PART I

Introduction

1

Cybercrime

1. The evolution of cybercrime

> Technology . . . is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other.[1]

In October 2014, Estonian national Sergei Tšurikov was sentenced to eleven years in prison in the United States for his part in a conspiracy which resulted in the loss of over US$9.4 million.[2] The offences occurred during 2008 when Tšurikov and others were able to hack into the computer network of RBS WorldPay. In what authorities described as 'perhaps one of the most sophisticated and organized computer fraud attacks ever conducted', the offenders were able to compromise the data encryption used by RBS and raise the account limits on 'payroll debit cards'.[3] They then provided a network of 'cashers' with forty-four counterfeit payroll debit cards that, in under twelve hours, were used to withdraw 'more than $9 million from over 2,100 automatic teller machines (ATMs) in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada'.[4] Adding insult to injury, Tšurikov and another hacker were able to monitor the withdrawals in real time using RBS' computer systems.[5]

Although a highly sophisticated example, this case illustrates many of the features and challenges of modern cybercrimes; it was organised, financially motivated, technologically sophisticated and transnational. It was also made possible by the ubiquity of digital technology in modern life; technology that has transformed the way in which we socialise and do business. While overwhelmingly positive, there is also a dark side to this transformation. Proving the maxim that crime follows opportunity,

[1] C. P. Snow, quoted by A. Lewis, *New York Times*, 15 March 1971, p. 37.
[2] US Department of Justice, 'International hacker sentenced', Press Release (24 October 2014).
[3] *Ibid.* [4] *Ibid.* [5] *Ibid.*

virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes.

The magic of digital cameras and the sharing of photographs is exploited by child pornographers. The convenience of electronic banking and online sales provides fertile ground for fraud. Electronic communications and social networking sites 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, computer espionage and the illegal use of computer systems.[6] As the technology evolved, so too did the nature of the offending, giving rise to the three 'generations' of cybercrime identified by Wall; from cybercrimes facilitating traditional offences such as fraud, through crimes across networks such as hacking, to crimes that are 'wholly mediated' by technology such as botnets.[7] The motivations of offenders have also evolved, from 'curiosity and status-driven activities to those which are now predominantly financially motivated and occur in a much more organised and systemic manner'.[8]

While the 1970s saw the first serious treatments of 'computer crime',[9] 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.[10] 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.

[6] U. Sieber, *Legal aspects of computer-related crime in the information society*, COMCRIME Study (European Commission, 1998), p. 19.
[7] D. S. Wall, *Cybercrime: The transformation of crime in the information age* (Cambridge: Polity, 2007), pp. 44–8.
[8] R. G. Smith, 'The development of cybercrime', in R. Lincoln and S. Robinson (eds.), *Crime over time: Temporal perspectives on crime and punishment in Australia* (Newcastle upon Tyne: Cambridge Scholars Publishing, 2010), p. 214.
[9] See, e.g., G. McKnight, *Computer crime* (London: Joseph, 1973); D. B. Parker, *Crime by computer* (New York: Scribner, 1976).
[10] M. D. Goodman and S. W. Brenner, 'The emerging consensus on criminal conduct in cyberspace' (2002) *UCLA Journal of Law and Technology* 3, 12.

The evolution of such legislation followed successive waves, reflecting changing concerns surrounding the misuse of computers.[11] 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 users to leave their devices constantly connected to the internet, thus making them more vulnerable to external attack.[12] Peer-to-peer (p2p) technology may not only be used to transfer illegal content, but also to orchestrate denial of service (DoS) attacks and disseminate malware.[13] The convergence of telecommunications and computing has transformed mobile phones into miniature networked computers. Increasingly, we also see internet connectivity incorporated into more and more everyday items; the so-called 'internet of things'.[14]

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.[15]

According to 'routine activity theory', there are three factors necessary for the commission of predatory crime: a supply of motivated offenders; the availability of suitable opportunities and the absence of capable guardians.[16] Translating this theory to the online environment, we see that on all three

[11] Sieber, *Legal aspects of computer-related crime*, pp. 25–32, 39.
[12] S. Morris, *The future of netcrime now: Part 1 – threats and challenges*, Home Office Online Report 62/04 (Home Office, 2004), p. 20.
[13] *Ibid*., p. 21.
[14] International Telecommunication Union, *ITU internet reports 2005: the internet of things*, Report (2005).
[15] 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 at 14 (D DC. 2006).
[16] L. Cohen and M. Felson, 'Social change and crime rate trends: A routine activity approach' (1979) 44 *American Sociological Review* 588, 589.

counts it 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 that 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 3 billion people with access to the internet, approximately 40 per cent of the world's population,[17] 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.[18] The ability to automate certain processes further amplifies this effect. For example, the 'Bredolab' botnet was estimated to have infected 30 million computers at its peak, generating 3 billion emails per day.[19]

B. *Accessibility*

Only a few decades 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.

In 2012–13, just over 80 per cent of adults in Australia, Canada and the United Kingdom had accessed the internet, with more than half accessing from mobile phones or other handheld devices.[20] In the United States, the percentage of households with access to the internet increased from 18 per cent in 1997 to 74.4 per cent in 2013.[21] Although internet

[17] International Telecommunications Union, *ICT facts and figures: The world in 2014* (2014).

[18] Model Criminal Code Officers Committee of the Standing Committee of Attorneys General, *Chapter 4: damage and computer offences*, Final Report (2001), p. 95.

[19] Sophos, *Security threat report 2013* (2013), p. 27.

[20] Australian Bureau of Statistics, *Household use of information technology, Australia 2012–13*, Cat. No. 8146.0 (2014); Statistics Canada, *Individual internet use and e-commerce, 2012* (28 October 2013); Office for National Statistics (UK), *Statistical bulletin: internet access – households and individuals* (2013).

[21] T. File and C. Ryan, *Computer and internet use in the United States: 2013* (US Census Bureau, November 2014).

access is highest in developed countries, the actual number of internet users in developing countries far outnumbers that in developed countries.[22]

The uptake of mobile phones is now reaching saturation point in some developed countries. In Australia in 2012, for example, 92 per cent of the adult population used a mobile phone, 49 per cent of which were estimated to be smartphones.[23] The increase in smartphone and tablet use has led to a boom in software applications or 'apps' being downloaded; with Apple reporting that more than 25 billion apps had been downloaded from its 'App Store'.[24]

For those criminal 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. Online marketplaces provide everything from hacking techniques and botnets to financial and identity information. Offenders, who might otherwise be isolated in their offending, can now find like minds, anywhere in the world, forming virtual communities to further their offending.[25]

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 internet protocol (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.

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

[22] United Nations Office on Drugs and Crime, *Comprehensive study on cybercrime*, Report (2013), p. 1.

[23] Australian Communications and Media Authority, *Communications report 2011–12 series, Report 3 – Smartphones and tablets take-up and use in Australia* (2013), p. 22.

[24] Apple, *Apple press info: Apple's app store downloads top 25 billion*, Press Release (5 March 2012), www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html.

[25] Morris, *The future of netcrime*, p. 18.

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. In a recent UN study, over half of responding countries reported that 'between 50 and 100 per cent of cybercrime acts encountered by police involved a "transnational element"'.[26] 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 that 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

[26] United Nations Office on Drugs Crime, *Comprehensive study on cybercrime*, p. 55.

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.[27] 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.[28]

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.[29]

There are almost as many terms to describe cybercrime as there are cybercrimes. Early descriptions included 'computer crime', 'computer-related

[27] L. Lessig, *Code and other laws of cyberspace* (New York: Basic Books, 1999), pp. 85–99.
[28] R. G. Smith, P. Grabosky and G. Urbas, *Cyber criminals on trial* (Cambridge: Cambridge University Press, 2004), p. 2.
[29] G. Urbas and K. R. Choo, *Resource materials on technology-enabled crime*, Technical and Background Paper No. 28 (AIC, 2008), p. 5.

crime' or 'crime by computer'.[30] As digital technology became more pervasive, terms such as 'high technology' crime were added to the lexicon.[31] The advent of the internet brought us 'cybercrime' and 'internet' or 'net' crime.[32] 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. 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.[33]

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.[34] Secondly, it has found its way into common usage.[35] Thirdly, it emphasises the importance of networked computers. Fourthly, it is internationally recognised, being adopted by the UN,[36] and in the Council of Europe Convention on Cybercrime.

For all the variations in terminology, there is now a broad consensus as to what these terms encompass. The two principal categories of cybercrime are 'cyber-dependent' and 'cyber-enabled' crimes.[37]

[30] House of Commons Standing Committee on Justice and Legal Affairs, *Computer crime*, Final Report (1983), p. 12; Sieber, *Legal aspects of computer-related crime*; Parker, *Crime by computer*.
[31] S. W. Brenner, 'Cybercrime metrics: Old wine, new bottles?' (2004) 9 *Virginia Journal of Law and Technology* 1, n. 4.
[32] Morris, *The future of netcrime*, p. vi.
[33] Morris, *The future of netcrime*, p. vi. See, e.g., S. W. Brenner, 'Nanocrime?' (2011) *University of Illinois Journal of Law, Technology and Policy* 39.
[34] It also (rarely) appears in legislation: see, e.g., the Cybercrime Act 2001 (Cth).
[35] The *Oxford English Dictionary* defines 'cybercrime' as 'crime or a crime committed using computers or the Internet'; *Oxford English Dictionary Online*, Oxford University Press, December 2014.
[36] United Nations Office on Drugs and Crime, *Comprehensive study on cybercrime* (2013).
[37] M. McGuire and S. Dowling, *Cyber crime: A review of the evidence*, Research Report 75, Summary of key findings and implications (Home Office, October 2013), p. 5.