

2

AT THE CROSSROAD

Cyber, Critical and Cultural Criminologies

Introduction

Criminology has a long tradition of examining both the socio-structural and socio-cultural bases of crime and justice. Emerging in the late 1960s, critical criminologies have sought to illuminate the various ways in which crime, and the institutions of crime control, 'reflect and reproduce patterns of power, inequality, exploitation and exclusion' (Yar, 2012c, p. 52). Cultural criminologies, meanwhile, have grown in breadth and popularity since the mid-1990s, focusing on the intersections of culture and crime: 'to account for the culture and subcultures of crime, the criminalization of cultural and subcultural activities, and the politics of these processes' (Ferrell & Sanders, 1995, pp. 3–4). Throughout this book, we advocate a reinvigoration of criminological research that extends beyond conventional 'cybercrime'. Indeed, as Danish criminologist Katja Franko Aas (2016) observes, 'Criminologists have been, with some exceptions, relatively slow to take on board, or at least to systematically theorize, the technologically-mediated nature of our sociality.' To do so, we suggest, requires inspiration from interdisciplinary theories, concepts and approaches. As such, we position digital criminology not as a new sub-discipline, but as a critical and cultural criminological orientation to crime and justice in a digital society.

Digital criminology represents the intersection of critical, cultural and socio-technical theory and research. The purpose of this chapter, then, is first to provide a brief history of cybercriminologies, and then to summarise the key features of digital society, before moving on to discuss critical and cultural criminologies as they relate to crime and justice in digital society. In doing so, we consider how these conceptual frameworks might be further developed by the addition of socio-technical concepts, before moving on to elaborate some fruitful avenues for digital criminological theory and research in subsequent chapters.

A Brief History of Cybercriminologies

The internet has long-reaching origins: from advances in computing in the 1950s; to the earliest electronic mail (and spam) in the 1970s; to the first messages sent via the US-military-funded

ARPANET in 1969; to online communications within private, closed networks in the 1980s; to the global web in the 1990s (Leiner et al., 2009). Indeed, technological developments and their associated implications for crime and criminology can be charted across three broad periods: the 'pre-web' era of the 1980s to early 1990s, the 'global web' era of the 1990s to early 2000s and the 'social web' era from the mid-2000s to the present day. We do not intend to suggest that the challenges and opportunities for crime and criminological scholarship presented by each era are replaced or discontinued with the next, but that each period brings with it unique advances in technology that have particular impacts for crime and that can be broadly linked with associated shifts in criminological thinking and research.

Pre-web Era: 1980s to 1991

It was not until the 1980s that personal computers¹ were widely adopted in workplaces and public institutions in the developed West (Ceruzzi, 2003). From the 1980s onwards, however, the information and activities of governments, education institutions and corporations were rapidly computerised and associated with greater electronic data storage, as well as increased connectivity within closed internal and private networks (Ceruzzi, 2003; Williams, 1997). Criminology in this pre-web era (1980s to 1991) recognised that such widespread computer availability and electronic data storage, combined with internally networked workstations and dial-in connections, had opened up governments, corporations and educational institutions to new forms of crime through technology misuse. Computer-related economic crimes (including financial data theft and identity fraud), 'eavesdropping' and the interception of confidential communications, and the security and privacy of confidential information systems, as well as software piracy via illegal disk-based copies, were among the predominant concerns of the time (Clough & Mungo, 1992; Sieber, 1986). As computer technology was predominantly adopted in public and corporate organisations, these emerging harms were largely associated with white collar crime (Croall, 1992; Kling, 1980; Montgomery, 1986).

The pre-web period also marked the first legislative steps to address computer-enabled crime. For example, one of the earliest laws that defined computer crime was passed in Florida in the United States in 1978 in response to the fraudulent printing of winning tickets at a dog racing track using a computer (Hollinger & Lanza-Kaduce, 1988). This law was notable because it defined all unauthorised access to a computer as an offence, regardless of whether or not there was malicious intent (Casey, 2011, p. 35). By 1983, another 20 states had introduced computer crime legislation. The US federal *Computer Fraud and Abuse Act* of 1984 criminalised various forms of unauthorised computer access of information. Information relating to defence or foreign relations matters was regarded as a felony offence, whereas intrusions designed to access or alter all other non-classified forms of information were regarded as misdemeanors (Griffith, 1990, p. 460). Similar computer crime laws were subsequently introduced elsewhere. In Australia, for instance, a 1989 amendment to the *Crimes Act* outlined three categories of computer 'hacking' crimes: mere access, without seeking out or altering specific information; access without initial intent but opportunistically seeking or altering information; and access with intent to seek or alter specific information. In England, meanwhile, it was 1990 before the first criminal statute to tackle the misuse of computers was passed (Wasik, 1991). Consistent with many legislative frameworks, the very act of using a computer to breach a network or database was highlighted as an offence, regardless of specific intent (Greenleaf, 1990, p. 21). A tension running throughout the debates that led to these initial legal reforms was the question of whether the act of

computer misuse or unauthorised access itself should be specifically criminalised, in addition to the equivalent terrestrial or analogue crimes that may result.

Global Web Era: 1990s to 2000s

The modern World Wide Web went live to a global public on 6 August 1991 (Leiner et al., 2009). While understanding and legislating computer crime typified criminological research of the 1980s and early 1990s, the 'global web' era (1990s to 2000s) brought an associated shift towards internet and cybercrime research. The increased accessibility of online information sharing and communications that the global web brought for everyday users was widely recognised as creating new and massively expanded opportunities for crime as 'the perpetrators who attacked machines through machines . . . started attacking *real humans* through the machines' (Jaishankar, 2011, p. 26, emphasis added). Thus, while financial fraud, data theft, information privacy and identity crime remained (and remain) persistent themes in criminological research, the attention of cybercrime scholars broadened to include interpersonal harms such as online child sexual exploitation and child pornography (Armagh, 2001; Esposito, 1998; Mitchell et al., 2010), both of which had become the focus of much public and policy concern.

The scope and focus of cybercrime scholarship in the global web era is well captured by David Wall's (2001) original and highly influential typology, which comprises four categories of cybercrime:

- (1) *cybertrespass*, incorporating unauthorised access to a computer system, network or data source, such as through on-site system hacking, online attacks and/or malicious software (malware);
- (2) *cyberdeception and cybertheft*, including financial and data thefts, intellectual property thefts and electronic piracy. Such crimes may be facilitated through fraudulent scams, identity fraud and malware;
- (3) *cyberporn and cyberobscenity*, referring to the online trading of sexually expressive material and including sexually deviant and fetish subcultures, sex work, sex trafficking, sex tourism and child sexual grooming and exploitation material; and
- (4) *cyberviolence*, referring to the various ways that individuals can cause interpersonal harms to others. Such harms include cyberstalking, cyberbullying, cyberharassment and communications that support prospective acts of violence or terror, such as threats of personal violence, bomb talk or circulating instructions for making explosives and other weaponry (Wall, 2001).

These categories can be understood according to a common categorisation in cybercrime research: the first category represents computer-focused acts (i.e. directed at the machine), while the latter three are more readily described as computer-assisted acts (Jewkes & Yar, 2010; Smith et al., 2004). Wall's early work (2001) identified that the internet had influenced crime across these categories in at least three broad ways. First, by providing a platform for communications that may enable and sustain existing harmful and criminal activities, such as drug trafficking, hate speech, stalking and sharing information on how to offend. Second, through enabling participation in a transnational environment that provides new opportunities and expanded reach for criminal activities which would be subject to existing law in sovereign states. Third, the distancing of time and space creates potentially new, unbounded, contestable and private harms, such as the misappropriation of imagery and intellectual property. In particular, he suggested that the shrinking role of the state and the relative ungovernability of cyberspace (discussed further in Chapter 3) present particular challenges both for policing 'virtual communities'

and for the discipline of criminology more broadly (Wall, 1997). Wall argued that, while the new cyberspace offered enormous democratising potential, 'there are also many opportunities for new types of offending' and that the internet posed a 'considerable threat to traditional forms of governance and . . . to traditional understandings of order' (Wall, 1997, p. 208).

Despite this broad potential focus for criminology, in practice much cybercriminology has focused on financial crimes, identity fraud and threats to market and state security: the first three aspects of Wall's (2001) typology. Interpersonal violence has received much less attention by comparison. While there are a plethora of studies on cyberbullying, these are focused almost exclusively on minors (aged 17 years or under) and young adults (up to 24 years), and they are undertaken more often in the contexts of psychology, social work and education than criminology itself. Similarly, the many studies on cyberstalking originate largely from within psychological frameworks. In both instances, these fields of research have come to dominate work on cyberviolence to the relative neglect of a broader range of interpersonal violence and their intersections with digital technologies, including: intimate partner violence, sexual violence, racially and/or sexuality based harassment and/or hate crime, as well as more traditional criminological concerns, such as male-to-male violence.

In addition to restricted *topics* of analysis, much criminological research has focused on cybercrimes, cybercriminality and cyber law enforcement with very few studies seeking to apply or adapt criminological *theory* to such research (see Holt & Bossler, 2014, 2015 for a discussion of these limitations). The works that have undertaken such conceptual development have drawn predominantly on a handful of 'rational choice', deviant lifestyle and subcultural theories of crime (for reviews see Diamond & Bachman, 2015; Holt & Bossler, 2014). In particular, Lawrence Cohen and Marcus Felson's 1979 Routine Activity Theory (RAT) features so often in cybercrime theorising that it might be described as the prevailing orthodoxy in such research (Holt & Bossler, 2008; Hutchings & Hayes, 2008; Pyrooz et al., 2015; Reyns et al., 2011; van Wilmsen, 2011; Yar, 2005). For example, as criminologist Peter Grabosky (2001) explains:

[o]ne of the basic tenets of criminology holds that crime can be explained by three factors: motivation, opportunity, and the absence of a capable guardian . . . derived initially to explain conventional "street" crime, it is equally applicable to crime in cyberspace (p. 248).

While not all criminologists agree on the applicability of the theory to cybercrime (Jaishankar, 2008; Yar, 2005), its dominance is arguably highly influential in framing the focus of much research with regards to identifying the motivations of individual cyber offenders, 'target hardening' and identifying 'risky' online victim behaviours, as well as the challenges of law enforcement (as a form of guardianship), a trend which has continued in computer and cybercriminologies. Indeed, in a recent review of the current state of cybercrime scholarship, Thomas Holt and Adam Bossler (2014, p. 21), describe how the preceding 20 years of criminological research have predominantly focused on the study of the 'impact of technology on the practices of *offenders*, factors affecting the *risk of victimization*, and the applicability of *traditional theories* of crime to *virtual offences*' (emphasis added).

Social Web Era: 2000s to present

With the millennium came Web 2.0 and the 'social web' (2000s to present) as online communications became increasingly collaborative, with expanded capacity for user-generated content development

and sharing, as well as online social networking. Between 2002 and 2010, there was an explosion of social networks and image-sharing platforms, including Friendster, MySpace, Facebook, YouTube, Twitter, Tumblr and Instagram. Research into cyberbullying, cyberstalking and online harassment rapidly expanded over this period as the relative ease, anonymity and reach of online communications was associated with continuing concerns regarding invasive and threatening communications (Pittaro, 2007; Reyns et al., 2011; Spitzberg & Hoobler, 2002), particularly in relation to vulnerable groups such as children and young adults.

As the social web expanded, so too did the ‘deep web’ and ‘dark web’; a shorthand for content on the internet that is not indexed by standard search engines (and is thus not searchable) and/or that is protected by layers of encryption and other security mechanisms (Bergman, 2001). While not *all* content on the dark web is necessarily, or by definition, illicit, the concealment of such underground networks provides the ideal environment for activities such as: illicit content, including child exploitation material; criminal organising, such as by terrorist or organised crime networks; and black markets, trading in items such as malware and illicit drugs (Martin, 2014; Sugiura, 2018; Yip et al., 2013). A growing focus of cybercrime research has thus been to identify and understand the nature and patterns of such online criminal social networks (Brewer, 2017; Décary-Héту & Dupont, 2012; Holt, 2013; Westlake & Bouchard, 2016).

A further feature of the social web era is the increasingly mobile web, with smartphones and wearable technology becoming ever-more common — almost ubiquitous — and simultaneously collecting expansive ‘big data’ about our selves, our identities and our everyday lives. Criminological research has also sought to engage with these increasingly automated, algorithmic and computational capacities as they relate to crime data analytics, law enforcement and justice system practices (Berk, 2008; Birks et al., 2012; Brantingham, 2011). Though there is, as yet, a comparative dearth of criminological research that has begun to empirically and critically explore the range of challenges and opportunities presented by ‘big data’ analytics. Most recently, Janet Chan and Lyria Bennett Moses (2016, p. 25) note the relatively small engagement from criminologists with big data research, which tends to lie in two main areas: social media data analysis and the uptake of computer modelling/ algorithms as a predictive tool in police and criminal justice decision making. They suggest that criminologists, and social scientists more broadly, must increasingly collaborate with technical experts to further progress this field.

Breaking Through the Binaries of Online/Offline and Real/Virtual

As the preceding discussion shows, we believe that there are notable gaps in the current field of cybercrime research (Aas, 2007a,b; Hayward, 2012; Holt & Bossler, 2014). Despite more than ten years since the rise of the social web, criminological scholarship remains focused on computing and internet technologies as either themselves the *targets* of crime or as mere *tools* in the commission of otherwise familiar and recognisable crimes. The topics and foci of much of the cybercrime research are likewise limited in scope. An overview of both seminal and contemporary works — books, edited collections and journal special issues — over the past 20 years yields recurring topics including: hacking, data theft, online fraud and scams, digital piracy, child exploitation materials (‘pornography’²), online sex work, cyberbullying, cyberstalking, cyberterrorism and online extremism; as well as challenges for cyber legislation and law enforcement (Grabosky & Smith, 1998; Holt, 2011; Jaishankar, 2011; Wall, 2007). There are also cybercrime works on topics including information privacy and data surveillance