Cybercrime: A social ecology
Ben Collier and Alice Hutchings

Abstract

From its roots as niche technically-driven crimes and online subcultures, cybercrime and online harm now dominate public debates. This chapter examines cybercrime from a criminological perspective, setting out foundational debates and contemporary controversies. We set the scene by tackling the question: *what is cybercrime*? We lay out foundations of the field, discussing whether cybercrime is a novel criminological phenomenon, and critically reviewing classic typologies. We distinguish cybercrime from *hacking,* discussing changes in the Internet and online harms. It is increasingly difficult to differentiate a 'cyberspace' given the digital technologies and infrastructures pervading contemporary societies.

We outline *core aspects of cybercrime* as a subject of scholarship, describing tools, technologies and practices associated with online deviance. We show how these link to the broader cybercrime economy. We discuss anonymity technologies and encryption, then move to less-technical practices supporting online crime through social deception. This section concludes with an overview of the wider implications of online harm, including leaks from the vast databases of sensitive information held by large companies about us, and corporate and white-collar crimes facilitated by technology.

The next section explores the broader *ecology of online offending* - the communities associated with cybercrime. We sketch the online deviant subculture literature, discussing the historic significance of the 'hacker ethic' to offenders' self-image. We discuss the sites these deviant subcultures interact - hacker conferences, chat channels, social media, forums, and underground marketplaces. We outline the roles around which deviant communities are structured, and the pathways in and out of them, reflecting critically on opportunities and challenges for desistance. We draw out links between the cybercrime literature, classic subcultural criminology, and the study of youth crime and deviance, asking if cybercrime is simply an online form of juvenile delinquency.

The last section discusses how various groups deal with these harms with varying levels of success. The landscape of *enforcement and control* for cybercrime is generally delocalised from the police, organised around polycentric networks or 'nodal' governance. These include a range of public, private, and third sector organisations arrayed in national and international coalitions. Traditional police forces face capacity issues, giving rise to centralised agencies such as the FBI and the UK's National Crime Agency (NCA), international collaborative bodies, and security services. We discuss private sector actors: platforms and private security companies. We draw out the foundations of a critical perspective on cybercrime policing - increasingly securitised, 'high-policing', and anti-democratic, and its implications. We conclude by sketching *potential futures of cybercrime scholarship* within the broader field of criminology.

Cybercrime: A social ecology

Introduction

In this chapter, we make the case that despite its increasingly contested nature as a field of study, cybercrime is an important area for mainstream criminologists to understand and engage with. The national and international contours of power, crime, and harm emerging in Internet societies are at the heart of many crucial areas of contemporary criminological debate.

Cybercrime scholarship has sat awkwardly within criminology for the past three decades. As an empirical phenomenon it has exploded from an initially niche interest to one which now dominates global news agendas. Despite the increasing prominence of cybercrime, its integration into mainstream criminology remains fragmented and piecemeal, long after its political and public relevance has become clear. While cybercrime scholars draw on classic theories from criminological scholarship, there has been little incorporation of new ideas from cybercrime studies into the criminological mainstream. In recent years, a clear shift has occurred - cybercrime has begun to stabilise, and sufficient empirical and theoretical scholarship now exists, providing the foundations of a recognisable sub-field. We sketch these foundations, looking ahead to possible futures, controversies, and politics in the next phase of cybercrime scholarship.

In this chapter, we introduce cybercrime, setting out key terms, ideas, and debates which have animated cybercrime scholarship *by criminologists*. We discuss the main aspects of cybercrime as a phenomenon, the core theory through which criminologists have attempted to reckon with it, and discuss ways in which nation state and private sector forces are attempting to govern crime on the Internet.

What is cybercrime? Setting the scene.

Is cybercrime novel? A critical look at typologies

What do we mean by ‘cybercrime’? The term is not straightforward, and the definitions we use are drawn from a previous era of digital technologies, when the ‘online world’ and the ‘physical world’ were more clearly separated (Cohen, 2007). One common typology distinguishes between cyber-enabled and cyber-dependent crime. Cyber-enabled crime refers to traditional offences that have moved online. Fraud and theft occur in physical space, but have online variants. However, cyber-dependent crimes are dependent on the technologies that enable them. These include malware, unauthorised access, and denial-of-service attacks - crimes which would not exist without a global infrastructure of networked computers.

We argue that the distinction between ‘traditional’ forms of crime and ‘true’ cybercrime is questionable. First, the distinction between traditional offences that have moved online and crimes that are dependent on technology is not clear cut. Denial-of-service attacks deny access to online resources, such as a webpage - these are often considered to be a ‘true’, or technologically-dependent form of cybercrime (Sauter, 2014). However, ‘real-world’ analogues of denial-of-service attacks clearly exist - there are other activities, such as protests, that can deny access to physical spaces, and sabotaging phone lines, highways, or postal services are also comparable. Denial-of-service attacks are also used for extortion, which is certainly a traditional type of offence (Karami, Park, and McCoy, 2016). Another example is ransomware, a type of malware that encrypts data until a fee is paid. While the use of malware (and by extension, ransomware) is a cyber-dependent crime, ransom is a traditional offence. Similarly, while unauthorised access may refer to accessing computer systems, it is similar to trespass on physical property.

The term ‘cyber’ is also contested. ‘Cyberspace’ was coined by William Gibson in the novel *Neuromancer* in 1984 to describe a virtual world divorced from terrestrial life. It is used synonymously with the internet and the world wide web. Some think of networked devices, physical and observable, while others think of cyberspace as a separate dimension, distinct from physical ‘meatspaces’. Thinking of ‘cyberspace’ as a distinct topology may have made more sense in the early years of the Internet, but as networked technologies have increasingly become incorporated and embedded in all aspects of our daily lives, digital sociologists understand our society as being made up of *hybrid* spaces which incorporate a range of digitally-networked and physical elements (De Souza e Silva, 2006; Brown, 2006). Although cybercrime has gradually become the most used term, it is by no means the only term used to refer to the same or similar phenomena, with synonyms including online crime, virtual crime, techno crime, electronic crime, high-tech crime, computer crime, e-crime, digital crime, and internet-related crime.

The second concern about these typologies is they are unlikely to age well. For the future ‘digital natives’, what is considered to be a ‘traditional crime’ will change. Future generations are likely to be puzzled by these distinctions in years to come, as they gradually fall out of favour. Digital networked technologies have shaped and been shaped by our societies in remarkable and often-unpredictable ways, and their growth and adoption has been accompanied by transformations in how people work and socialise, the way people interact with each other and their daily routines. Within a lifetime, we have seen rapid changes in technology, from mainframe computers, to personal computers, laptops, and smartphones. Once, computers took up entire rooms, now we can wear them on our wrists. Our lives have also become more datafied - mediated and monitored by flows of data. While this brings efficiency, convenience and arguably better, data-driven decisions, it also creates opportunities for harm in almost every aspect of our lives. The cybercrimes of the future will evolve as future technologies are developed (Tuptuk & Hailes, 2018).

The question then turns to how future criminologists will define cybercrime. Perhaps once the novelty wears off, it will no longer be distinguished from other types of crime. Research tells us cybercrime offenders tend to differ from other types of offenders (Weulen Kranenbarg et al., 2018), so it’s unlikely that those who steal from people’s homes turn to

more technically sophisticated methods. Long-used definitions like violent crime and property crime may be perfectly applicable to cybercrime in the future.

Hacking versus cybercrime

The term ‘hacking’ is often used uncritically by criminologists and the media to refer to unauthorised access and other high-tech crimes. However, in computer science the term has a longer, more complicated, history. The hacker subculture emerged initially in the 1950s and 1960s in the US, fusing the countercultural libertarian radicalism and utopianism of youth cultures at the time with the work and ideas being explored in the government/academic computer labs developing networked computing technologies. “Hackers” were once operators of legitimate amateur radio and computer programmers, who were admired for their technical skills rather than reviled. “Hacking” referred not (necessarily) to illegal activities, experimenting with technology and pushing it to the point of breaking to find new and unexpected behaviours and potential uses never considered by its designers; to circumventing ‘hard coded’ restrictions; or to build new and exciting technologies which disrupted established institutions and social structures. The current criminalisation of the term can perhaps be traced back to Levy’s (1984) book, *Hackers: Heroes of the Computer Revolution*. While Levy was using the term to refer to those who ‘... guid[ed] computers to greater heights than anyone expected’, he also outlined a ‘hacker’ code of ethics, which is occasionally misapplied as techniques of neutralisation to justify causing harm. American academic and military researchers working on computer networks in the 1950s, before modems were developed, and when programs ran using punch cards, developed a unique set of ethics, which Levy (1984) summarises as follows:

> *Access to computers – and everything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!*
>
> *All information should be free.*
>
> *Mistrust Authority – Promote Decentralization*.
>
> *Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position*.
>
> *You can create art and beauty on a computer.*
>
> *Computers can change your life for the better.*

These ethics should be considered in the historical context in which they were created. For example, the principle ‘all information should be free’ referred to a ‘free exchange of information’ (Levy, 1984, p. 27), such as sharing computer programs, rather than accessing another computer system illegally. Similarly, the authorities that were to be mistrusted were not necessarily law enforcement agencies, but rather ‘bureaucracies, whether corporate, government, or university, as they limited the free exchange of information’. Within computer

science, the term hacker still carries this somewhat positive connotation, with some puzzlement as to why so many criminologists use it to describe criminal activities.

As cybercrime has developed into more businesslike forms, it has become alienated from the practices of experimentation and creativity which typify traditional hacking. However, the hacker ethic still provides an important touchstone for the cybercrime subculture, even if it is increasingly divorced from the reality of cybercrime work (Collier et al. 2021). The core values and aesthetics still prove important to the meanings, identities, and communities which form around cybercrime; ideas of technical mastery, anti-authoritarianism, and techno-libertarianism still bring cybercrime communities together. The political goals espoused in the 'hacker ethic' often animate more activist forms of cybercrime, and the aesthetics of hacking, through pop culture representations, provide a powerful attraction to newcomers, meaningful shared identities to existing members, and contribute to classic subcultural processes of labelling and group identification.

The activities and communities of cybercrime have developed their own subcultures, distinct from the increasingly institutionalised, politicised, and legitimate world of hackers. In English-language communities, this draws from the libertarian, nihilistic culture associated with trolling communities - online subcultures of 'digital tricksters' (Coleman, 2014) who cause havoc, deliberately provoke outrage, and engage in online harassment (Hodge and Halgrimmsdottir, 2020). Few genuine hacktivists emerge from cybercrime forums, which are mostly concerned with petty scams, gendered violence, illicit businesses, get-rich-quick schemes, and entrepreneurial, rather than activist, values. These cybercrime subcultures are now rarely centred around the cultivation of serious technical skill - the majority of crimes constitute petty fraud, cyberstalking and harassment, or repurposing well-worn exploits into easy-to-use tools. Where aspirations of 'hacker' status come in directly, they are generally linked to a stereotyped form of masculinity (as hard technical mastery) which gives alienated young men a route to other 'masculinities' with which they can identify (Bada et al., 2021; Hutchings and Chua 2016; Holt et al., 2020; Messerschmidt 2005). This combines to give these communities an adolescent 'boys club' atmosphere.

Cybercrime communities also draw on and overlap with a range of other online subcultures, and although we focus on US and European communities, there is substantial variation in cybercrime and hacker cultures around the world. These are shaped by the local political and cultural environment - e.g., the Russian cybercrime scenes operate in a generally more permissive law enforcement environment (as long as attacks are targeted internationally rather than domestically) and so are less dominated by petty scams and romance fraud. In China there are a range of cybercrime communities aligned with pro- and anti-government groups, including a thriving community operating 'airport' services to allow access to the rest of the world through the Great Firewall (Chua and Collier, 2019).

Cybercrime as routine activity

Cohen and Felson's (1979) routine activity approach is the criminological theoretical framework most often applied to online offending. This developed from the concerns of the Chicago School, attempting to understand how large-scale changes in movements and activities of people and the environment of the city shaped the cultural and social

phenomena they were studying. The premise is predatory crime occurs in the presence of likely offenders and suitable targets, and the absence of capable guardians. As the emphasis is on criminal acts, rather than individual factors, it is well suited to the study of large-scale social changes, such as the growth of suburbs, the rise of consumer capitalism, and changes in women's access to work, and how they present novel opportunities for crime (such as unattended houses full of lightweight, expensive luxury goods) or on the 'micro-chemistry' of opportunity presented by particular criminal situations.

According to Felson (2008), technological developments are among the main factors changing people's routine activities, and so RAT is an easy at-hand theoretical tool for use in the study of cybercrime. This focuses on analysing 'criminogenic situations', with the Internet's digital infrastructures bringing together potential offenders and victims, lowering barriers to offending, and thus creating opportunities for crime. As our daily activities are lived through digital networks and services, we are linked more to other people around the world, and hence increasingly exposed to threats and risks.

The crime survey for England and Wales included fraud and computer misuse offences for the first time in 2016. This revealed - contrary to previous trends - the crime rate was not dropping, it was moving online but not being captured in the data. When the crime survey was changed, the crime rate doubled overnight. This problem where a lack of collection about online crime creates a perceived crime drop is widespread (Tcherni et al., 2016).

Of course, the data now being collected still have many limitations. The definition of computer misuse offences used in the crime survey are quite limited, capturing 'computer viruses', and unauthorised access to personal information. As we show later, the range of cybercrimes is much more extensive. Furthermore, surveys only capture those who are aware they have been victimised, and individual targets, rather than organisations and government agencies. While ground truth is problematic, the crime survey illustrates that cybercrime is a particularly important aspect of crime.

The routine activity approach can also be used to explain changes to cybercrime during and following the COVID-19 pandemic. As property crime and violence went down, many types of cybercrime increased (Buil-Gil et al, 2020; Horgan et al, 2021). Analysis of an online blackmarket showed that during the start of the pandemic, there was a significant increase in transactions (Vu et al., 2020). This market stimulation occurred as our routine activities were changing - and not just those adapting to working from home. In particular, forum discussions indicated it was a period of intense boredom and economic change. Lallie et al. (2021) found as governments were scrambling to implement lockdowns, distribute PPE and implement stimulus packages to offset economic hardships brought about by the pandemic, criminals were leveraging government announcements and key events in their cybercrime campaigns.

However, the routine activities approach has also come in for significant criticism (Wortley, 2010). At the heart of much contemporary RAT scholarship is an assumed technological determinism - new technologies and social arrangements act unidirectionally to reshape society, with little room for individual agency, culture, or community action. This is mirrored in the 'situational crime prevention' (Clarke, 1995) policy programmes which RAT scholarship suggests, which mandate hardening of targets through the purchase of private security,

‘hostile architecture’ changes to the online built environment to prevent crime through design, and the incorporation of technical controls into the workings of the Internet which allow intrusive government and corporate surveillance. This both ignores the ethic at the heart of online deviance - technologies are malleable, and can be subverted, repurposed, and destroyed by ingenious human creativity - and paints a vision of the future based around technocratic control, centralised design, and marketised private security, rather than collective goods, democracy, and liberation. Technological solutionism - realised in the idea that we can design crime out of our online spaces - has similarly negative results in offline crime control. It has been largely co-opted into neoliberal and post-neoliberal agendas (despite its ‘high modern’ roots as a philosophy of social design) to alienate public space, push social problems out of the view of middle-class society, and entrench technocratic control in the built environment.

The tools, technologies, and practices of cybercrime

One of the difficulties with researching cybercrime is that relevant datasets can be hard to come by. There is no central way to report cybercrime, so data held by police agencies, online platforms, and financial institutions will each only represent a fraction of the overall problem. Therefore, comparing which types of cybercrime are more common or cause the most harm is difficult. Here, we examine some of the types of cybercrime most often prosecuted in the UK.

Data or system breach and vulnerability exploitation

Breaches can occur at a variety of levels. For example, a computer system may be breached, providing access to all the data on a computer. Alternatively, an individual account may be breached, such as email (Mirian et al., 2019). Once access is obtained, data may be stolen (although this does not necessarily deprive the data holder of access, so is dissimilar to theft of physical property). Data may also be damaged, destroyed or deleted. Data breached in this way can subsequently be monetised, by demanding the victim pay a ransom for its return, threatening disclosure (doxxing), or selling it for subsequent misuse, such as credit card fraud (Porcedda & Wall, 2019).

Data or system breaches can involve technical attacks, which exploit unforeseen weaknesses in computer systems. An example is SQL injection, which hijacks parts of a website where users enter their own data (such as their name). If these fields are not set up correctly, an attacker can use them to smuggle database code directly into the server, allowing them to execute commands on the website’s databases and gain access to sensitive data. Alternatively, they can be very non-technical in nature, such as reusing passwords. In some cases, the person may have legitimate access to the computer system but use access in an unauthorised way. In the UK many police officers and staff have been prosecuted for misusing access to police databases (Hutchings & Collier, 2019).

Social exploitation - romance scams, get rich quick schemes, impersonation, and frauds

Online deception can take many forms, from elaborate advance fee frauds, to credit card fraud, and the online sale of counterfeit, non-existent or stolen products. These often involve elements of social exploitation, deceiving others for a financial advantage. Developments in technology have created more opportunities for fraud, from romance scams on dating platforms, to investment scams advertised on social networks (Cross, 2019). A variety of media may be used, including email, social network sites, and online trading sites, to manipulate others into providing money or identity details. Other frauds occur in the workplace, such as altering computer data to divert funds for personal use or manipulating financial records to hide unauthorised transactions.

Research into fraudulent activities targeting organisations reveals so-called CEO fraud is commonly conducted electronically. In this type of fraud, managerial-level staff are impersonated in money transfer requests sent by email. Junger et al. (2020) found CEO fraud is often seasonal, targeting potential victims during holiday periods when those impersonated are likely to be away from the office. Even offline scams often have an online component. Bidgoli and Grossklags (2017) found scams conducted by phone involved telephone number spoofing and electronic payment. The inverse is also true, with technical support scams, where victims are infected with malware when they believe they are receiving assistance, starting with a phone call (Miramirkhani et al., 2016).

Malware and toolkits

Malware refers to malicious software - programs which, when executed, can facilitate a range of harms, depending on the type of malware. Some forms of malware can control an infected computer remotely, logging all the users' keystrokes, take screenshots when a mouse is clicked, stealing credentials and cookies to imitate sessions, and controlling webcams. Malware can connect infected machines to large networks of other infected machines (called botnets) which can be used as a criminal infrastructure to launch further attacks, send spam, evade law enforcement, or mine cryptocurrency.

Ransomware has become prominent in recent years due to its use in high-profile attacks on major companies and critical national infrastructure. Ransomware can infect a single computer, or spread around a target network. It typically encrypts data and renders it inaccessible until a payment is made (Paquet-Clouston et al., 2019). As a wide range of major businesses and services now hold increasing amounts of intimate user data - from banks, to hospitals, to hotels - ransomware gangs often threaten to publish any sensitive data. This combination of tactics has led to private and public sector organisations paying millions of dollars in ransom fees to regain access.

Malware is often differentiated by the method in which it is spread. Worms are self-replicating and self-spreading, with the Morris worm being an early example. Viruses are also self-replicating, but require assistance to spread, such as sharing files and discs with other users. One example is leaving USB drives in carparks, particularly if attempting to infect a targeted organization. Trojans are not self-replicating and require manual

intervention to install. Like the Trojan horse from Greek mythology, the malware is hidden inside a seemingly innocent computer file. On the other hand, drive-by-downloads are spread by visiting a website using a vulnerable browser, typically requiring little human intervention.

Malware can vary in sophistication, with those exploiting zero-day (undetected) vulnerabilities being the most valuable. While stories of targeted malware used by nation states is news-worthy, the majority of malware is spread in a scattergun fashion. Simoiu et al. (2020) examined at scale malware spread by email, finding much was distributed globally and indiscriminately, rather than in a targeted manner.

Toolkits are attack tools made available for cybercrime. They automate the attack process. They are often customisable, some can be updated, so attackers can use the most recent version, and some come with support services. Toolkits can lower the barrier to entry for offenders, as they don't have to program the entire attack from scratch each time, and some come with nice graphical user interfaces, making them even more usable.

Denial-of-Service and low-level cybercrime

Although media accounts focus on high-profile attacks, the vast majority of cybercrime is petty. Denial-of-service attacks are an example of this ‘low-level’ cybercrime, involving directing massive amounts of computer traffic at a victim, knocking them offline. This was originally carried out as a ‘digital sit-in’, with large numbers of volunteers using their own computer to access the websites of political targets at the same time - causing them to become choked with traffic. As automated approaches were developed - such as networks of infected computers which could be directed to send this traffic - this developed into a prank or harassment tactic associated with the Anonymous (and later, Lulzsec) groups (Coleman 2014, Sauter 2014). As the commercial possibilities of these attacks became clear, a market emerged for selling denial-of-service tools and services.

While cases involving denial-of-service attacks rarely turn up in the criminal courts, this is a frequently occurring type of crime, with attacks at least in the tens of thousands *per day* (Collier et al., 2019). The majority of such attacks are never reported to the authorities. Of those that are, only a fraction are investigated, and there are often difficulties finding the attack source. One reason is most denial-of-service attacks are of a short duration, aimed at knocking services offline momentarily. Most attacks are against home IP addresses, presumably to gain an unfair advantage in an online game.

These types of denial-of-service attacks, as well as other types of cybercrime, including fraud, are often characterised as ‘high volume, low value’. The few that are reported are seldom investigated. Police tend to prioritise low volume but high value crimes, which means the vast majority of reports will never be looked into, even if individually they contain valuable parts of the overall puzzle. If online offenders can take basic precautions to not make their identities obvious, in many cases they are operating with impunity.

Operational security and avoiding the cops - anonymity networks, currencies, and encryption

Cybercrime offenders have a range of ways to avoid detection. Operational security (or 'opsec') techniques include the use of anonymity networks, proxies and VPNs, and alternative currencies. The most well-known example of an anonymity network is Tor, initially invented by the US Naval Research Laboratory as a means of securing military connections on insecure networks run by foreign governments. Tor sends user signals through the Tor network - a global network of volunteer-operated servers (or 'relays') - hiding the routing information in three layers of encryption, which are decrypted one-by-one as the traffic bounces between relays. This means no part of the network - and hence no observer - knows both where the encrypted traffic comes from and where it is going. Lots of people using Tor at the same time around the world makes any individual hard to trace - and so it is often used by individuals to make their web browsing hard to surveil by governments, and to circumvent censorship, allowing access to websites blocked by Internet Service Providers. Tor can also be used to set up 'Onion Services' - websites, such as forums or marketplaces, which are only accessible through the Tor network. This makes the true location of the server very difficult to establish and are therefore difficult to take down. While Tor often gets a bad reputation, as we discuss below, the vast majority of cybercrime does not use it. In the meantime, Tor has many legitimate, useful purposes (Mirea et al., 2019), including by journalists and activists within oppressive regimes. This is one reason why Tor still receives US government funding - much like 'Radio Free Asia' before it, it contributes to the USA's use of the Internet as a tool for global soft power.

Another way for cybercrime offenders to hide their tracks is to use proxies and VPNs - servers located around the world which are used to hide where signals are coming from and going. These act as intermediaries, to make it look like the traffic is coming from somewhere else. Their use does not eliminate all risks for cybercrime offenders. Law enforcement have gone as far as operating VPNs, to access relevant data. However, this level of complexity is often not required, as many VPNs will provide logs to law enforcement on presentation of a warrant. There are indications VPNs are not as trusted as they used to be. Proxies are also used as intermediaries. Botnet-based proxy networks use compromised machines as intermediary points for traffic. Proxies are readily offered for sale on stolen data markets (Hutchings & Holt, 2015).

Tracing the money is an important aspect of investigating financial crimes. There are two aspects to this. One is understanding how the crime works, the other is attribution. Currency exchange is a big aspect of cybercrime, and receiving payments for cybercrime goods and services can be a huge undertaking. Some cybercrime relates directly to currency transfer, such as monetizing stolen credit card data, or stealing money from bank accounts. Compromised accounts are used for this purpose, and it often requires the use of mule accounts to move money around.

Alternative currencies provide opportunities for cybercrime. Amazon gift cards, often used for receiving payment from fraud victims, are exchanged on cybercrime forums (Pastrana et al., 2018). Other alternative currencies, such as airline loyalty point accounts, are targets for compromise (Hutchings, 2018). Western Union is used for transferring funds across borders,

often for legitimate purposes, but sometimes for reasons connected with crime generally, and cybercrime specifically.

eCurrencies are another form of alternative currency. Unlike Western Union, which is based on traditional currencies and therefore more likely to be subject to local regulatory agencies, digital currencies are less likely to be regulated. Two digital currency providers, Liberty Reserve and e-gold, were alleged to facilitate money laundering and online crime, and were shut down amid US prosecutions. Others, like webmoney and RBK money are commonly offered as payment options on cybercrime markets.

Cryptocurrencies use blockchain as a ledger, which provides a degree of transparency. One analysis of online blackmarket activity shows after Liberty Reserve was taken down in 2013, there was a corresponding increase in the use of Bitcoin, perhaps pointing to a displacement effect (Atondo Siu et al., 2021). While remaining a popular cryptocurrency in cybercrime markets, Bitcoin is particularly open to traffic analysis (Vasek & Moore, 2015). Paquet-Clouston et al. (2019) analysed ransomware payments, finding a small number of actors receive the majority of payments. It seems those who use Bitcoin for high profile cybercrime events can experience difficulty getting it out of the system and turning it into cash, although there are ways to obfuscate the trail, such as using mixers (Meiklejohn et al., 2013).

Corporate cybercrime

Large amounts of personal information are collected about individuals and stored by companies. This introduces security, as well as privacy, concerns if the data are breached. In many cases, there is an information asymmetry, with individuals having little information about what data is held about them, nor about the corporations holding such data, while they know everything about us (Zuboff, 2019).

Such databases provide opportunities for crime to a number of different parties. First, they are a target for unauthorised access by outsiders, those who identify vulnerabilities in the security of the company holding the data. Second, they are a target for access by those within the organisation, employees or contractors, who may misuse their authorised access. Third, companies themselves may engage in wrongdoing (whether this is labelled as ‘criminal’ or not).

The data footprint we leave behind enables corporations to predict our future behaviour. Online, this means we may see more personalised content, such as advertisements tailored to us. Those with access to the data and a large user base can do this at scale. But it’s not just about selling us the latest products. Cambridge Analytica showed us how such data can be used for nefarious purposes, such as swaying elections and cementing power (Wylie, 2019).

Cybercrime communities

The structure of cybercrime economies

Cybercrime has not remained static over the past thirty years, and as the nature of online crime has evolved, so have the structures of its associated communities. While much cybercrime involves interpersonal abuse, targeted harassment, or deliberate harm, much of it is also *work* - efforts by individuals to start small businesses, run infrastructure, make money, achieve particular goals, or provide services for one another. Economics is shaped by social structure - and as cybercrime has evolved, so have the communities and cultures with which it is associated.

Early research on cybercrime focused on the phenomenon of *hacking* and the *hacker*, generally depicting cybercrime as committed by talented lone actors building and researching their own tools and exploits. However, this picture of hackers as heroic, lone actors bending the online world to their will is misleading. Although some genuine lone actors do exist, these tend to be rare - cybercrime is mostly a community endeavour. As more cybercrime research emerged in the 1990s, a community-based model became prevalent. In this model, cybercrime communities could be divided between a small group of ‘l337’ (or ‘elite’) hackers who come up with new exploits and develop tools, and a much larger group of ‘skids’ or ‘script kiddies’ for whom cybercrime is more like lockpicking - learning to use pre-made tools bought from others. This made cybercrime and ‘hacker’ status aspirational - one could start off as a low-level script kiddie and slowly develop technical skills and online ‘street-cred’.

These tool-sharing communities have evolved in the same way business models for legitimate online services have. Rather than selling hacking tools to customers, who then have to figure out how to use them, a burgeoning cybercrime entrepreneur can instead turn these tools into an infrastructure - a cybercrime platform which they can rent out as a service. One example is Zeus, a popular type of banking malware. In 2011, the source code for the toolkit was leaked, meaning those who sold the software could no longer make a profit. As an alternative way of monetising the malware, Zeus-as-a-Service business models began emerging, allowing users to hire networks of infected computers. For the provider, this maximises potential earnings, as you are providing the same service to multiple users. There are economies of scale at play here. For the user, it reduces the initial financial outlay, outsources logistical and maintenance requirements, and reduces the risk of failure (Hutchings & Clayton, 2017).

Another as-a-service business is booter services, which provide denial-of-service attacks for a fee. Denial-of-service attacks can be difficult to monetise, at least in a way that provides a stable income over time with minimum effort. By providing a subscription service, with short attacks, there can be a steady income stream with relatively little effort (Hutchings & Clayton, 2016). Booters are advertised towards gamers, with subscription options starting around $5/month. For the user, the barrier to entry is greatly reduced; you can order strong attacks armed with nothing more than a PayPal account and your opponent’s IP address. As this model has emerged in the last fifteen years, it has transformed cybercrime from a small-

scale, high-harm crime characterised by small numbers of high-profile attacks to a true ‘volume’ crime.

This somewhat short-circuits the aspirational model of cybercrime. Rather than developing their own skills as an ‘apprentice’, novice entrants to cybercrime communities instead now constitute a consumer class, purchasing services from the relatively small number of people who run cybercrime infrastructure as a business. While one can join one of these illicit businesses or ‘gangs’, the work required is now a long way from the creative exploitation of old - these services need customer support, website developers, system administrators, and social media promoters rather than hackers developing creative new attacks. These jobs are far less exciting and intellectually stimulating than the traditional work of ‘hacking’ - and increasingly, exit is through burnout and boredom rather than in handcuffs, with only small numbers of motivated individuals progressing to genuinely skilled forms of crime (Collier et al., 2021).

Thus, an ecology has emerged - a tiny group of people create new exploits and identify vulnerabilities (outside legitimate security researchers and nation state actors, probably only a few thousand in the world). A slightly larger group package these up as tools. Bigger groups build and maintain infrastructure, running customer service and curating the ‘business’ side. A community of ‘skids’ who buy and sell tools are now followed by a sea of people - cybercrime customers - with no skills at all, who use these services.

Key sites in the cybercrime ecology

The online spaces of cybercrime have grown up and evolved along with the changing Internet. Initially, communities were organised over BBSes - dial-up bulletin boards connected to over phone lines, where people shared pirated software, hacking tools, tips, and culture[1]. The World Wide Web gave rise to a flowering of new online sites, with hacker forums and mailing lists emerging. These fulfil a range of functions, allowing people to teach and learn computer skills, coding, and basic ‘hacks’, providing a space for buying and selling hacking tools and ‘how-to’ guides, facilitating a marketplace in semi-licit goods, and acting as a place where people come to discuss social life and politics, and hang out with like-minded people. Most of the larger ‘open’ forums have little technical component, focusing on ‘hacker culture’ discussions, social engineering, basic hacks, and petty scams. Although the more technical and serious crime can be found largely on small, members-only forums, the larger forums play an important role in the wider ecology. These act as wider spaces for different communities to come together in a central site, and can be crucial places where powerful new malware is leaked, new forms of crime emerge, and cybercrime services sold.

One ‘space’ in particular looms large in popular depictions of cybercrime - ‘The Dark Web’, also known as ‘the Dark Net’. This term is often ill-specified - media and law enforcement tend to use it to mean ‘bad things on the Internet’, while more informed commentators use it to refer to the network of hidden services hosted on the Tor network (or other anonymity networks like I2P). These include both hidden forums and the legendary ‘cryptomarkets’ -

[1] Archives of many classic BBSes (a rich primary research resource) curated by Jason Scott can be found at www.textfiles.com

which function as marketplaces for drugs and other illicit services (Barratt & Aldridge, 2016). Tor's relevance for cybercrime is overstated - cryptomarkets and hidden forums *do* exist on Tor, but the vast majority of online crime and illegal trading is committed elsewhere, on open sites and social media platforms on the 'clearnet'.

Despite its powerful anti-surveillance properties for web browsing and hosting, Tor is an ineffective tool for committing serious technical online crime. It is much slower than the regular Internet, services can be easily made unavailable through denial-of-service attacks, and the skill barrier to entry for most is still too high to grow illicit businesses into genuine mass markets. A range of much more effective tools for online crime and illicit anonymity exist (such as VPSs, VPNs, botnets, etc.). So why do people still use Tor? Its early notoriety meant a range of communities sprang up who admired what they saw as its embodiment of a technolibertarian politics of privacy and anonymity. The 'free' marketplaces for all kinds of licit and illicit goods provided a template for others, and a set of communities and practices which persists. Although other, better tools are available, its open nature and existing communities effectively allow it to function as a social network and a community of security practice - enough people are aware of it and use it that, if you have something to sell, you know there will be a relevant market on Tor of people with shared cultures, understandings, and anonymity practices (Bancroft and Scott Reid, 2017).

Although forums and markets still have their place in this ecology, the rise of social media has provided a range of new and diverse sites where people exchange and advertise tools and skills and participate in the cultural life of cybercrime communities. Entry-level skills are increasingly learned through YouTube videos, discussions about hacks and tools occur on Twitter and other apps, and services are advertised on Instagram. Messaging platforms play an important role, with new types of spaces developed from the old IRC chatroom model (where lots of hacking used to be done). These now appear in a 21st Century guise as Whatsapp, Discord, and Telegram - often sites made for very different purposes (such as managing a videogame fan community or speaking to family and friends) are being repurposed to manage the business of cybercrime.

Finally, it is important to remember that despite the online nature of cybercrime, the people in these communities live in physical spaces of their own, with offline social networks, friend groups, and family ties. People can get their friends involved and are often more likely to target friends or enemies at their own school or in their local communities. Their motivations for entry and exit are rooted in their own lives and the social forces at play in their immediate environment - both digital and physical. Local organised crime gangs still operate and draw in young people to cash out fraud earnings or engage in low-level cybercrime (Leukfeldt and Holt, 2021). Poverty, racism, and overpolicing still affect these young people - the 'digital' dimension of offending does not overcome their rootedness in long-standing networks of power, oppression, and harm.

Understanding pathways and desistance

The question of *who* commits cybercrime has been central to cybercrime scholarship. Administrative research aims to help the police profile potential offenders. Critical

scholarship explores the broader dynamics of cybercrime as a (potentially) novel phenomenon (Yar & Steinmetz, 2019). Cybercrime is generally understood to involve a different 'typical offender' than other forms of crime; it is also generally committed by young men, but *some* evidence suggests those who commit cybercrime are often more affluent. The gender skew is (of course) not due to a lack of technical skills; as shown by the many women, queer, and nonbinary 'hackers', engineers, and technologists who built the computer industry, the Internet, and the technologies on which they rely (Light, 1999; Abbate, 2012). Rather, it is more likely this is due to the pervasive misogyny of cybercrime communities (Marganski, 2020), a phenomenon mirrored in wider programming-centred online communities (Nafus, 2012, Brooke, 2021). Some studies have shown routes of initiation into cybercrime behaviours to involve online gender-based violence and controlling or abusive behaviour, with many becoming involved in these communities because they want to stalk, harass, or spy on a romantic partner or another young person (Bada et al., 2021).

Despite repeated assertions to the contrary by police and policymakers, there is no conclusive evidence of a causal link between being on the autism spectrum and cybercrime. Although some studies have attempted to suggest the hyperfocus associated with some forms of autism is linked to coding skill, these have generally failed to be replicated, with some studies showing a weak 'autism-link' with non-technical forms of cybercrime and no link with technical forms (Lim et al, 2021). The forms of work involved in contemporary cybercrime are dependent on complex social coordination, with teamworking, business, and social engineering skills being far more important than technical prowess. Despite this, this narrative has taken hold - and shapes policing and sentencing, leading to a 'self-fulfilling prophecy' and classic labelling. Future scholarship could focus on how these perceptions are causing serious stigmatisation and targeting of autistic young people.

One possible entry point for cybercrime 'careers' is online videogames. This synthesises theories of drift and 'deviant leisure' in the context of online communities, with a pathway emerging in which young people come across cybercrime networks while attempting to cheat or modify videogames, from which they progress into more serious forms of online deviance and criminal offending (Goldsmith and Brewer, 2015). There is some evidence to support a pathway from videogaming, though as this is now a near-ubiquitous cultural phenomenon, it may simply be many of the teenagers at peak offending ages also tend to play videogames recreationally.

The attractive forces which bring people into cybercrime communities are better understood. For some, the 'hacker ethic' and its glamorous image provide a clear identity and set of core values, with the practices of hacking and coding providing excitement and stimulation (Goldsmith and Wall, 2019; Steinmetz, Schafer, and Green, 2017). Cybercrime communities provide spaces of community and shared identity, with much of the activity involving simply 'hanging out' with like-minded young people. Financial gain is a motive for some - however, while the small amounts of money made through basic scams and illicit businesses may appear enticing to teenagers, this rarely evolves into long-term financial means. In general, while a few talented individuals specialise in particular forms of crime and become part of cybercrime 'supply chains' and supportive networks of services, most engage in 'cafeteria-style' (Leukfeldt and Holt, 2021) offending, flitting between different forms of petty online crime and rarely 'cashing out' in stable long-term assets.

Desistance from cybercrime is generally conceptualised by law enforcement (with some justification) as repurposing the same skills but for ‘legitimate’ work for private security companies and the spy agencies - the ‘poacher turned gamekeeper’ narrative. From the available evidence, there is a clear pathway for those who have the technical skills and motivation not to simply ‘age out’, and who are able to avoid being caught, for a transition to state security services or the well-paid world of information security. For others, this is less clear, as most involved in cybercrime lack even the basic skills necessary for an entry-level IT job. As with ‘traditional’ crime, most people appear simply to age out, desisting due to life changes or boredom.

As early scholarship tried to come to terms with cybercrime as an apparently novel phenomenon, it asked whether cybercrime is simply ‘old wine in new bottles’ (Grabosky, 2001): a digital form of juvenile delinquency well-known to criminologists (Yar, 2005). Some cybercrime displays subcultural qualities, however this is complicated by the interpenetration into this ecology of state security services, and organised crime. The massive disruptive power of digital infrastructure is a complicating factor - facilitating far more extensive and complex forms of crime, harm, and deviance with legitimate services which can be co-opted for harm, or illicit infrastructures which can be bought as a service. In many ways, however, the classic structural conditions for harm still pertain. Thus, we argue for a critical reappraisal of state-focused ideas of cyber-‘criminality’ - many of which criminalise legitimate forms of technical experimentation, hacking and research, stigmatise young people engaged in petty online deviance (Lavorgna, 2019), and focus on criminal justice responses to crime rather than addressing structural issues.

Interventions, governance, and control

Policing the (post-)neoliberal Internet

The policing of the Internet has long reflected the neoliberal politics dominant in the US and Europe in the 1990s and 2000s. In this period, the commercialisation of the World Wide Web accelerated the Internet’s spread around the world and its increasing use by business and the general public. US politicians and policymakers explicitly saw the spread of the Internet as part of post-Cold War global economic and social liberalisation, with former president Bill Clinton famously contending:

> “Liberty will be spread by cell phone and cable modem… We know how much the Internet has changed America, and we are already an open society. Imagine how much it could change China…. Now there’s no question China has been trying to crack down on the Internet… Good luck. That’s sort of like trying to nail jello to the wall.”
>
> Bill Clinton, speaking in 2000, quoted in John Lanchester (2019)

This now seems naive, with an online landscape now shaped by two decades of the USA’s global War on Terror and the Internet emerging as a powerful technology of repressive control in a multitude of states, including both the USA and China (Lyon, 2014). However,

the ‘laissez faire’ approach to regulation which this thinking embedded in the early years of the commercial Internet has been important in structuring how law enforcement works online. Instead of a top-down hierarchy of state agenda-setting, cybercrime policing is *polycentric*, organised around loose coalitions of many different actors in the public and private sector, reflecting both its international character and the difficulty which police have had in ‘getting to grips’ with the Internet (DuPont 2017, 2018). This is also aligned with ideological commitments by a number of Western nations to free market, private sector provision of services, which overlapped at a crucial period with the values of the technical experts designing and expanding the global Internet in the 1990s - who were suspicious of centralised state control (Pickard, 2007; Chenou, 2014).

The policing of crime online, as a result, epitomises the neoliberal model - in which public goods such as security and justice are purchased on the free market by ‘responsibilised’ citizens who are expected to see to their own safety online. Rather than be protected by the state, the public buy their own antivirus software and security products, adopt their own defensive behaviours and measures such as passwords, and have little recourse to justice or compensation if these fail. Private companies are similarly expected to secure their own systems, which in practice means securing large quantities of sensitive data about their customers - who have little say in these security arrangements. This encourages a conceptual turn away from cybercrime as a ‘crime’ problem and towards a ‘security’ problem - which is not dealt with by the state, but by individuals and private companies. In this model, the state acts as a ‘steering, not rowing’ force, shaping market conditions indirectly through policy, law, and regulation and stepping in where the market fails. This is reflected in the wider *structural patterns* of cybercrime enforcement. Unlike for other forms of crime, in practice, power and priorities do not flow from the state - rather they circulate around complex international networks, in which the state and its representatives are only one node of many (Dupont, 2017).

Despite the apparent primacy of the free market, the neoliberal model relies on strong forms of state intervention and centralised repressive power to support and defend these free markets and the global economic and social conditions (and inequality) on which they rely. Cybercrime policing is no different - beneath the free market of private-public provision lies the hard power of the security services. In the post-9/11 world, more serious forms of online crime and harm are dealt with by the security services - part of an increasing penetration of ‘high policing’ techniques into the everyday management of crime (Brodeur, 2007). In the latter half of the 2010s, the governmentality of online law enforcement has shifted considerably towards muscular state regulation, with law enforcement and governments moving to centre themselves and their agendas in these relationships. States are imposing stronger regulation and responsibilities on the dense networks of intermediaries - payment companies, social media platforms, etc. - on which the Internet is built. Although online policing is still a network of private and public partners, states are increasingly attempting to centre themselves in these partnerships, co-opting the Internet infrastructure as a technology of control.

Police and cybercrime

The decentralised multi-agency structure of cybercrime policing is a matter of government philosophy, but is also shaped by the practical realities of cybercrime. For traditional police, cybercrime poses a range of challenges which mean they are rarely the 'go-to' authority for responding to online harm. Of primary relevance is how cybercrime complicates the principles of *sovereignty* and *jurisdiction* on which policing is founded. For 'traditional' crime, the assumed co-presence of victim and offender at the moment of a criminal act means jurisdiction is generally straightforward (with exceptions, such as threatening or libellous communications, or situations like those depicted in popular Nordic Noir series *Broen*, where a crime occurs on the bridge connecting Sweden and Denmark). However, cybercrimes can often be initiated in one country, with victims, platforms and intermediating infrastructure all located in different jurisdictions.

This means complex and expensive co-ordination between authorities is required to procure evidence, to apprehend an offender, to decide on which jurisdiction they should be tried in, and to bring a successful court case. This occurs through established links between jurisdictions (often mediated by centralised law enforcement agencies), through international collaborative bodies like Interpol, or specialist co-ordination groups themed around particular issues, such as child abuse. Where any technological or human link in this chain occurs in a country with weak international ties to the others, as is often the case for cybercrimes originating in jurisdictions hostile to the USA, it can be near-impossible to begin an investigation, let alone have a realistic prospect of finding or extraditing a suspect. Over time, this means the technical infrastructure and human organisations which drive serious cybercrime have concentrated in particular jurisdictions, making intervention difficult through normal channels.

Beneath this web of international cooperation (or its lack) lie a range of further challenges. Investigating online crime requires serious technical skill and relationships with Internet intermediaries and other jurisdictions. Police recruitment and training, along with laws, processes, and practices are still in many ways rooted in a pre-digital era, although this is beginning to change. Rather than establish these capacities individually in dozens of local police forces, the tendency has been to centralise them in specialist agencies (Wall 2007; Harkin and Whelan, 2021) or enrol private security and forensic consultancies.

The lack of a clear role for the police, the reframing of cybercrime as a 'security' problem, and the persistent responsibilisation of victims, means people do not know where to report crime, or may not be taken seriously when they do. Issues with recording and reporting mean official records of cybercrimes are likely to be significant underestimates. Victimisation can take different forms than for other kinds of crime - in some cases, people may not know they have been targeted, while in others, hundreds of thousands of accounts can harass a single person. The forms of harm and victimisation produced by cybercrime are not necessarily novel in themselves (often following classic patterns, e.g., gendered violence), but can be realised in novel ways. The victim of a harassment campaign is often advised by police to either leave online life altogether (impossible for many) or to adopt exhaustive and complex operational security techniques to avoid being victimised. Equally, victims are often told by the police they are one of many people targeted by a single fraud gang - which police

may not be able to adequately explain - and due to jurisdictional issues, there is nothing they can do (Cross, 2020). Generally, the belief of most low-level cybercrime actors they are largely safe from police action has often been a correct one.

Thus, the police role has often been relegated to information-gathering for the security agencies, responsive work with victims, and awareness-raising through public messaging campaigns. However, there is increasing evidence these campaigns fail to meet objectives, framed as they are in top-down, one-size-fits-all modes, which belie how privacy and security needs vary between communities, cultures, and places - and are collectively, rather than individually, produced (Horgan, 2021; Lewis, 2018).

Cybercrime and high policing

The increasing construction of cybercrime as national security threat, particularly in the years since 9/11, has seen the security agencies take on a role in targeting the most serious, often nation-state backed, forms of cybercrime. The ‘Five Eyes’ nations - the US, UK, Australia, Canada, and New Zealand - play an international role in sharing intelligence on threats, co-operating in surveillance of the Internet backbone. The ‘high policing’ of the Internet is a crucial aspect of global politics and control over the Internet - both as a means for spreading information through *soft power* and through dominating and surveilling communications in support of *hard power*.

The USA is a central actor in shaping the global Internet, and as a result, the 9/11 attacks were foundational in reshaping how the Internet was policed. There was an enormous expansion of domestic and international surveillance by the Five Eyes nations - as documented in leaks by NSA contractor Edward Snowden in 2013. From a 1990s ‘anonymous’ Internet, we now face an Internet which carries and records traces of all of our most intimate social interactions, and which is able to store these for the purposes of surveillance. With the cooperation of Internet Service Providers and other platforms and intermediaries, this gives the state an unprecedented capacity for mass surveillance, assisted by ‘machine learning’ algorithmic approaches for processing huge quantities of data. That Snowden was employed by a private sector security company, yet still had access to these flows, is evidence of a continuing and complex relationship between government and the free market in how high policing is carried out.

Under the spy agencies, centralised law enforcement bodies such as the FBI and NCA engage in their own high-profile attempts to disrupt online crime. Aside from high-profile arrests, agencies engage in a range of proactive policing measures, as well as assisting incident response and investigation for high profile attacks. Traditional approaches, such as arrests and sentencing, tend to be less effective for online crime networks, with replacements or competitors filling the vacuum rapidly, and crackdown tactics stimulating community solidarity (Ladegaard 2019). Proactive disruption of technical or social infrastructure - such as taking down forums, messing with reputation systems, hitting hosting providers, payment systems, and hardening security for potential targets all appear to be more effective, again, requiring the co-opting of licit and illicit infrastructure. More recently, agencies have adopted softer approaches - such as ‘influence’ policing involving

diversionary targeted advertising campaigns, and direct diversion (the poacher-turned-gamekeeper model) but also wider PREVENT-style campaigns borrowed from counterterrorism (Collier et al., 2020).

Private sector security

With the eyes of police and the security services trained on ‘high policing’ threats, more mundane (but still harmful) forms of cybercrime and online fraud proliferate, and individuals and companies are often left to purchase their own security privately. This can involve personal protection for individuals through technologies such as antivirus and password managers, the adoption of security behaviours or the purchase of insurance. For medium and large businesses, security is explicitly a product - either needing to be provided as a ‘cost centre’ within the organisation or purchased from a range of private sector providers. These companies can provide direct security for their customers, deploying security products, testing defences through ‘red team’ offensive hacking (or ‘penetration testing’) and provide ‘blue team’ counter-hacking services to protect networks actively. Further services are based around intelligence gathering, with companies like Flashpoint creating fake identities to infiltrate crime groups and forums and sound the alarm if a company’s data is put up for sale. For large corporations, there exist a range of major players providing ‘mission control’ style full-service cybersecurity.

While many governments lack the ability to cultivate the surveillance infrastructure of the Five Eyes Nations (and within nation states, access to such infrastructure may be restricted to security services), a range of private sector providers have emerged as a global market for nation states looking to purchase these capacities for themselves. These consultancies build a security or surveillance infrastructure once then sell it off-the-shelf to multiple nations. These provide ‘governmentality-as-a-service’, providing the data infrastructures for digital government to nation states, but also incorporating advanced tracking and surveillance tools (e.g. Palantir, NSO Group). These services have been controversial and are associated with serious human rights abuses.

Infrastructures and platforms

Finally, the Internet infrastructure provides a dizzying array of technical sites and actors through which crime is governed. Online communication of all kinds is dependent on intermediaries - e.g., Internet Service Providers filter traffic passing through their systems (Kohl, 2012). At the lowest level, the private companies and collaborative bodies responsible for the wires, servers, cables, and modems which allow the Internet to work are a crucial ‘control point’ for governments as they carry and view all web traffic (DeNardis and Musiani, 2016). A substantial amount of online crime is policed by intermediaries at this deep technical level, with the use of blocklists and scanning to semi-automatically weed out suspicious traffic. Over time, industry organisations and collaborative bodies have sprung up to coordinate this work as a public good, sharing lists of harmful domains associated with

cybercrime which should be blocked. This is one of the levels at which access to raw Internet traffic is provided to the security services.

Above the level of the ‘bare metal’, a range of other intermediaries, platforms, and service providers police their own areas of the Internet. The contemporary Internet is typified by a platform model - rather than hosting our own websites and homepages, we browse and upload on centralised sites which aggregate content, process transactions, advertise products, and give us an online presence. These intermediaries span the globe, and after years of attempting to appear as ‘neutral service providers’, a range of scandals have propelled them to the frontline of policing, taking more responsibility for crime and abuse on their own networks and services. This occurs both through design innovation - finding automated ways to reduce or detect illicit activity - and through the more expensive processes of manual human review, with content moderators emerging as a new exploited class of digital worker. In taking this role, the platforms have accrued substantial political power (Myers West, 2018).

Current controversies and critical futures of cybercrime within criminology

We welcome the inclusion of this new chapter in the Oxford Handbook - this reflects the increasing importance of cybercrime as a criminological phenomenon and the increasing maturity of cybercrime studies as a subfield within broader criminological scholarship. We have aimed to summarise the key scholarship on cybercrime over the last twenty years, and to chart its emergence as a criminological subfield. In the final section, we map potential futures of the study of cybercrime within criminology.

The empirical project of ‘cybercrime studies’ or ‘cybercriminology’ began with a frantic effort to document new forms of crime, social developments, and control strategies. This has now stabilised, with cybercrime reaching the ‘steady state’ characteristic of other forms of crime (Anderson et al., 2019). Although the marketing arm of the security industry continues to ‘discover’ new crimes, attacks, or vulnerabilities, these increasingly constitute new spins on existing, well-understood forms, with genuinely novel developments rare, niche, or overstated. There is fertile empirical ground in the continuing development of links between cybercrime academics and security academics - reflecting the broader interdisciplinary character of criminology. The security industry conducts advanced research on new forms and structures of criminal phenomena, with findings emerging from the frontlines of practice often running alongside or ahead of academic work (see further reading). However it is important that criminologists understand where this knowledge has come from – paying critical attention to the ideas and motivations behind it.

Cybercrime studies are breaking new frontiers in novel forms of empirical work, drawing on the very large datasets which online forums, chat channels, and social media make available. By bringing in ‘big data’ techniques to study online traces (Hughes, Chua, Hutchings 2021) a range of new studies are attempting to analyse discourse, practice, and culture in online spaces at scale. Other forms of Internet measurement, in collaboration with

computer scientists, give rise to opportunities to study natural experiments and Randomised Control Trial-like designs to measure traces of crime and evaluate interventions. However, there is a continuing need for more qualitative work, particularly on contemporary cybercrime communities. As policing cybercrime becomes more interventionist, there will be more to study and evaluate.

Despite almost three decades of study, criminology has yet to integrate an account of digital technology - particularly the rich and complex technologies of the Internet - in its core work of developing theorisations of crime, deviance, harm, or government power. Cybercrime scholarship is dominated by Routine Activities Theory, but this often paints a frustratingly deterministic account of technological change, with technologies existing outside social life and shaping it unidirectionally. Perspectives from Internet studies, digital sociology, and Science and Technology Studies are slowly being incorporated, but much of this work draws on theories of society and technology from the 1980s. Despite a paper by Brown (2006) which set the scene for an STS renaissance within cybercrime scholarship, there is still a dearth of critical scholarship on the role played by technology in online crime and power. There is some promising work using Actor Network Theory to account for the role of technologies in contemporary theorisations of crime, but this focuses on the agency of technological actors (or 'actants') within criminal situations, and nuances, rather than challenges, dominant situational and RAT framings (van der Wagen 2018). Other developments of STS theories within non-cybercrime criminological scholarship also point towards potential fruitful avenues (particularly the rich scholarship of Armstrong (2017) which develops links with visual criminology and Crockett Thomas' (2020) exploration of crimes as assemblages). Recent scholarship has also used interactionist frameworks, such as social worlds theory, to understand crime and power in digital infrastructures and link these to interactionist accounts of crime, or to governmentality scholarship. However, this remains an under-explored domain.

More critical perspectives on the *criminal* aspects of cybercrime scholarship have also begun to emerge in recent years, notably through authors such as Steinmetz (2016), who draw on the radical tradition in criminology. The cybercrime subfield has additional potential for critical criminologists to look beyond governmental power - large online corporations increasingly exert more, and different kinds of, power online than many governments. This suggests the potential for fruitful collaborations with zemiology and its radical reimagining of harm, rather than crime, as at the centre of critical criminological enquiry. Additionally, while subcultural and desistance framings have proven useful in sketching the initial foundations of theoretical work on cybercrime, there remain important critiques from the post-subcultural and critical desistance literature which could shed welcome new light on these areas.

The next era of cybercrime scholarship is faced with the same choices as many other subfields of criminology - namely, its orientation to and relationships with the state and private security, where the lens of enquiry is trained, how knowledge is produced, for whom, and to what end. A truly critical criminology of cybercrime might focus more on a critique of power and policing, new networked modalities of control, the role of infrastructural power, and the rise of online reactionary movements. What radical anticolonial scholars have to tell us about the links forming between the policing of cybercrime and the development of the neocolonial security state remains largely unexplored. How can the work of Angela Davis, Stuart Hall, Paul Gilroy, contribute to our understanding of the state's mobilisation of

nationalism, crisis, punishment, race, and power in controlling the Internet? What do police abolitionists have to tell us about how police work is reconfiguring to investigate online offences, and what communities might do to prevent crime? We might find possibilities of productive exchange with the pioneering work of feminist and queer scholars of the Internet, with digital anthropologists, social movement scholars, activist movements, and others whose work on online harms is in some ways more developed than our own. While criminology's focus on state-regulated harms and control projects gives us our own unique contribution to these debates, we would do well to resist the temptation to establish cybercriminology as the core site of knowledge about crime and harm in digital societies. We contend instead that, with criminologists as one perspective among many, these collaborations might form the seeds of an optimistic future for the criminology of cybercrime.

Further reading

Grugq. (2022). Grugq's domain. https://gru.gq/
Krebs, B. (2022). Krebs on Security. https://krebsonsecurity.com/
Security Research, Computer Lab, University of Cambridge. (2022). Light Blue Touch Paper. https://www.lightbluetouchpaper.org/
Violet Blue. (2022). Violet Blue - Journalist. https://www.engadget.com/about/editors/violet-blue/

Bibliography

Abbate, J. (2012). Recoding gender women's changing participation in computing. Cambridge, Mass.: MIT Press.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. *Workshop on Economics and Information Security (WEIS19)*, Boston, 3-4 June.

Armstrong, S. (2017). Seeing and seeing-as. *Routledge International Handbook of Visual Criminology*, 416.

Atondo Siu, G., Collier, B., & Hutchings, A. (2021). *Follow the money: The relationship between currency exchange and illicit behaviour in an underground forum*. Proceedings of the 6th IEEE European Symposium on Security and Privacy Workshop on Attackers and Cyber-Crime Operations, virtual event.

Bada, M., Chua, Y. T., Collier, B., & Pete, I. (2021). Exploring masculinities and perceptions of gender in online cybercrime subcultures. In *Cybercrime in Context* (pp. 237-257). Springer, Cham.

Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society*, *20*(4), 497-512.

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets*(* but were afraid to ask). *International Journal of Drug Policy*.

Bidgoli, M., & Grossklags, J. (2017). "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. In *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 57-69). IEEE.

Brodeur, J. P. (2007). High and low policing in post-9/11 times. *Policing: A Journal of Policy and Practice*, *1*(1), 25-37.

Brooke, S. J. (2021). Trouble in programmer's paradise: gender-biases in sharing and recognising technical knowledge on Stack Overflow. *Information, Communication & Society*, 1-22.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223-244.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Chua, Y. T., & Collier, B. (2019). Fighting the "blackheart airports": internal policing in the Chinese censorship circumvention ecosystem. In *2019 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-9). IEEE.

Clarke, R. V. (1995). Situational crime prevention. *Crime and justice*, *19*, 91-150.

Cohen, J. E. (2007). Cyberspace as/and Space. *Colum. L. Rev.*, *107*, 210.

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books.

Coleman, E. G. (2012). *Coding freedom*. Princeton University Press.

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2021). Cybercrime is (often) boring: infrastructure and alienation in a deviant subculture. *The British Journal of Criminology*.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2021). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, 1-22.

Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019). *Booting the Booters: Evaluating the effects of police interventions in the market for denial-of-service attacks*. Proceedings of the ACM Internet Measurement Conference, Amsterdam.

Crockett Thomas, P. (2020). Crime as an assemblage. *Journal of Theoretical & Philosophical Criminology*.

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice*, *5*(2), 120-131.

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, *20*(3), 358-375.

DeNardis, L., & Musiani, F. (2016). Governance by infrastructure. In *The turn to infrastructure in Internet governance* (pp. 3-21). Palgrave Macmillan, New York.

De Souza e Silva, A. (2006). From cyber to hybrid: Mobile technologies as interfaces of hybrid spaces. *Space and culture*, *9*(3), 261-278.

Dupont, B. (2017). Security in the Age of Networks. In *Crime and Security* (pp. 79-94). Routledge.

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, law and social change*, *67*(1), 97-116.

Dupont, B. (2018). The global anti-cybercrime network: Mapping the polycentric regulation of online harms. In *Criminal Justice and Regulation Revisited* (pp. 163-185). Routledge.

Felson, M. (2008). A routine activity approach. In R. Wortley & L. Mazerolle (Eds.), *Environmental Criminology and Crime Analysis* (pp. 70-77). Collumpton: Willan Publishing.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. London: Pearson Education Limited.

Gibson, W. (1984). *Neuromancer*. Routledge.

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112-130.

Goldsmith, A., & Wall, D. S. (2019). The seductions of cybercrime: Adolescence and the thrills of digital transgression. *European Journal of Criminology*, 1477370819887305.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles?. *Social & Legal Studies*, *10*(2), 243-249.

Harkin, D., & Whelan, C. (2021). Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management*, 14613557211036565.

Hodge, E., & Hallgrimsdottir, H. (2020). Networks of hate: the alt-right,"troll culture", and the cultural geography of social movement spaces online. *Journal of Borderlands Studies*, *35*(4), 563-580.

Holt, T. J., Navarro, J. N., & Clevenger, S. (2020). Exploring the moderating role of gender in juvenile hacking behaviors. *Crime & Delinquency*, *66*(11), 1533-1555.

Horgan, S. L. (2021).The reality of 'cyber awareness': Findings and policy implications for Scotland. *SCCJR Justice Fellowship briefing paper*

Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology*.

Hughes, J, Chua, Y. T., & Hutchings, A. (2021). Too much data? Opportunities and challenges of large datasets and cybercrime. In A. Lavorgna & T. J. Holt (eds.), *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*. Oxon: Palgrave Macmillan.

Hutchings, A. (2018). Leaving on a Jet Plane: The trade in fraudulently obtained airline tickets. *Crime, Law and Social Change, 70*(4), 461-487.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*(10), 1163-1178.

Hutchings, A., & Clayton, R. (2017). Configuring Zeus: A case study of online crime target selection and knowledge transmission. In *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 33-40). IEEE.

Hutchings, A., & Chua, Y. T. (2016). Gendering cybercrime. In *Cybercrime through an interdisciplinary lens* (pp. 181-202). Routledge.

Hutchings, A. & Collier, B. (2019). *Inside out: Characterising cybercrimes committed inside and outside the workplace*. Proceedings of the 4th IEEE European Symposium on Security and Privacy Workshop on Attackers and Cyber-Crime Operations, Stockholm.

Hutchings, A. & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*(3), 596-614.

Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, *9*(1), 1-15.

Karami, M., Park, Y., & McCoy, D. (2016). Stress testing the booters: Understanding and undermining the business of DDoS services. In *Proceedings of the 25th International Conference on World Wide Web* (pp. 1033-1043).

Kohl, U. (2012). The rise and rise of online intermediaries in the governance of the Internet and beyond–connectivity intermediaries. *International Review of Law, Computers & Technology*, *26*(2-3), 185-210.

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, *63*, 113-121.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lavorgna, Anita (2019) Cyber-organised crime. A case of moral panic? *Trends in Organized Crime*, 22 (4), 357-374.

Leukfeldt, R., & Holt, T. J. (2021). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, 106979.

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Garden City: Anchor Press/Doubleday.

Lewis, S J. (2018). Queer Privacy. Lulu.com.

Light, J. S. (1999), When computers were women. Technology and Culture, 40(3), 455-483.

Lim, A., Brewer, N., & Young, R. L. (2021). Revisiting the Relationship between Cybercrime, Autistic Traits, and Autism. *Journal of Autism and Developmental Disorders*, 1-12.

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: a qualitative study. *Security Journal*, *32*(2), 102-118.

Mirian, A., DeBlasio, J., Savage, S., Voelker, G. M., & Thomas, K. (2019, May). Hack for hire: Exploring the emerging market for account hijacking. In *The World Wide Web Conference* (pp. 1279-1289).

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140).

Messerschmidt, J. W. (2005). Men, masculinities, and crime. *Handbook of studies on men & masculinities*, 196-212.

Miramirkhani, N., Starov, O., & Nikiforakis, N. (2016). Dial one for scam: Analyzing and detecting technical support scams. In *22nd Annual Network and Distributed System Security Symposium (NDSS* (Vol. 16).

Myers West, S. (2018). Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms. *New Media & Society, 20*(11), 4366-4383.

Nafus, D. (2012). 'Patches don't have gender': What is not open in open source software. *New Media & Society*, *14*(4), 669-683.

Pastrana, S., Thomas, D. R., Hutchings, A., & Clayton, R. (2018). *CrimeBB: Enabling cybercrime research on underground forums at scale*. Proceedings of the ACM International World Wide Web (WWW) Conference, Lyon.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1), tyz003.

Porcedda, M. G., & Wall, D. S. (2019). Cascade and chain effects in big data cybercrime: Lessons from the TalkTalk hack. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 443-452). IEEE.

Marganski, A. J. (2020). Feminist theories in criminology and the application to cybercrimes. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 623-651.

Sauter, M. (2014). *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the Internet*. Bloomsbury Publishing USA.

Simoiu, C., Zand, A., Thomas, K., & Bursztein, E. (2020). Who is targeted by email-based phishing and malware? Measuring factors that differentiate risk. In *Proceedings of the ACM Internet Measurement Conference* (pp. 567-576).

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime* (Vol. 2). NYU Press.

Steinmetz, K. F., Schaefer, B. P., & Green, E. L. (2017). Anything but boring: A cultural criminological exploration of boredom. *Theoretical Criminology*, *21*(3), 342-360.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly, 33*(5), 890-911.

Tuptuk, N., & Hailes, S. (2018). Crime in the age of the Internet of Things. In *Routledge Handbook of Crime Science* (pp. 288-308). Routledge.

Vasek, M., & Moore, T. (2015). There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In *International conference on financial cryptography and data security* (pp. 44-61). Springer, Berlin, Heidelberg.

van der Wagen, W. (2018). The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 157-178.

Vu, A. V., Hughes, J., Pete, I., Collier, B., Chua, Y. T., Shumailov, I., & Hutchings, A. (2020). *Turning up the dial: The evolution of a cybercrime market through set-up, stable, and COVID-19 eras.* Proceedings of the ACM Internet Measurement Conference, Pittsburgh.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183-205.

Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J. L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life-Course Criminology*, *4*(3), 343-364.

Wortley, R. (2010). Critiques of situational crime prevention. Sage Publications, Inc.

Wylie, C. (2019). *Mindf*ck: Inside Cambridge Analytica's plot to break the world*. London: Profile Books.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. Sage.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.