipulation, computer sabotage,

1 *Brooks* v. *US*, 267 US 432, 438–9 (1925).

computer espionage and the illegal use of computer systems.[2] While the 1970s saw the first serious treatments of 'computer crime',[3] the relatively limited role of computers in daily life meant that such offences typically related to theft of telecommunication services and fraudulent transfer of electronic funds.[4] In subsequent decades, the increasing networking of computers and the proliferation of personal computers transformed computer crime and saw the introduction of specific computer crime laws.

The evolution of such legislation followed successive waves, reflecting changing concerns surrounding the misuse of computers.[5] Initial concerns which related to unauthorised access to private information expanded into concern that computers could also be used for economic crimes. As computers became more and more central, the concern was to protect against unauthorised access to computer data per se. Increasing connectivity not only magnified these concerns; it gave rise to new problems, such as remote attacks on computers and networks, and gave new life to old offences such as infringement of copyright, the distribution of child pornography and global fraudulent schemes.

Rapid technological development continues, and will continue, to present new challenges. The increasing uptake of broadband allows many home users to leave their computers connected to the Internet, thus making them more vulnerable to external attack.[6] Peer-to-peer technology may not only be used to transfer illegal content, but also to orchestrate Denial of Service ('DoS') attacks and disseminate malware.[7] The convergence of telecommunications and computing has transformed mobile phones into miniature networked computers, with attendant potential for criminality.

2 U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, COMCRIME Study, European Commission (1998), p. 19.
3 See, e.g., G. McKnight, *Computer Crime* (London: Joseph, 1973) and D. B. Parker, *Crime by Computer* (New York: Scribner, 1976).
4 M. D. Goodman and S. W. Brenner, 'The emerging consensus on criminal conduct in cyberspace' (2002) *UCLA Journal of Law and Technology* 3, 12.
5 Sieber, *Legal Aspects of Computer-Related Crime*, pp. 25–32, 39.
6 S. Morris, *The Future of Netcrime Now: Part 1 – threats and challenges*, Home Office Online Report 62/04 (2004), p. 20.
7 *Ibid.*, p. 21. The nature of this technology is discussed at p. 222.

2. The challenges of cybercrime

> [W]e live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology.[8]

It has been said that there are three factors necessary for the commission of crime: a supply of motivated offenders, the availability of suitable opportunities and the absence of capable guardians.[9] On all three counts, the digital environment provides fertile ground for offending. While specific impacts will be discussed in subsequent chapters, it is useful to summarise briefly some of the key features of digital technology which facilitate crime and hamper law enforcement.

A. Scale

Unlike more traditional forms of communication, the Internet allows users to communicate with many people, cheaply and easily. The estimated 1.6 billion people on the Internet, approximately 24 per cent of the world's population,[10] provide an unprecedented pool of potential offenders and victims. This acts as a 'force multiplier', allowing offending to be committed on a scale that could not be achieved in the offline environment.[11] The ability to automate certain processes further amplifies this effect.

B. Accessibility

Not so long ago, computers were large, cumbersome devices utilised primarily by government, research and financial institutions. The ability to commit computer crimes was largely limited to those with access and expertise. Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims.

8 Dr Carl Sagan, cited in *In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Trap & Trace Device on E-Mail Account*, 416 F Supp 2d 13, 14 (D DC 2006).
9 L. Cohen and M. Felson, 'Social change and crime rate trends: A routine activity approach' (1979) 44 *American Sociological Review* 588, 589.
10 Internet World Stats, *Internet Usage Statistics: The Internet big picture – world Internet users and population stats* (2009), www.internetworldstats.com/stats.htm.
11 Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, *Chapter 4: Damage and Computer Offences, Final Report* (2001), p. 95.

In 2007–8, 67% of Australians had access to a computer at home,[12] while in 2006, 70% had used the Internet[13] and 82% a mobile phone.[14] In 2003, 64% of Canadian households had at least one member who used the Internet regularly[15] and in 2006, 67% of households reported having a mobile phone.[16] In 2003, 75% of adults in the UK had a mobile phone,[17] while in 2007 61% of households could access the Internet from home.[18] In the United States, the percentage of households with computers rose from 8.2% in 1984 to 61.8% in 2003,[19] while those with access to the Internet increased from 18% in 1997 to 54.7% in 2003.[20] The ubiquitous 'Internet café' also provides a ready source of connectivity.

For those activities that may be beyond the skills of the individual, the Internet provides easy access to those who will do it for you, or tell you how. Offenders who might otherwise be isolated in their offending, can now find like minds, forming virtual communities to further their offending.[21]

C. Anonymity

Anonymity is an obvious advantage for an offender, and digital technology facilitates this in a number of ways. Offenders may deliberately conceal their identity online by the use of proxy servers, spoofed email or IP addresses or anonymous emailers. Simply opening an email account which does not require identity verification provides a false identity. Confidentiality may be protected by the use of readily available encryption technology, while traces of digital evidence may be removed using commercially available software.

12 Australian Bureau of Statistics, *Household Use of Information Technology, Australia 2007–08*, Cat. no. 8146.0 (2008).
13 Australian Government, Department of Broadband, Communications and the Digital Economy, *Online Statistics* (2008), www.archive.dbcde.gov.au/2008/01/statistical_benchmarking/online_statistics.
14 *Ibid.*
15 Statistics Canada, *Household Internet Use Survey-Microdata User's Guide 2003*, Cat. no. 56M0002GIE (2004), p. 7.
16 Statistics Canada, *Residential Telephone Service Survey*, The Daily (2007), www.statcan.gc.ca/daily-quotidien/070504/dq070504a-eng.htm.
17 National Statistics, *Adult Mobile Phone Ownership or Use: By age, 2001 and 2003*, Social Trends 34 (2009), www.statistics.gov.uk/STATBASE/ssdataset.asp?vlnk=7202.
18 National Statistics, *First Release: Internet access 2007: Households and individuals* (2007), p. 1, www.statistics.gov.uk/pdfdir/inta0807.pdf.
19 US Census Bureau, *Computer and Internet Use in the United States 2003* (2005), p. 1, www.census.gov/prod/2005pubs/p23–208.pdf.
20 *Ibid.* 21 Morris, *The Future of Netcrime*, p. 18.

The networked nature of modern communications in itself means that data will routinely be routed through a number of jurisdictions before reaching its destination, making tracing of communications extremely difficult and time sensitive. Accessing wireless networks, with or without authorisation, may conceal the identity of the actual user even if the location can be identified. Data may be stored deliberately in jurisdictions where regulation and oversight is lax.

D. Portability and transferability

Central to the power of digital technology is the ability to store enormous amounts of data in a small space, and to replicate that data with no appreciable diminution of quality. Storage and processing power which would once have occupied rooms, will now fit into a pocket. Copies of images or sound may be transmitted simply and at negligible cost to potentially millions of recipients. The convergence of computing and communication technologies has made this process a seamless one, with the ability to take a digital image with a mobile phone and then upload it to a website within seconds.

E. Global reach

Criminal law is traditionally regarded as local in nature, being restricted to the territorial jurisdiction in which the offence occurred. Modern computer networks have challenged that paradigm. As individuals may now communicate overseas as easily as next door, offenders may be present, and cause harm, anywhere there is an Internet connection. Whether it be a fraudulent scheme, a DoS attack or the distribution of child pornography, there is no need for offenders and victims to be in the same jurisdiction. Not only does this provide, literally, a world of opportunity for offenders, it presents enormous challenges to law enforcement and harmonisation.

F. Absence of capable guardians

An important factor which may affect offending behaviour is the perceived risk of detection and prosecution. In this respect, digital technology presents law enforcement with a range of challenges. The volatile nature of electronic data requires sophisticated forensic techniques to ensure its retrieval, preservation and validity for use in a criminal trial. Apart from the sheer volume of users, the networked nature of modern

communications makes surveillance extremely difficult. Much of the infrastructure is privately owned, meaning that law enforcement agencies must deal with a number of different entities. Communications will routinely be routed through multiple jurisdictions, necessitating the assistance of local law enforcement agencies. Even if the assistance of local authorities can be obtained, data retention may be limited or non-existent. If the defendant is present in another jurisdiction, can he or she be extradited? The complexity and cost of such investigations necessarily means they will not be undertaken lightly.

As in the offline environment, it is neither practical nor desirable that police be everywhere. The role of 'guardian' must be shared with others across the community, whether it be parents monitoring their children's use of the Internet, financial institutions looking for suspicious transactions or system administrators detecting network intrusions. All play an important guardianship role, as do industry groups and government regulators. ISPs are particularly significant, being effectively the gatekeepers of data on the Internet.

Effective regulation requires a broad range of responses, addressing the four modalities of constraint identified by Lessig: the law, architecture, social norms and the market.[22] The focus of this book is on one component of the regulatory mix, namely the application of the substantive criminal law to the digital environment. Such 'tertiary crime prevention' operates not only through deterrence and incapacitation, but also influences social norms as to what is, and what is not, acceptable behaviour in the online environment.[23]

3. Defining cybercrime

> The range of technology-enabled crime is always evolving, both as a function of technological change and in terms of social interaction with new technologies.[24]

22 L. Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), pp. 85–99. See generally, N. K. Katyal, 'Criminal law in cyberspace' (2001) 149 *University of Pennsylania Law Review* 1003; O. S. Kerr, 'Virtual crime, virtual deterrence: A skeptical view of self help, architecture and civil liability' (2005) *Journal of Law, Economics and Policy* 197; S. W. Brenner, 'Toward a criminal law for cyberspace: Distributed security' (2004) 10 *Buffalo Journal of Science and Technology* 1; and M. E. O'Neill, 'Old crimes in new bottles: Sanctioning cybercrime' (2000) 9 *George Mason Law Review* 237.

23 R. G. Smith, P. Grabosky and G. Urbas, *Cyber Criminals on Trial* (Cambridge: Cambridge University Press, 2004), p. 2.

24 G. Urbas and K. R. Choo, *Resource Materials on Technology-Enabled Crime*, Technical and Background Paper no. 28 (AIC, 2008), p. 5.

There are almost as many terms to describe cybercrime as there are cybercrimes. Early descriptions included 'computer crime', 'computer-related crime' or 'crime by computer'.[25] As digital technology became more pervasive, terms such as 'high-technology' or 'information-age' crime were added to the lexicon.[26] The advent of the Internet brought us 'cybercrime' and 'Internet' or 'net' crime.[27] Other variants include 'digital', 'electronic' (or 'e-'), 'virtual', 'IT', 'high-tech' and 'technology-enabled' crime.

If taken literally, each term suffers from one or more deficiencies. Those definitions that focus on 'computers' may not incorporate networks. Others such as 'cybercrime' or 'virtual crime' may be seen as focusing exclusively on the Internet.[28] Terms such as 'digital', 'electronic' or 'high-tech' crime may be seen as so broad as to be meaningless. For example, 'hi-tech crime' may go beyond networked information technology to include other 'hi-tech' developments such as nanotechnology and bioengineering.[29]

Such terms should not, however, be approached literally, but rather as broadly descriptive terms which emphasise the role of technology in the commission of crime. Although it is still the case that no one term has become truly pervasive, with many being used interchangeably, 'cybercrime' has been adopted in this book for a number of reasons. First, it is commonly used in the literature.[30] Secondly, it has found its way into common usage.[31] Thirdly, it emphasises the importance of networked computers.[32] Fourthly, and most importantly, it is the term adopted in the Council of Europe Convention on Cybercrime.[33]

25 House Of Commons Standing Committee On Justice And Legal Affairs, *Computer Crime*, Final Report (1983), p. 12; Sieber, *Legal Aspects of Computer-Related Crime* and Parker, *Crime by Computer*.

26 S. W. Brenner, 'Cybercrime metrics: Old wine, new bottles?' (2004) 9 *Virginia Journal of Law and Technology* 1, n. 4.

27 Morris, *The Future of Netcrime*, p. vi.

28 According to the *Oxford English Dictionary*, in later usage the prefix 'cyber' has come to be used to form terms relating to the Internet.

29 Morris, *The Future of Netcrime*, p. vi.

30 It also (rarely) appears in legislation; see, e.g., the Cybercrime Act 2001 (Cth).

31 The *Oxford English Dictionary* defines 'cybercrime' as 'crime or a crime committed using computers or the Internet'.

32 Although the term 'cyber' is technically limited to crimes involving the Internet, it is used more broadly to refer to crimes committed using stand-alone computers; P. Grabosky, *Electronic Crime* (New Jersey: Pearson Prentice Hall, 2007), p. 2.

33 See p. 21.

For all the variations in terminology, there is now a broad consensus as to what these terms encompass. This involves a three-stage classification, as summarised by the US Department of Justice:

1. Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DoS attacks.
2. Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement and fraud.
3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the computer of a murder suspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more a repository for evidence.[34]

We therefore see a tripartite classification of computer crimes, computer-facilitated crimes and computer-supported crimes.[35] This form of classification, or a variant of it, has also been used in Australia,[36] Canada,[37] the UK,[38] and at an international level.[39] Our focus is on the first two categories of cybercrime, with computer-supported crimes raising issues of procedural and evidentiary law which are beyond the scope of this book.[40]

This classification also addresses the question of whether cybercrime is an entirely new form of offending, with no analogues in the offline environment, or whether it is simply old crimes committed in new ways.[41] The answer is both. The majority of cybercrimes discussed in this book

34 Computer Crime and Intellectual Property Section, US Department of Justice, *The National Information Infrastructure Protection Act of 1996*, Legislative Analysis (1996), www.cybercrime.gov/1030analysis.html.

35 This latter term is adopted in Canada: M. Kowalski, *Cyber-Crime: Issues, data sources, and feasibility of collecting police-reported statistics*, Cat. no. 85–558, Canadian Centre for Justice Statistics (2002), p. 6.

36 Urbas and Choo, *Technology-Enabled Crime, p.* 5. 37 Kowalski, *Cyber-Crime*, p. 6.

38 National Criminal Intelligence Service, *Project Trawler: Crime on the information highways* (1999), www.cyber-rights.org/documents/trawler.htm; and Morris, *The Future of Netcrime*, p. 3.

39 A. Rathmell et al., *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*, Study for the European Commission Directorate-General Information Society (2002), p. 16.

40 See Smith, Grabosky and Urbas, *Cyber Criminals on Trial*; Computer Crime and Intellectual Property Section, US Department of Justice, *Manual on Prosecuting Computer Crime* (2007), www.cybercrime.gov/ccmanual/01ccma.pdf.

41 Brenner, 'Cybercrime metrics', 15.

are existing offences committed in new ways. The true 'cybercrimes', in the sense of offences that would not exist at all without computing, are those against computers and computer networks themselves.

4. Cyberterrorism

> Without a great deal of thought about security, the Nation shifted the control of essential processes in manufacturing, utilities, banking, and communications to networked computers.[42]

Reliance on digital technology, particularly networked communications, has now become so pervasive that it is regarded as part of the critical infrastructure.[43] Consequently, another motivation for attacks on computer networks is to further a political, religious or ideological cause – so-called 'cyberterrorism'. Such attacks have the potential to cause considerable harm, possibly disrupting essential services such as water, power, hospitals, financial systems, emergency services, air/shipping control and the like.

Although, to date, the threat has been more potential than real, studies suggest that there has been an increase in the number of cyber-attacks against critical infrastructure, including Supervisory Control And Data Acquisition systems (SCADA), namely computer systems which are relied upon to automatically monitor and adjust critical infrastructure.[44] Attacks against networked infrastructure may also be used to 'leverage' physical attacks, for example by hampering the ability of emergency services to respond.[45] It is therefore important to clarify what is meant by this emotive and imprecise term.

Given differing views on the meaning of 'terrorism', it is not surprising that the term 'cyberterrorism' is ill-defined.[46] It may, however, broadly

42 The White House, *The National Strategy to Secure Cyberspace* (2003), p. 5, www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

43 See for example, Organisation for Economic Co-Operation and Development, *OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security* (OECD, 2002); Parliamentary Joint Committee on the Australian Crime Commission, *Cybercrime* (Parliament of the Commonwealth of Australia, 2004), Ch 5.

44 C. Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and policy issues for Congress*, Congressional Research Service Report for Congress, (Congressional Research Service, 2005), pp. 8–10.

45 The White House, *The National Strategy to Secure Cyberspace*, p. 7.

46 S. Keith, 'Fear-mongering or fact: The construction of "cyber-terrorism" in US, UK, and Canadian news media', Paper presented at Safety and Security in a Networked World: Balancing cyber-rights and responsibilities, sponsored by the Oxford Internet Institute, Oxford, England, 8–10 September, 2005, pp. 1–2.