# Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies

Ben Collier[1], Richard Clayton[1], Alice Hutchings[1], Daniel R. Thomas[2]

[1] Cambridge Cybercrime Centre, Department of Computer Science & Technology, University of Cambridge, UK
[2] University of Strathclyde, UK

**Abstract**

It is generally accepted that the widespread availability of specialist services has helped drive the growth of cybercrime in the past fifteen to twenty years. Individuals and groups involved in cybercrime no longer need to build their own botnet or send their own spam because they can pay others to do these things. What has seldom been remarked upon is the amount of tedious administrative and maintenance work put in by these specialist suppliers. There is much discussion of the technically sophisticated work of developing new strains of malware or identifying zero-day exploits but the mundane nature of the day to day tasks of operating infrastructure has been almost entirely overlooked. Running bulletproof hosting services, herding botnets, or scanning for reflectors to use in a denial of service attack is unglamorous and tedious work, and is little different in character from the activity of legitimate sysadmins. We provide three case studies of specialist services that underpin illicit economies and map out their characteristics using qualitative sociological research involving interviews with infrastructure providers and scraped data from webforums and chat channels. This enables us to identify some of the distinct cultural and economic factors which attend this infrastructural work and to note, in particular, how its boring nature leads to burnout and the withdrawal of services. This leads us to suggest ways in which this new understanding could open novel avenues for the disruption of cybercrime.

## 1 Introduction

Cybercrime is often depicted as an alternative pathway to an otherwise dreary career in our industrialised societies. Indeed, the early days of cybercrime were characterised by small numbers of high-profile individuals who committed lucrative crimes, and were romanticised by the media as defiant, highly skilled, and posing an existential threat to contemporary society. In this paper, we argue that cybercrime, which is now a volume crime (Anderson et al., 2019), has itself become industrialised, with boring, tedious maintenance and infrastructure jobs outsourced to lowly paid contractors.

Criminological research has often tended to view cybercrime (and crime more broadly) as driven by either economic rationales (Kshetri, 2006; Moore, Clayton, & Anderson, 2009), by the pursuit of cultural capital within deviant online subcultures (Holt, Brewer, & Goldsmith, 2019; Holt, 2019), or by the allure of the experience of these illicit activities (Katz, 1988; Goldsmith & Wall, 2019). The pursuit of the 'hacker ethic', the thrill of online deviance, the joy of creative experimentation, and the formation of a deep relationship with complex technological work has been a key aspect of much of the criminological literature on cybercrime (Yar, 2005b; Holt, 2007; Steinmetz, 2016). The actors whose motivations, behaviours, and decision-making are considered by criminologists, security economists, and cybercrime researchers tend as a result to be those involved in active, prominent roles: researching vulnerabilities, compromising systems, and performing key functions within cybercrime groups (Benjamin & Chen, 2012). However, these romantic notions of those involved in cybercrime ignore the often mundane, rote aspects of the work that needs to be done to support online illicit economies.

There exists a fairly well-established working model of cybercrime economies focused around tool development and skill-sharing (Hutchings, 2014; Hutchings & Clayton, 2017). This essentially hierarchical understanding of cybercrime economies posits a 'core and periphery' social structure, whereby a very small community of highly-skilled actors develop exploits and vulnerabilities into tools, which are then sold to and used by much larger communities of lower-skilled actors, often known as 'script kiddies' or 'skids' (Johnson & Powers, 2005; Wall, 2007). While this model has a great deal of value for making sense of some of the dynamics of these communities, we now argue that it misses out important aspects of how these illicit economies have developed over time.

We present in this paper a study of cybercrime economies which extends this standard model to highlight the increasingly important role of shared, purpose-built illicit infrastructure. This brings to the fore some of the less glamorous aspects of cybercrime – the many different types of often-tedious, but nonetheless important, hidden work performed by low-skilled actors which supports these infrastructures and allows illegal markets to operate on a much larger scale.

The past two decades have seen the structures of cybercrime economies changing substantially. This is often described as a shift to subscription- and platform-based 'cybercrime-as-a-service' business models (Manky, 2013; K. Thomas et al., 2015; Hutchings & Clayton, 2017; Hyslip & Holt, 2019; Noroozian et al., 2019). This has generally been accompanied by a technological shift in these economies, facilitated by shared illicit infrastructures, such as botnets, bulletproof hosting, and illicit markets, among others. Sometimes this shift has come from generic economic pressures – the economies of scale, the advantages of specialisation – and has often led to areas of concentration which may or may not indicate viable intervention strategies (Clayton, Moore, & Christin, 2015). However, sometimes these shifts have resulted from externalities. For example, Hutchings and Clayton (2017) describe how the leak of the Zeus source code meant the sale of the crimeware became unprofitable, leading to 'Zeus-as-a-service' as an alternative monetisation strategy.

As these shared illicit infrastructures have begun to emerge, there has been a change in the kind of work involved in cybercrime economies. We argue that, for many people involved, cybercrime is boring: an office job sustaining the infrastructure on which these global markets rely. In this paper, we seek to bring to life these shared infrastructures and hidden forms of work and their importance, reflecting on the crucial supportive role which they play in cybercrime economies. First, we discuss current representations of cybercrime economies within criminological and security scholarship. Then, we extend this to include the roles played by shared illicit infrastructures, drawing on frameworks from Susan Leigh Star's infrastructure studies research (Star, 1999). After discussing our methodological approach, we then outline three case studies that illustrate the pivotal role played by shared infrastructures in scaling up illicit online economies. We then draw these together into a framework of key characteristics of illicit infrastructures and of the work required to sustain them. Finally, we reflect on the implications of our findings for broader understanding of cybercrime economies, and explain how this new framing might lead to new styles of intervention to disrupt them.

## 2 Tools and skills: the mainstream view of cybercrime

The typically-conceived picture of cybercrime actors in the research literature from the 1990s onwards has focused on the idea of the 'hacker'. Indeed, much criminological scholarship has used the terms hacking and cybercrime interchangeably. We much prefer to separate these terms, with 'hacking' a set of practices and cultural sensibilities relating to obscure tinkering, technological exploration, engagement in law-making around technology, the creation of novel 'rebel infrastructures', political tool-breaking, and civil disobedience (Levy, 1984; Coleman, 2017). These activities, although often portrayed as 'deviant', are not necessarily illegal. In contrast, many of the illegal online activities which constitute cybercrime require little technical creativity or skill, and have tenuous links to the rich subculture which surrounds hacking. Much cybercrime scholarship elides the broader aspects of 'hacking', and as a result, the portrayal of those who commit cybercrime as hackers has impacted how cybercrime has been understood by researchers and policymakers. We believe this conflation of the two communities has

contributed to romanticised notions of the capabilities, the skills and some of the motivations of those who take part in cybercrime.

Criminologists have generally framed cybercrime using two distinct theoretical approaches – one sub-cultural and the other economic/opportunistic. Sub-cultural accounts stress the existence of online communities where skills and cultural norms can be learned, focusing on hacking as a subcultural pursuit with a distinct ethic and set of associated practices (Yar, 2005a; Turgeman-Goldschmidt, 2011). This often draws upon sociological findings from hacker groups not involved in illegal activities (such as local computer clubs), using these results to attempt to understand the technical communities involved in cybercrime (Steinmetz, 2016). The economic/opportunistic approaches make sense of cybercrime by focusing more on material situations and technological affordances, as well as the costs and benefits of cybercrime to those who commit it (Yar, 2005b; E. R. Leukfeldt & Yar, 2016).

The two approaches lead to differing policy implications, with the first focusing on interventions within places and communities, and the latter emphasising traditional situational crime prevention approaches, such as target hardening, increasing effort and risk, and decreasing profit (Brewer et al., 2019). According to the sub-cultural view, the economic approach of increasing skill barriers through target hardening and increasing risk through arrests (to increase the perceived costs for potential new entrants) may actually lead to increased offending, due to higher 'street cred' from success, reduction of the police's perceived legitimacy, political defiance, or merely the love of a challenge (Ladegaard, 2019). Being involved in illicit behaviour may be seen as a 'badge of honour' (Hodgkinson & Tilley, 2007), glamorising the outsider status of illegal activities, or reinforcing a sense of outsider group identity (Becker, 1963). Similarly, increasing the perception of the risk associated with cybercrime may lead it to be perceived as more exciting, and the 'forbidden fruit effect' (Grabosky, 1996) may even entice new actors into trying out illicit behaviours.

In terms of organisation, the 'classic' model of cybercrime communities has moved from a 1980's view that cybercrime is committed by highly-skilled individual actors (demonised as 'superusers' (Ohm, 2008)) to a more top-down, or concentric, view of large subcultures of 'script kiddies' clustered around small numbers of genuinely skilled individuals (Hutchings, 2014). Cultural capital in the underground hacker scene is still very much linked to the cultivation of technical prowess (sometimes known as 'l337' or 'elite' status). A (very) small core of actors actually develop exploits, a slightly wider group package up, monetise and distribute them, a large group of 'skids' use these packages and scripts, and yet larger groups (who aren't really technical at all) coalesce at the edges of these communities, purchasing services, running scams, performing other kinds of work (such as graphic design) and reselling products. This has been described in previous criminological research as the 'cyber kill-chain' (Porcedda & Wall, 2019). These communities have existed in a range of different online spaces, which have proven fruitful sites for criminological research (Holt, 2007; Yip, Webber, & Shadbolt, 2013; Hutchings, 2014; Shakarian, Gunn, & Shakarian, 2016; Pastrana, Thomas, Hutchings, & Clayton, 2018; Pastrana, Hutchings, Caines, & Buttery, 2018). Over time, driven by technological change, these online cybercrime spaces have moved from dial-up bulletin boards (Meyer, 1989) and IRC channels (R. Thomas & Martin, 2006) to web-based cybercrime forums (Pastrana, Thomas, et al., 2018), to open chat channels on Discord and Telegram (Kamps & Kleinberg, 2018), with actors maintaining a presence on social media channels such as Facebook and Twitter (C. Chen, Zhang, Xiang, Zhou, & Oliver, 2016; Holt, Bossler, & Seigfried-Spellar, 2017). While actors in these communities are perceived as responsible for high volume, low value/harm crimes, these are punctuated by small specialised groups or teams (who occasionally have links to state security services) who perform low volume, high harm attacks (R. Leukfeldt & Holt, 2019).

A wide set of motivations have been posited to explain participation in cybercrime economies. These revolve around the pursuit of profit, subcultural acclaim, social capital, and political goals (Holt, 2007; Turgeman-Goldschmidt, 2005; Workman, Phelps, & Hare, 2013; Yar & Steinmetz, 2019; Goldsmith & Wall, 2019). The perceived profits to be made may be an illusion created by overestimating the amount of cybercrime (Herley & Florêncio, 2010) or aspirational (much as drug dealers tend to live with their parents (Levitt & Venkatesh, 2000)). Importantly, these motivations are extended to include factors that are neither economic nor acquisitive – that persist regardless of failure, outlay, or risk. It is clear from

the extensive literature on the (often non-criminal) computer hacker culture that many take part in these activities primarily for the enjoyment and excitement of the process of re-purposing, experimenting with, and building computer systems and – when combined with political activism – society (Jordan & Taylor, 1998; Coleman, 2017). The motivations of those in hacker subcultures, for example, have been extensively studied by anthropologists, sociologists, and criminologists, and these (as will become clear) yield important insights for understanding these behaviours (Coleman & Golub, 2008; Steinmetz, 2016; Coleman, 2017).

However, there is one important aspect that has been largely neglected in prior research. This undue focus on excitement, glamour, and prestige comes at the expense of understanding the dull and tedious nature of much of the work in which these actors are engaged. Most previous criminological research that has explored boredom and anomie have framed them as an initiator for crime, particularly functionalist (Merton, 1938) and subcultural accounts of involvement in illicit economies, which frame crime as an exciting diversion from work or adolescence within the tedium of capitalist societies. Some work within cyber-criminology has explicitly used this to explain involvement in cybercrime communities (Steinmetz, 2016). Conversely, we argue that as these illicit economies have grown and become more formalised, so has much of the work involved become equally rote and tedious – the underground equivalent of an office job. While prior research has not examined in detail the boring, tedious and mundane aspects of cybercrime, Meyer's (1989) classic work on the social organisation of underground bulletin board systems noted:

> Pirated commercial software is very rare; any programs that are available are usually non-copyrighted specialized programs used to automate the more mundane aspects of phreaking or hacking.

Cybercrime communities effectively provide a tool/skill-sharing economy, where skill-sharing takes place through creation of tools, scripts, and methods which are packaged up and can be used by others with lower levels of technical skill, or through directly contracting services through one-to-one agreements. Entry to these communities is no longer limited to those with technical skill, but now allows in those with the resources to purchase services, sometimes on a subscription basis. While they may sound glamorous, providing these cybercrime services require the same levels of boring, routine work as is needed for many non-criminal enterprises, such as system administration, design, maintenance, customer service, patching, bug-fixing, account-keeping, responding to sales queries, and so on. In the following section, we discuss this service economy in more depth.

# 3 Mass-scale cybercrime and the transition to infrastructure

Although the service-based aspects of cybercrime economies, and the role played by specialisation, have been well-documented in the criminological and cybersecurity literature (Grier et al., 2012; Broadhurst, Grabosky, Alazab, & Bouhours, 2013; Manky, 2013; Lusthaus, 2018; Noroozian et al., 2019), we argue that a key element has been overlooked in this scholarship: these shared, purpose-built illicit infrastructures are themselves developed, supported and maintained only through a great deal of tedious and boring work by people with skillsets that are essentially the same as those who develop, support and maintain legitimate infrastructure.

Coleman's work on hacking extends the commonly-conceived idea of it being oriented solely around practices of creative breaking to include other kinds of work, such as the creation of new tools and infrastructures which subvert established technologies, means of social control, and social structures (Coleman & Golub, 2008; Coleman, 2017). Within cybercrime economies, these two kinds of work are connected. A clever exploit or vulnerability discovered in a computer system may be used by its creator in the commission of high-harm (and probably low-volume) crime. However, for a large-scale cybercrime economy to develop, these exploits have to be packaged up within an exploit platform and resold. It is then that the scale of harm becomes significantly extended, as the skill barrier to using these tools is substantially reduced (Porcedda & Wall, 2019).

However, much more is needed than merely offering to sell an exploit. There are skill, trust and funding barriers which inhibit the the development of truly mass-scale cybercrime economies. Buyers need to find sellers in scam-ridden underground communities, purchase often-expensive exploit kits, make them work properly, and successfully cash out any funds received or sell on stolen information. Substantial scale in illicit economies has generally only been achieved where communities have developed (and often rented out) shared illicit infrastructure, providing its capabilities as a service to prospective users, who then require no technical skill whatsoever.

Although this disintermediatation of the value chain has been widely discussed in the research literature with notable early work by Team Cymru (R. Thomas & Martin, 2006), this has tended to focus on the specialisation and compartmentalisation of cybercrime as a service economy (R. Leukfeldt & Holt, 2019) whilst the way in which the infrastructure is actually run has generally been overlooked. Where the infrastructure has been studied it has generally been to document what is available (Sood & Enbody, 2013), how to identify it (Konte, Perdisci, & Feamster, 2015) or computing the cost to society it engenders (Y. Chen et al., 2017). There has been little to no discussion as to how the rising importance of shared illicit infrastructures fundamentally transforms the kinds of work involved in cybercrime economies, and how it has created a wide range of administrative and maintenance jobs servicing these infrastructures.

In order to explore these under-researched forms of work and the crucial role played by these infrastructures in supporting cybercrime economies, we make use of a framework and set of approaches from Susan Leigh Star's (1999) infrastructure studies scholarship. Star's framing of infrastructure rests on nine key characteristics. Firstly, infrastructure is embedded in social relations and other structures, and its sub-units and component elements are often difficult to distinguish from one another to the outsider. It is also transparent to the user, meaning that it should ideally smoothly facilitate their actions with minimal friction, and the reality of how it actually works only becomes visible on breakdown – when it ceases to work smoothly. Infrastructure is necessarily broad in scope, extending beyond a single site or action to facilitate social action more broadly of different kinds and in different places. It is learned as part of the membership of a community: the ability to navigate and make use of shared infrastructure is a key part of 'fitting in' to subcultures and social groups, as is learning the conventions of practice associated with it. In its wider constitution, it embodies a set of standards, plugging into and linking with other technologies in a standardised fashion, and it is built on a pre-installed base, rather than from scratch, making use of existing infrastructures (such as the Internet itself) as a platform on which to build further capabilities. Finally, it is fixed in modular increments, rather than globally, and building or changing an infrastructure is by necessity piecemeal and complex, rather than top-down (Star, 1999).

This sociological conceptualisation of infrastructure is particularly useful in making sense of how shared illicit infrastructures change the character of work in cybercrime economies, guiding research to the interesting human and technical interrelationships which are important in supporting such infrastructures. For Star, infrastructure is not only a descriptive term for large-scale and extensive physical artefacts, but a *quality* in its own right: something achieved by work performed both by technologies and by the humans who attend to them (Star, 1999). Thus, a physical system such as the road network possesses the qualities of an infrastructure only when combined with the maintenance, administration, governance, and policing work which allows it to function smoothly and reliably for its users. Infrastructural studies research, therefore, involves studying both of these together, mapping the interactions between material technologies and human work which 'produce' the qualities of infrastructure for users; focusing on the technology or the people in isolation misses out key aspects of these phenomena.

In this paper, we use Star's framework as a guide to investigate and characterise the invisible work which supports cybercrime infrastructures. For criminological research into cybercrime, we argue that this approach has the capacity to unearth important, under-considered aspects of cybercrime economies, with implications for policy interventions and law enforcement approaches to online crime. The application of this approach to *illicit* infrastructures is of additional theoretical interest, as these infrastructures are purpose-built to facilitate a range of criminalised activities. The interactions between

Star's more general characteristics of infrastructure and the mechanisms of law enforcement intervention which illicit infrastructures face bring out a range of other important considerations, which we will explore.

# 4 Methods

In characterising and exploring illicit infrastructures and the work which supports them, we draw on two main qualitative data sources. The first data source is from interviews with individuals involved in the administration and maintenance of 'booter' services (which provide denial of service attacks for a fee). We also use the Cambridge Cybercrime Centre's *CrimeBB* dataset (Pastrana, Thomas, et al., 2018), obtained by scraping a range of online forums and chat channels used by communities involved in cybercrime, and made available to researchers through access agreements. Ethical approval was granted for both of these approaches. When making connections with other kinds of infrastructural work through our case studies, we also draw extensively on the research literature.

The research by Hutchings and Holt (2018) informed our strategies when interviewing participants involved in the administration and maintenance of 'booter' services. In total, eleven interviews took place, with some participants interviewed more than once, and some interviewed in small groups. Participants were recruited by posting requests on the websites and chat channels used by booter providers to manage their user communities. The initial goal of this research was to characterise the kinds of work and practices in which actors in these cybercrime economies were engaged. Interviews were conducted in a semi-structured, exploratory manner, with questions focused on the details of the particular *practices* and kinds of work through which the interviewees contributed to the cybercrime economy and how they felt about and understood them. The qualitative interviews were carried out with the assurance of anonymity for participants and under the principle of informed consent and with approval from our ethics review committee. As the interviews detail activities which are illegal in many jurisdictions, care has been taken to omit any identifying information in the analysis and illustrative quotes presented here which might potentially bring harm to participants.

Specialist online forums and chat channels (as we discuss below) are important sites for cybercrime communities, where people can buy and sell services and tools, learn cybercrime skills, develop networks of friends and collaborators, and internalise the norms, values, and cultural mores of the underground cybercrime subculture (Hutchings & Holt, 2015; Pastrana, Hutchings, et al., 2018). Many of these are publicly accessible, as the need to attract new entrants to these economies mandates keeping barriers to access as low as possible (at least for the kinds of low-level volume crime we discuss in this paper). The Cambridge Cybercrime Centre archives 25 of these community sites, with over 70M posts dating back as far as 2002.

Although informed consent has not been sought for the use of these data from the members of these forums, it has been well-established by decades of online sociological research that publicly available online data can, with careful consideration of ethical issues, be a suitable subject for research (British Society of Criminology, 2015; D. R. Thomas, Pastrana, Hutchings, Clayton, & Beresford, 2017). CrimeBB only includes data from publicly available forums, where there is a reasonable expectation that participants would be aware that their posts would be subject to public scrutiny. Furthermore, in order to mitigate any potential harm to members of these forums, we present only outputs referring to the characteristics and behaviours of populations, rather than individuals, and have removed any identifying information from the illustrative quotes used.

In terms of the analytical process, Star's research provides a set of 'tricks of the trade' (Star, 1999) for making sense of the different kinds of work involved in infrastructure and how they fit together. This facilitates deep explorations of the relationships between the human and technical elements of these systems and the complex ways in which they depend on one another, without unduly prioritising one over the other. In particular, Star suggests a focus on finding and bringing into the foreground the invisible work, such as design or maintenance, on which infrastructures depend. She additionally

argues that detailed study of the category systems (for example, of users, use cases, and adversaries) which are built in to these infrastructures can tell us a great deal about why they have been designed to work the way they do, the hidden fault-lines and dependencies within them, and their broader impact on society (Star, 1999).

Analysis of these data sources was conducted on an inductive, exploratory basis, with Star's infrastructural framework acting as a guide and series of 'sensitising concepts'. From our earliest interviews, Star's direction to focus on hidden work was a valuable lens. It became apparent that, when asked more generally about how they actually spent most of their time, the majority of our participants' time was spent on tedious supportive and maintenance work, which was crucial to the success of these economies. As this picture emerged, we set out to characterise this hidden work in depth: to establish its features and its place in cybercrime economies. This took place through inductively coding our interview data (using the NVivo qualitative coding software), which yielded a set of initial findings and codes which were used to drive the archival research on the webforums. Relevant discussions from these forums and chat channels, namely those which referenced supportive infrastructural work, were harvested using text search and coded inductively. The combination of these two rounds of inductive analysis led to the development of the higher-order categories around which the findings in this paper are structured. We present these below through three case studies of different cybercrime infrastructures, from which we draw out eight characteristic qualities of the supportive work on which this illicit infrastructure relies.

# 5 Purpose-built illicit cybercrime infrastructures: three case studies

By way of illustration, we will now discuss examples of purpose-built illicit infrastructures which fulfil a supportive function in three different cybercrime economies. We use these to highlight the importance of these infrastructures and the kinds of work on which they depend, using them to illustrate some of this work's core qualities on which we focus in more depth in the subsequent section. Although they are doubtless important, we do not consider here generic infrastructures built for legitimate purposes (such as online payment providers, social media sites, mail servers, Internet Service Providers, the Tor network, cryptocurrency infrastructure, or the broader Internet itself) which are being abused to facilitate crime. For the purposes of this paper, we only consider infrastructures built specifically for the purpose of illegal activity.

## 5.1 Botnets and booters

The first illicit infrastructure which we consider are botnets. These are networks of infected computer systems which are connected to the Internet and controlled by an attacker through a Command and Control (C&C) server. Attackers 'herd' this botnet by attempting to infect more machines, often running a separate server which scans for vulnerable computer systems on the open Internet (high-profile recent botnets have included Mirai, Kelihos, and Necurs), while attempting to avoid being detected and losing control of machines (Cooke, Jahanian, & McPherson, 2005; Silva, Silva, Pinto, & Salles, 2013; Kolias, Kambourakis, Stavrou, & Voas, 2017).

Botnets are an important part of the cybercrime ecosystem, and have a variety of illicit uses. They can be used to 'proxy' traffic, bouncing signals from their users to obfuscate their identity and location. They can also be used to launch a variety of different attacks, including Distributed Denial of Service (DDoS) attacks, where the infected computers are compelled to direct traffic to a victim, knocking them offline (Kolias et al., 2017; Wang, Chang, Chen, & Mohaisen, 2018), and spamming, where mailboxes are flooded with emails containing unsolicited advertisements, extortion attempts, or malware (Xie et al., 2008).

As the botnet ecosystem has grown, botnet owners have begun to monetise them directly, selling excess capacity to others. This has turned botnets into an infrastructure that can provide resources for people to use in attacks to a variety of ends, allowing access to these capabilities to those with very low or no technical skill. The market for DDoS services has seen particular growth with its facility for disrupting

online multiplayer gaming, becoming a market for 'booter' services used to disconnect opponents during competitive play (Santanna et al., 2015; Hutchings & Clayton, 2016; Karami, Park, & McCoy, 2016; Collier, Thomas, Clayton, & Hutchings, 2019).

The rise of the booter service is a particularly striking example of this turn to shared infrastructure in cybercrime economies. Originally, DDoS attained prominence in the public eye as a protest tactic (particularly associated with the Anonymous movement), where individuals from around the world would direct their own computers to send packets to knock services online as part of a digital sit-in (Jordan & Taylor, 1998; Coleman, 2014; Karanasiou, 2014), using tools such as the Low Orbit Ion Cannon (Sauter, 2013). As the Anonymous movement evolved, splinter groups began to use DDoS attacks for harassment or amusement, using their own botnets and other means of generating large amounts of traffic without mass participation. These 'trolling' sensibilities gained purchase in the online gaming community, which had long nurtured a minority interested in cheating and 'griefing' other players, leading to the growth of a market for these services for those who lacked the skills or risk appetite to manage their own botnet (Sauter, 2013). Denial of Service thus evolved from a low-volume, high harm crime, where small groups would launch DDoS attacks for political or personal reasons, to a mass market for cyberattack services, spreading these capabilities to a much wider range of actors who require no technical skill whatsoever to carry them out (Brunt, Pandey, & McCoy, 2017).

Although the 'infrastructure' of compromised machines is repurposed from existing (though badly configured) computer infrastructure, botnets require their own hosting for control panels that track the constituent machines, issue commands, upload new payloads and generally maintain the botnet structure. When numbers drop, recruiting new bots requires creating or purchasing new malware samples that are not detected by anti-virus, installing 'drive-by' infection systems on websites or launching email spam campaigns. Alternatively, Internet-of-Things botnets such as Mirai recruit new victims through Internet wide scans for machines with default or otherwise weak passwords, or unpatched vulnerabilities that can be exploited to run malware on the devices (Kolias et al., 2017).

Someone setting up a booter to provide DDoS-as-a-service will need a botnet to provide firepower. Alternatively, Internet-wide scans will be needed to identify misconfigured machines that will reflect (and amplify the size of) UDP packets. The lists of these reflectors is supplied to attack servers that can spoof outgoing packets so as to cause the amplified traffic to be sent to the victim (D. R. Thomas, Clayton, & Beresford, 2017). Whatever the technical mechanism, a booter will need a customer-facing website to track users, to collect payments and to allow attack instructions to be entered. The largest booter services operate dozens of servers in total, all of which need to be rented out, configured and then maintained to ensure they remain operational and secure (Karami & McCoy, 2013; Karami et al., 2016; Hutchings & Clayton, 2016).

Thus, whatever the underlying technology, the operation of a booter service requires a substantial degree of maintenance and administrative work. Given the competitive nature of the booter market, stability and reliability are key to the success of these services and they are often run by teams or groups of people who each do different jobs. Previous research has shown that a particularly important skill set is 'server management', involving purchasing and administering web servers, avoiding being banned by hosting companies, and relocating in the event of being shut down, and there is a distinct shortage of competent people who are prepared to do this job (Collier et al., 2019). When such people decide to leave their posts the booter can rapidly lose its reputation and will no longer attract large numbers of customers. In addition, running a booter service often requires substantial investment in customer support work, through a ticketing system or a realtime chat service, when issues arise with payments or with customers failing to understand how to use the service.

## 5.2 The Zeus banking trojan

Our second case study, which demonstrates the transition of a product from tool to infrastructure, is the Zeus malware (Tajalizadehkhoob, Asghari, Gañán, & Van Eeten, 2014; Hutchings & Clayton, 2017). Zeus entered the wild in 2007 as a multi-purpose malware platform, which was originally sold for

several thousand dollars a copy on online illicit markets. Zeus was mainly used for 'man in the browser' attacks against banking websites, but could also steal credentials, cookies or keystrokes.

The communities which grew up around Zeus originally had a tool-purchasing structure where users would buy the malware directly and then purchase (or perhaps develop their own) configuration files to tailor it for a particular target (choosing how to recognise the bank website, which fields to extract or indeed what extra fields should be inserted into the page to capture more data). Having purchased and configured Zeus these individuals would then use their own mechanisms to deploy the malware on to victim machines – such as sending spam that enticed receivers into clicking on executable attachments (Hutchings & Clayton, 2017).

When the source code for Zeus was leaked there was no longer a market for Zeus itself, but the Zeus community found new ways to monetize this new resource, transitioning to a service-based model where users could, for a monthly fee, pay for someone else to configure and maintain the malware to their specifications (Hutchings & Clayton, 2017).

Thus the Zeus economy was underpinned by a novel form of work: the creation and maintenance of custom Zeus configurations for the end customer. The combination of the Zeus platform and the market for configuration and maintenance constitutes a service infrastructure, opening this kind of illicit activity up to low-skilled users. Without the configuration files market, each individual user would need to assemble and tailor Zeus for a particular target from scratch – which would mean a lack of the 'transparency' which Star suggests is a key characteristic of infrastructure. The creation of a human and technical infrastructure for the set-up, configuration, and curation of Zeus therefore meant that those with the moderate levels of skill required could advertise opportunities for 'passive income generation' to their low-skilled clients, who would pay them to set up and maintain Zeus on their behalf..

## 5.3 Underground forums and markets

Our final example of a purpose-built illicit infrastructure has been extensively studied in the cybercrime literature (though rarely as an infrastructure): the underground forum or marketplace. These constitute some of the earliest cybercrime infrastructures, with roots in the bulletin board systems used by those distributing 'warez' (illegally copied software) in the 1980s (Cangialosi, 1989; Cortner, 2008; Wasiak, 2019), developing through Usenet boards and IRC channels (Décary-Hétu, Dupont, & Fortin, 2014; Benjamin, Li, Holt, & Chen, 2015) to the purpose-built underground forums which still dominate these communities as a space of interaction (Pastrana, Hutchings, et al., 2018). These websites, hosted either on the regular Internet or as Onion Services through the Tor network, provide a social and market infrastructure for cybercrime communities, generally supporting a range of different kinds of activities, including skill-sharing, social interaction, learning and teaching cybercrime skills, purchasing services and tools, and participation in the cultural life of cybercrime (Bancroft & Scott Reid, 2017). These online marketplaces support other tool economies to achieve scale; cryptomarkets and underground forums give the high-skilled 'inner' members of the cybercrime economy a place to sell the tools and platforms they develop to groups and individuals who lack the ability to develop these themselves, who can make use of the trust and reputation mechanisms used by these sites to assure a minimum quality level for the goods and services they purchase.

There is, accordingly, an enormous amount of (largely hidden) work involved in administering a successful marketplace or forum. At the high level, this involves managing the mechanics of hosting the website itself and making decisions about policy. For underground sites where explicitly illegal conduct is discussed, this entails dealing with a number of additional issues: finding hosting providers which are stable and unlikely to ban users, but still accessible enough to attract a sizeable community, avoiding DDoS attacks from competitor sites, and watching out for and banning scrapers. In addition, a number of policy decisions need to be made and enforced, from the kinds of activities and topics which will be permitted (which often entails rather difficult decisions about risk), to how trust, reputation, and escrow will be managed, to what the main categories for the different boards and areas of the site will be. This involves a minimal level of technical skill, usually looking out for obvious patterns (such as scrapers

reading every post in the forum in sequence), managing hosting, and implementing web design, and these are often facilitated by the existence of usable tools, guides, and toolkits like forumBB.

There are also a range of 'lower level' forms of work, which centre around managing and curating the user experience on the site and policing norms. For the moderators, this can involve manually screening and approving vast numbers of posts, processing abuse reports, and banning abusive individuals, though sometimes involves more active community management, with moderators becoming involved in discussions, warning where content skates close to the line, and explaining site policies. This is generally low-skilled, non-technical work, and the substantial volume to which this can grow in successful forums and marketplaces means that these often have teams of low-level employees who work for free, for small sums of money (often around $20 per month), or make money by abusing their position to promote services on behalf of selected forum members. This work is crucial to the underground cybercrime economy. Without this administrative work, these websites would provide a rather different experience for their users, evidence of which can be seen from failed or abandoned forums where this work is no longer carried out. These ghost websites tend to be overwhelmed with spam and low-quality posts, or have fallen apart due to rifts in the community, particularly risky or offensive activity which has drawn the attention of law enforcement, or which have simply become unstable and gone offline.

There is evidence that some of these communities are moving to generic platforms like Discord, Twitter, Facebook, and Telegram, and away from purpose-built community sites (Kamps & Kleinberg, 2018; Brewster, 2019). A range of groups, servers, and channels on these generic sites carry not only discussion about illicit activities but also advertisements for infrastructure-based services, such as secure hosting, reselling, advertising, and cash-out services. Although using the generic platform has some advantages, in particular that a great deal of administrative work is taken care of by the generic provider, it has a range of drawbacks for illicit communities which mean that there is still a major role for purpose-built sites. In particular, as the illicit economy has shifted to these new platforms they have found that they are not entirely welcome and that the generic providers are improving their abuse detection systems to locate and ban this activity, creating further tedious administrative work for the illicit admins, who need to evade bans, manage communities, police content, remake services when shut down, and ensure that their community transfers to their own new service rather than a duplicate set up by a scammer.

Across all three of these case studies, what stands out is that there is a great deal of hidden work ongoing which is vital to the success of these economies, and which produces the *infrastructural* quality of the technical systems which support them. It is this quality which enables the scaling-up of cybercrime to a volume crime. This work ensures, for example, that (successful) booter services don't shut down every other day, that (some) banking Trojans reliably earn income for their owners, and that (some) forums and marketplaces aren't flooded with spam or dominated by internecine conflict. In the following section, we draw from our empirical research across these three cases, pulling out key characteristics of this hidden work.

# 6 Features of infrastructural cybercrime work – the life of a deviant sysadmin

From our interviews, scraped data sources, and our review of the relevant literature, we have identified what we believe to be a set of key characteristics of illicit infrastructure and the work which supports it. Although there is a wide research literature covering the role played by botnets, the malware trade, and online forums and marketplaces in cybercrime economies, exploring the work that supports these infrastructures opens up important avenues for research. In analysing this hidden work in further depth, we are particularly struck by the substantial quality of maintenance and administrative work on which these infrastructures rely. This appears to be both vital to the stability and capacity of these infrastructures, but also to operate on rather different principles from the kinds of work generally understood to be important in cybercrime, such as experimentation, entrepreneurship, programming,

social engineering, probing vulnerabilities, and creative disruption.

We now draw on our empirical research, focusing on characterising this largely hidden administrative work in each of our case studies, to better understand what keeps these 'infrastructural' cybercrime economies afloat. In doing this, we identify eight important features of deviant infrastructural work:

1. *Supportive* of broader illegal action
2. Concerned with maintaining and managing *stability and transparency* (or usability)
3. Naturally tends towards *centralisation*
4. Has *low hacker cultural capital*
5. Involves *creatively defending against law enforcement*
6. Necessitates *managing and enforcing norms* around use and abuse
7. Promotes the *diffusion of risk and culpability*
8. Ultimately underpinned by *boredom* rather than excitement

We will now examine each of these in more detail, drawing from our empirical data where appropriate.

## 6.1 Supportive

The first feature of this work is the *supportive* role it plays in these economies. As this was one of the core criteria for which we selected in our analysis this is not in itself a conclusion drawn from the data, however we include a brief discussion of this supportive quality to better contextualise our other findings.

Built atop the existing Internet infrastructure (and generally following its topologies), and 'plugged-in' to other existing infrastructures, such as PayPal's payment systems, or the Bitcoin or Tor networks, these illicit infrastructures are an end in themselves, with the actions in which they become involved being directed by their customers rather than the owners. Drawing from Star's (1999) characterisation of infrastructure, the utility of these infrastructures come from the fact that they do not need to be assembled anew by each individual user or for each individual purpose. Rather, they can support a range of use cases which may in practice be rather different from one another, and the same infrastructure can support action by groups with very different, or even conflicting aims. This shapes many of the further qualities we discuss in this section, fundamentally changing the character of the work involved in important ways. Crucially, this enables these economies to achieve greater scale, as where previously a group or individual wanting to use a botnet would have to have the skills and resources to put one together, with shared illicit infrastructures, this work is centralised around a much smaller number of dedicated maintainers, dramatically reducing the barriers to entry.

> Top quality service. Lad sells bullet proof botnets, and a good list of nets to offer. Got my shit done in very short time. Only a few mins and he had me set up with the ... bot I asked for. Thanks to [provider]'s botnet set up I now mine about $40 worth of zCash a day and soon ill be upping my bot number and ill quit my job. Top quality lad right here. Don't hesitate to do business. Never have any problems with my net or this guy. – *Post in a cybercrime forum*

This also maximises the productivity of these infrastructures, ensuring that any excess unused capacity is available for sale to a range of other groups.

## 6.2 Stability and transparency

Due to this essentially supportive character, the new types of work involved in maintaining these infrastructures are largely concerned with maintaining *stability and transparency* for their users – the second

characteristic we identify in this paper. This ties into Star's (1999) characterisation of infrastructure as smoothly facilitating user action, with the technical workings remaining invisible except when it breaks down. In fact, the illicit infrastructures on which these economies depend all rely on a substantial quantity of hidden administration and maintenance work to maintain this stability and transparency. True to Star's characterisation, traces of these forms of 'hidden work' often only appear where it ceases to function:

> Dont buy server from [provider]. After more then week of downtime he give us half a server, we was supposed to receive soon the second one (since 5days) service shut down for no reasons and taking more than thirty hours to reboot or what ever. Yesterday we asked him for refund or server delivery before ooh he say yes (as always lol) and today we can see he block us and suspended server [provider] is a scammer. – *Booter user, posted on a chat channel*

> Hello everybody, first I'm very sorry for the problem with the layer 4 [DDoS services]. Every time this week I have tried to fix it with the host but they are stupid – they promise no downtime will back again but as we can see we have more downtime than uptime. I can't continue like this for you and for my business. So I will add new servers from new host in the next 24–48 hours, power will be upgrade and everyone will have 24h added to they plan. So please don't report me downtime from the next 24–48h. I know the problem and I can't do something. So please @everyone wait just 24–48h I will order today new servers. – *Booter provider, posted on a chat channel*

Despite the rote nature of these kinds of work, they have generally not been automated because of the lack of technical skill of many of these groups (who may be able to purchase the necessary technology, but unable to work automation of this administrative work into their processes). Equally, these service infrastructures often themselves are built on or rely on licit infrastructures such as Discord, PayPal or Internet Service Providers, which means they are routinely shut down by service providers and law enforcement (as we discuss below). In the case of booter providers, whose profits come directly from consumers, this can be of particular importance for smaller services, as drops in usability and stability can often result in users moving quickly to competitors. For forum moderators, maintaining usability can mean manually reading through hundreds of messages and abuse reports in order to lock out spammers and abusive members. Further, the Zeus set-up market is an example of the importance of *usability* for these infrastructures, as the leak of the source code for Zeus led to the formation of a market for configuration files (given the low usability for most technically-unskilled users of the malware platform) (Hutchings & Clayton, 2017). This generated profitable supportive work in putting together, marketing, and selling these files en masse, which in combination with the leaked Zeus technology created a social and technical infrastructure which could permit a market for wider use at scale for a range of activities. Finally, 'downtime' is a serious issue for markets and forums, particularly those hosted on Onion Services, which are especially vulnerable to DDoS attacks.

## 6.3 Centralisation

The third feature of this kind of work is *centralisation*, or what Clayton, Moore, and Christin term "concentration" (Clayton et al., 2015). This is well-established as a naturally-emerging feature of cybercrime economies, and of infrastructure more generally – the tendency for services to centralise through the economies of scale, and for specialisation of labour to develop to improve productivity (A. Smith, 1776). This is particularly well-documented in the literature on decentralised system design, which often notes that achieving and maintaining decentralisation in technical networks is very difficult (Raman, Joglekar, Cristofaro, Sastry, & Tyson, 2019; Marlinspike, 2019). So it is mainly economic factors that mean that the particular kinds of skills required for illicit infrastructural work (and its supportive role) lead to centralisation around a small number of administrators.

The importance of stability, which we discussed above, means that initial success can bring with it serious issues, as an influx of users or customers can overwhelm existing administrative capacity, causing

downtime, and hence irritation, suspicion that the service is a scam, and displacement to competitor services. Over time, this means that the few services which are able to make these underlying maintenance processes work well tend to grow, while those which don't contribute to a 'churn' of short lived forums and services. Newer entrants therefore tend to 'piggyback' on the administrative work of these larger services. Where there are established players, economic imperatives, skill barriers, and the tedious nature of much of this administrative work encourage newer services to base themselves on reselling the capacity of existing ones (or setting up shop on existing popular forums) over the creation of new infrastructure.

> [takedowns] can effect providers. If we went down, Man literally everything would be fuckked Couldnt count on both my hands and my toes how many others use our API [resell our attack capacity] – *Booter provider*

> 70% of my power comes from other sites. If I get messed with by law enforcement I just send the cops to them – *Booter provider*

Network effects then mean that these larger services become the 'go-to' for new users, further contributing to growth and centralisation. For example, although there are a large number of 'hacking' forums, the majority of the volume-crime activity is concentrated around a few long-running sites, with smaller forums often being more important for low-volume, high-harm offending.

## 6.4 Low hacker cultural capital

The fourth feature of this kind of work is relatively *low hacker cultural capital*. Social capital and the respect within these communities which it represents is an important aspect of cybercrime subcultures (and illicit subcultures more generally). However, this supportive work does not generally possess the qualities valued by underground hacker culture, unlike the more technical and creative forms of cybercrime work traditionally depicted in the criminological literature. These forms of labour lack the overt forms of technical mastery or creativity to engender much respect or reputation within hacker subcultures, and because of the rote nature of the work and the fact that the action is impelled by users, they lack the deviant, exciting, or political character which forms this cultural connection for other low-skilled 'script kiddie' activities.

> Lots of people are starting to see what I and lots of others see. [running a booter is a] place where you learn nothing new and don't go much of anywhere... [people will] disengage entirely. Thats what I pretty much did – *Ex-booter provider*

Equally, the nature of these forms of supportive work means that they are often only noticed when they fail, meaning that these workers are more likely to become known as dependable service workers rather than 'elite' hackers.

> *USER 1:* you mods/admins on [cybercrime forum]. idk [I don't know] how you do it. there's like a million topics where things are getting uploaded that you guys look into and approve manually. what do you do? split up responsibility to different parts of the forum or something? that's crazy, idk how you do it. on top of that, keeping tabs on where certain topics need to be and moving them when necessary. seems to me like you guys do a lot and this is a HUGE forum, i couldn't imagine trying to take care of something like this especially the way you do.
>
> *ADMIN 1:* YAY. I MAKE A DIFFERENCE! No. Really, no. This isn't a bureaucracy. We aren't skilled workers. If [lead admin] left and somebody else took over, we would be demoted and the new guy would pic new staff. But you know dem admins are amazing. Irreplaceable. Super cool. Hard workers. Did I mention amazing? (Enough sucking up)
>
> *ADMIN 2:* So honest! My lovely r******d children... Running a sweatshop really...

> *ADMIN 3:* This how [cybercrime forum] does it. Have lots of staff and positions. lol Minions take care of certain sections. Moderators watch over minions and all sections. Simple. – *Discussion on a cybercrime forum*

Accordingly, while the administrators of these services don't accrue 'hacker' cultural capital (in terms of reputed technical prowess), more senior admins do have the capacity to develop substantial social capital in other ways, usually as a trusted intermediary or community member. This reputation is generally linked to the supportive role which they play, particularly where they manage to maintain a high degree of stability and hence keep their work as 'hidden' as possible. Despite this, however, the generally low-status nature of this work appears to be a key factor in burnout for these maintainers.

## 6.5 Creatively defending against law enforcement

Despite this lack of hacker cultural capital and low levels of technical skill, this maintenance and administrative work isn't completely devoid of creativity. The fifth feature of this kind of work is that it involves *defending these illicit infrastructures* against law enforcement and the administrators of the legitimate infrastructure (such as hosting companies, PayPal, and social media platforms) on which it itself is built or relies. Where the hacker ethic comes out, it is in developing, learning, and passing down clever rules of thumb and adaptations to bans and takedowns, abortive attempts at automation, and a variety of ways in which these admins avoid being caught (even though, as they only become visible when they don't work, this doesn't necessarily lead to kudos in the wider community). This is of particular importance for server management, but is also relevant to keeping Tor relays, cashout systems and other forms of infrastructure in working order.

> A lot of people were [cashing out] through like, Western Union, and you could get quite easily caught out that way... So what we would do is hook up a random PayPal account from a random email, and basically attach a VISA giftcard which we could buy from a supermarket in abundance, and you only have to put a small amount on it to actually purchase it... and there was no ties back to who purchased it... The Paypal accounts would only become limited when we would receive a large amount of funds... we would just withdraw it to the card and then pull it out at an ATM. To avoid a mass stream of money coming in from one PayPal account at a time, our payment service would keep track of how much each account had, and the payment would be directed to one of these accounts. When one got full, we got notified by a service that we scripted - *Booter provider*

Although this work is 'low-skilled' in the sense that the people who practice it lack a systematic understanding of computer systems, and often have little knowledge of *why* their actions result in the (apparently protective) effects they do, they do in fact cultivate a particular set of skills. These are rather different from the traditional picture of hacking, which involves deep understanding and well-informed experimentation with technical systems. Instead, the work associated with this administrative and maintenance labour is more akin to the cultivation of folk wisdom, involving learning rules of thumb passed between practitioners, trying out different things over time and developing a set of practical knowledge about the system and how to maintain it as stable and free from law enforcement action. As such, the practices and kinds of knowledge involved in these forms of hidden infrastructural work are very different from those with which much of the cybercrime literature concerns itself.

## 6.6 Managing and enforcing norms

It may seem contradictory for what are effectively illegal services, however these infrastructure administrators in fact insist on strong conditions around the kinds of activities for which these their platforms will be allowed to be used. *Managing these norms around use and abuse* is therefore an important sixth characteristic of this infrastructural work. This is for both practical and normative reasons. Practical reasons tend to centre around keeping the activities for which the infrastructure is used within the bounds of the risk appetite of the providers (who may be fine with a market being used for selling marijuana, but not for bomb-making material) and to avoid attracting undue attention from law enforcement, either

for the arrest of the infrastructure providers, or more prosaically, to avoid takedowns and maintain the stability of the service.

> Secondly, banned topics. Paypal Fraud, Silk Road, Deepweb/Darkweb/Deepnet whatever the hell you want to call it, Credit Cards, etc etc. ... Are you serious? You're complaining because you want [the forum owner] to allow people to PUBLICLY announce they are doing something illegal? The website and domain would be seized and he would be arrested, ALONG with the members being arrested. If anything, you should thank him for it. Disallowing topics that are ILLEGAL (real hacking is NOT illegal, I'm not sure where people get this idea either) is a good thing. – *Post in a cybercrime forum*

In addition, the operators of these infrastructures often enforce genuinely-held norms and values around which activities are acceptable. This is distinct from 'legalese' copy-and-paste notices advising users that they have liability for illegal conduct, which is prohibited by the site; rather than half-hearted, unenforced, and often tongue-in-cheek warnings (which are often evident), these norms are actually enforced, through bans and built-in blocks on particular use cases.

> Fentanyl and any analogue of it is strictly prohibited on [cryptomarket]. It's clearly stated in the rules and I've reiterated this message several times. I'm not fucking around; I've banned 3 vendors already this evening for listing fentanyl and carfent on the market. I'm not giving warnings anymore. Should you wish to not heed my warning then you're GONE. So, if you are reading this and have fent or an analogue listed, get rid of it before you're the one gotten rid of. I'm currently doing a full market sweep. The clock is ticking. These rules are in place for everybody's safety, not to spoil fun. People are buying this shit online and misrepresenting it as heroin to boost profit margins on the street. This isn't going to be happening on our watch, nor will it be facilitated by [cryptomarket]. Thank you to the vast majority that do follow the rules. Stay safe, people. – *Administrator post in a cryptomarket forum*

> You are not allowed to ddos educational websites or IP addresses using our stresser. That means you can't ddos school websites, school IP addresses and educational websites like a math website that schools use. – *Booter provider, posted on a chat channel*

Taken together, this set of prohibited and permitted use cases constitutes a category system embedded at the heart of the infrastructure, which is of particular importance in making sense of its role in illegal economies. Rather than constituting the intended use case for a single tool used by a particular group to a defined end, this is the product of the overlapping intentions of a wide range of different groups who share the infrastructure, driven by the risk appetite and values of the infrastructure providers. This has important implications for the *particular qualities* of the volume crime which these infrastructures enable; they enforce an 'Overton window' on their users, enforcing (or at least encouraging) an agreed set of norms on the broader cybercrime economy. Enforcing these norms in itself constitutes a substantial quantity of work for the administrators of these services, markets, and forums, including processing abuse reports, pre-moderating comments, and reviewing user activity logs. Enforcing and reinforcing these norms helps counter the destabilising effect of information asymmetry and is hence crucial to managing trust, reputation, and, ultimately, the success of forums and markets (Allodi, Corradin, & Massacci, 2015).

## 6.7 Diffusion of risk and culpability

The seventh feature of this kind of work is the *diffusion of risk and culpability*. The criminological literature on involvement in illegal activities often draws on Sykes and Matza's foundational work on 'neutralisations', cognitive justifications which allow individuals to remain involved in harmful, illegal, risky, or norm-breaking activities while still maintaining a coherent and positive sense of self (Sykes & Matza, 1957). Illicit infrastructural work provides particularly fertile ground for these neutralisations, on the part of both users and administrators. Users can displace blame to providers, and individually

their actions are fairly petty and low-harm, while administrators, as they do not initiate the harmful actions themselves, can displace blame to users as they claim to be simply 'providing a service'.

> By using this stresser [booter service] you are responsible for what you are using it for. You have to stick with the laws from where you come from,remember you are responsible for your own actions and a reminder that [this] is a stress testing networking tool. – *Booter provider*

These similarly function to neutralise perceptions of the risk of arrest and prosecution, as users (generally correctly) believe that their involvement is too petty to warrant police attention, while administrators often believe (generally incorrectly) that their users assume full legal responsibility for their actions (Hutchings & Clayton, 2016).

## 6.8 Boredom

The final, and potentially most important, feature of this work is the that it is strongly characterised by *boredom*, which also appears to be a limiting factor in involvement. The emphasis on stability and the need to avoid being banned from hosting services means that the day to day experience of many of these 'hidden' jobs is one of deep tedium, involving work which is repetitive, does not challenge or stimulate, and is frustrating. At the beginning, this can be an attraction for labourers in cybercrime economies; these are routine, low-involvement ways to earn money and participate in a deviant subculture: 'autopilot' jobs which can be done while playing videogames and smoking marijuana (as one interviewee argued):

> Its profitable (decently) and its autopilot. I can sit in my chair, smoke weed and still make money – *Booter provider*

While the users of these services may well be looking for excitement, the rote nature of this work can in fact be part of its attraction to providers, making it easier for them to neutralise their culpability for the problematic or harmful use cases to which the service is put, necessitating fairly low levels of involvement which can easily be worked around school or other responsibilities, and allowing them to make a relatively stable income while engaging in recreational activities such as gaming. In fact, this kind of work plays into many of the same rhythms and logics as some kinds of contemporary online videogaming, where players perform repetitive tasks for long periods of time for rewards, often described as 'farming' or 'grinding' for points or in-game currencies (Dubbell, 2015; Möring & Leino, 2016). However, in the absence of strong cultural and political motivations or advancement to more challenging and lucrative kinds of work, this can, over time, lead to burnout:

> And after doing for almost a year, I lost all motivation, and really didn't care anymore. So I just left and went on with life. It wasn't challenging enough at all. Creating a stresser is easy. Providing the power to run it is the tricky part. And when you have to put all your effort, all your attention. When you have to sit in front of a computer screen and scan, filter, then filter again over 30 amps per 4 hours it gets annoying – *Booter provider interview*

> I had a Mirai botnet but got bored n deleted it – *Cybercrime community channel chat log*

This burnout is an important feature of this kind of supportive work, which is characterised less by a progressive disengagement with a once-interesting activity, and more by the gradual build-up of boredom and disenchantment, once the low ceiling of social and financial capital which can be gained from this work is reached.

## 6.9 Summary

Taken together, these qualities characterise the important, but under-considered forms of infrastructural work which underpin many of these illicit online economies. It also bears noting at this stage that, although we focus on three case studies here, our findings are more generally applicable to a wide range

of other kinds of shared illicit cybercrime infrastucture, including the markets for pay-per-install botnet curation (K. Thomas et al., 2016), the large amounts of customer support work which encourages the victims of ransomware to believe it to be worthwhile to transfer cryptocurrency to their attackers (Turkel, 2016), and the extensive market for bulletproof and semi-bulletproof hosting services (Noroozian et al., 2019).

# 7 Discussion and conclusions

Having characterised the hidden work required to sustain purpose-built illicit infrastructures, we now discuss what our findings mean for broader criminological understandings of cybercrime economies and consider the potential for new types of intervention by law enforcement and others.

## 7.1 Implications for criminological research

Shifting focus to the proliferation of forms of tedious supportive work in cybercrime economies has implications for criminological research. The role played by *boredom* was a particularly striking finding in our study of these infrastructures, which bears further consideration. Boredom has long been a productive concept within criminological research, however this has generally been framed rather differently from the research we present here. Ferrell argues that boredom, either the tedium of work or of unemployment, is a fundamental characteristic of the experience of life in industrial capitalist societies: that, although boredom is not exclusive to capitalism, the particular rhythms and logics of work in these societies, coupled with the individualist, entrepreneurial norms and values which they embody, give rise to particularly corrosive and oppressive forms of boredom. These form part of a more general *anomie*, or undermining of commonly-held social norms and values (Merton, 1938; Ferrell, 2004; H. P. Smith & Bohm, 2008). This reflects a wider preoccupation within mid-20th Century criminological scholarship with the perceived social issues posed by the delinquency of young men who failed to conform as members of the industrial working classes.

Underneath this macro-social *anomie* – at the level of the individual – boredom and dissatisfaction with conventional jobs, social roles and leisure activities underlies some elements of strain and subcultural theories of offending: that for many people, conventional pathways and occupations fail to allow them access to commonly-held measures of social success, and they instead find themselves stuck in laborious, unfulfilling labour (or face teenage life in towns and cities with little provision for young people) (Merton, 1938; Kaufman, 2017; Bell, 2010; Agnew, 1992). This is effectively portrayed as an *anomic boredom*; not simply a lack of excitement, but a broad social phenomenon tied to a deep dissatisfaction, the deprivation of personal fulfilment, a sense of social worthlessness, and disconnection from mainstream social values and narratives around personal success (something also drawn out extensively in the prisons literature) (Cohen & Taylor, 1976; Hagan, Hefler, Classen, Boehnke, & Merkens, 1998; Leslie, 2009; Kaufman, 2017).

These perspectives often frame participation in crime and deviance as partly 'arising' from this boredom, with exciting deviant subcultures and activities presenting alternative means of gaining social and financial capital, and permitting an escape from conventional forms of labour within capitalist societies, from the tedium and pains of imprisonment, or from the problems of teenage life (Bell, 2010). For adolescents, deviant subcultures can provide alternative sources of excitement, productive activity and social status in places where opportunities for conventional leisure activities and association are blocked. The link between this deviant leisure activity and criminal offending is conceptualised in some of the youth crime literature through the lens of the 'leisure career', in which particular patterns of adolescent leisure activity (shaped by the opportunities available) influence and develop into other pathways through housing, drug-use, employment, or in some cases 'criminal careers' (MacDonald & Shildrick, 2007). The experience of deviance as exciting is itself well-recognised within criminological scholarship as important in involvement in illegal activities and deviant forms of leisure (Hayward & Fenwick, 2000). Steinmetz, Shafer, and Green (2017) draw on exactly this framing to discuss the importance of boredom

in crime, tying this explicitly to participation in hacking. Although they acknowledge some aspects of 'hacking' can be tedious, this is always underpinned by the promise that this often-laborious work (which draws on an intimate knowledge of technology) will yield eventual excitement when the exploit or 'hack' finally works. This, in accordance with wider research around hacker subcultures, frames involvement in these communities as partly driven by the pursuit of challenge and stimulation (Levy, 1984).

Our work frames boredom and its implication in illegal economies rather differently. As opposed to understandings of crime as being born of boredom, (which put a focus on individual, low-level crime), we find that as cybercrime has developed into industrialised illicit economies, so too have a range of tedious supportive forms of labour proliferated, much as in mainstream industrialised economies. We argue that cybercrime economies in advanced states of growth have begun to create their own tedious, low-fulfilment jobs, becoming less about charismatic transgression and deviant identity, and more about stability and the management and diffusion of risk. Those who take part in them, the research literature suggests, may well be initially attracted by exciting media portrayals of hackers and technological deviance. However, the kinds of work and practices in which they actually become involved are not reflective of the excitement and exploration which characterised early 'hacker' communities, but are more similar to low-level work in drug dealing gangs, involving making petty amounts of money for tedious work in the service of aspirations that they may one day be one of the major players. This creates the same conditions of boredom, and, ultimately, of anomie, which are found in mainstream jobs when the reality emerges that these status and financial goals are as blocked in the illicit economy as they are in the regular job market.

As cybercrime economies have begun to progress to this 'industrialised' stage, so too have they begun to take on the characteristics of other forms of crime which have made this transition, such as fraud or drug dealing. Although this is often described as cybercrime becoming 'organised', this should not be taken to mean that it is always conforms to typically-conceived ideas about the severity, hierarchical structure, or implication in power relations which commonly attend the category 'organised crime' (Lusthaus, 2013; Hutchings, 2014; R. Leukfeldt, Lavorgna, & Kleemans, 2017), much as drug crime and fraud themselves often do not. Instead, we argue that this is part of more general, partial, and ad-hoc processes of industrialisation and organisation, similar to that described in Densley's research on the drug economy, which shows the progression of 'gangs' through recreational, criminal, enterprise, and governance stages (Densley, 2014).

The menial nature of much of the work involved and the importance of supportive, mediating and administrative roles is a common feature in research on these other illegal economies (Cook, Harris, Ludwig, & Pollack, 2014). In addition, this research also characterises the progression of these economies from excitement and experimentation to more businesslike approaches, with illegal activities moving from being an end in themselves to being a means of making money (Shammas, Sandberg, & Pedersen, 2014). It is clear that many aspects of cybercrime are becoming similarly industrialised, and given the skillsets and technical requirements of much of online crime, the attendant service economy is largely focused around the provision of supportive technical infrastructure (rather than couriering or the provision of physical security). For criminologists, the complex technical detail involved in understanding sophisticated communication technologies threatens to pose a barrier to making sense of what the interesting research questions, findings, and dependencies are therein. Here, there is a clear utility for Star's infrastructural studies research in providing a way forward for working through this dense technical detail, and making sense of the 'technosocial' dimension of communications infrastructures and their implication in illicit economies (Star, 1999).

There are of course exceptions to the pathway we describe herein. The case of Marcus Hutchins, recently profiled in *Wired* (Greenberg, 2020), follows the 'escalation' narrative which is common in cyber-criminological scholarship, wherein low-level activites such as running booter services are the first step on a pathway which progresses to more serious and technically skilled forms of online crime (Goldsmith & Brewer, 2015). Nevertheless, it is of particular note that the boring administrative work involved in running a booter service is specifically highlighted in the profile of Hutchins' life and his

pathway through various kinds of illicit online activity:

> Hutchins says, he still saw what he was doing as several steps removed from any real cybercrime. Hosting shady servers or stealing a few Facebook passwords or exploiting a hijacked computer to enlist it in DDoS attacks against other hackers—those hardly seemed like the serious offenses that would earn him the attention of law enforcement... In fact, within a year Hutchins grew bored with his botnets and his hosting service, which he found involved placating a lot of "whiny customers." So he quit both and began to focus on something he enjoyed far more: perfecting his own malware. – *Wired, 2020*

What makes individuals like Hutchins exceptional is that he was one of the few people who become involved in infrastructure provision with the skills, focus, and interest to progress to more complex and technical (and therefore more interesting and engaging) forms of illegal activity. This means that rather than dropping out of these low-level forms of online crime, individuals with a pre-existing talent for technical work may well escalate to more complex forms of offending when the boredom of administrative work becomes too much. Hutchins' turn to more socially productive forms of hacking and security work later in life, however, suggests that for these skilled individuals, opportunities in the licit cybersecurity economy may indeed form useful pathways to desistance.

## 7.2 Policy implications

What makes for successful interventions to prevent or reduce cybercrime is still poorly-understood in academic research and policymaking, with little in the way of well-established best practice (Brewer et al., 2019). In general, the research literature suggests that traditional policing approaches based on economically rational offenders, which revolve around the use of arrests and harsh sentencing, may have little, or at worst, entirely counterproductive effects (Ladegaard, 2019; Collier et al., 2019; Chua et al., 2019; Holt et al., 2019). Ladegaard's work in particular shows that wide-ranging 'crackdowns' on online illicit markets can in fact unite communities, giving them a common sense of struggle and persecution (Ladegaard, 2019). Instead, we argue that reframing and broadening understanding of cybercrime actors as we have done in this paper suggests a number of potential avenues for intervention in these communities.

As the actors supporting the 'volume crime' problem of cybercrime are largely low-skilled maintainers, they are subject to rather different conditions than the kind of high-skilled actors which traditional interventions assume. Much as with drug and fraud enterprises, arresting prominent, high-up members of networks may lead to positive reporting in the press, however the structure of these economies means that there are usually a wealth of lieutenants and competitors ready to take their place. Similarly, these administrative jobs inherently neutralise and diffuse the perceptions of risk and culpability which arrests aim to affect, and increasing the notoriety and sense of shared struggle against law enforcement may well pull these communities together (Becker, 1963; Ladegaard, 2019). Resisting the urge to focus on arrests and crackdowns as a primary strategy, which stems from the assumption that cybercrime is a problem of high-skilled actors who take a fundamentally rational approach to minimising risk and maximising profit, opens up a range of interventions which instead target the administrative work which allows these economies to achieve scale.

This rote work is vulnerable to interventions which can be conceived in the language of economics, but which do not focus on the calculus of profit or risk. Instead, interventions might productively focus on the economics of attention and boredom – how boring and laborious can we make this work before people quit? By making this work more boring, interventions can have a real impact on these markets by encouraging 'burnout', while avoiding some of the unintended harms of more traditional policing. For example, the whack-a-mole approach of engaging with legitimate hosting providers to get websites taken down is often seen as pointless because the illicit infrastructure just appears somewhere else. However, every time there is a takedown there is further repetitive, tedious, work for the administrators to set up their sites anew (Hutchings, Clayton, & Anderson, 2016).

Recent research shows that the booter market is particularly susceptible to interventions targeted at this infrastructural work, which make the jobs of these server managers more boring and more risky (Collier et al., 2019). As they tend to support a range of other booter services, encouraging even a few administrators to quit can cause substantial destabilisation. Equally, intervening directly with these administrators, in the understanding that they maintain a normative order around acceptable behaviour and tolerable risk, (such as when the FBI advised the administrators of *Hack Forums* to stop permitting discussion of booter services on their website) can have significant effects on these markets (Collier et al., 2019).

Refocusing interventions in this way might also be supported by changes to the predominant forms of messaging used by law enforcement and policy professionals around cybercrime. If participation within these economies is in fact based in deviant aspiration rather than deviant experience, the currently-dominant approaches to messaging, which tend to focus on the dangerous and harmful nature of these behaviours, the high levels of technical skill possessed by cybercrime actors, the large amounts of money made in illicit online economies, and the risk of detection, arrest, and prosecution are potentially counterproductive, only feeding the aspiration which drives this work. Conversely, by emphasising the tedious, low-skilled, low-paid, and low-status reality of much of this work, messaging could potentially dissuade those involved in deviant online subcultures from making the leap from posting on forums to committing low-level crime.

Additionally, diversionary interventions that emphasise the shortage of sysadmin and 'pen tester' workers in the legitimate economy ("you could be paid really good money for doing the same things in a proper job") need to recognise that pathways, motivations, and experiences may be rather more prosaic than might be expected. Conceptualising cybercrime actors as high-skilled, creative adolescents with a deep love for and understanding of technology may in fact mischaracterise most of the people on whom these markets depend, who are often low-skilled administrators who understand fairly little about the systems they maintain and administer, and whose approach is more akin to the practical knowledge of the maintainer than the systematic knowledge of a software engineer or security researcher. Finding all these bored people appropriate jobs in the legitimate economy may be as much about providing basic training as about parachuting superstars into key positions. Equally, our depictions of the 'boredom' of the untrained administrative work carried out in the illicit economy should not be taken as impugning the valuable and complex work of legitimate system administrators, (which is in itself a worthy profession) – rather, it is to recognise that this is a different *kind* of knowledge and set of skills from engineering work, which needs to be taught, learned, and managed differently.

We have sketched in this paper an outline of what we believe to be an unremarked-upon facet of cybercrime economies, and hinted at some potential avenues for intervention. However, if there is one key take-away from this paper it is that, although it is exciting to find that 'boredom' is a valuable new way of looking at cybercrime, there is much still to be done to establish quite how to leverage this new understanding effectively. It remains for future research to consider how best to speed up the process of persuading those involved in cybercrime economies that there are more socially-beneficial, well-remunerated, and indeed far more interesting things to do with computers than their current job as a deviant sysadmin, or underground 'microserf'.

# References


Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47–88.

Allodi, L., Corradin, M., & Massacci, F. (2015). Then and now: On the maturity of the cybercrime markets the lesson that black-hat marketeers learned. *IEEE Transactions on Emerging Topics in Computing*, *4*(1), 35–46.

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., … Vasek, M. (2019). Measuring the changing cost of cybercrime. In *Workshop on the Economics of Information Security*.

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

Becker, H. (1963). *Outsiders: studies in the sociology of deviance.* New York: Free Press.

Bell, A. (2010). The subculture concept: A genealogy. In *International Handbook of Criminology* (pp. 179–210). CRC Press.

Benjamin, V., & Chen, H. (2012). Securing cyberspace: Identifying key actors in hacker communities. In *IEEE International Conference on Intelligence and Security Informatics* (pp. 24–29).

Benjamin, V., Li, W., Holt, T., & Chen, H. (2015). Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In *IEEE International Conference on Intelligence and Security Informatics* (pp. 85–90).

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Springer.

Brewster, T. (2019). Discord: The $2 billion gamer's paradise coming to terms with data thieves, child groomers and FBI investigators. *Forbes*. Retrieved 2020-02-24, from `https://www.forbes.com/sites/thomasbrewster/2019/01/29/discord-the-2-billion-gamers-paradise-coming-to-terms-with-data-thieves-child-groomers-and-fbi-investigators/#c4b26d137416`

British Society of Criminology. (2015). *Statement of ethics.* Retrieved 2020-02-26, from `http://www.britsoccrim.org/ethics/`

Broadhurst, R., Grabosky, P., Alazab, M., & Bouhours, B. (2013). Organizations and cybercrime. *Available at SSRN 2345525*. doi: 10.2139/ssrn.2345525

Brunt, R., Pandey, P., & McCoy, D. (2017). Booted: An analysis of a payment intervention on a DDoS-for-hire service. In *Workshop on the Economics of Information Security.*

Cangialosi, C. (1989). The electronic underground: Computer piracy and electronic bulletin boards. *Rutgers Computer & Tech. LJ*, *15*, 265.

Chen, C., Zhang, J., Xiang, Y., Zhou, W., & Oliver, J. (2016). Spammers are becoming "smarter" on Twitter. *IT Professional*, *18*(2), 66–70.

Chen, Y., Kintis, P., Antonakakis, M., Nadji, Y., Dagon, D., & Farrell, M. (2017). Measuring lower bounds of the financial abuse to online advertisers: A four year case study of the TDSS/TDL4 botnet. *Computers & Security*, *67*, 164–180.

Chua, Y. T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G., & Hutchings, A. (2019). Identifying unintended harms of cybersecurity countermeasures. In *2019 APWG Symposium on Electronic Crime Research (eCrime).*

Clayton, R., Moore, T., & Christin, N. (2015). Concentrating correctly on cybercrime concentration. In *Workshop on the Economics of Information Security.*

Cohen, S., & Taylor, L. (1976). *Escape attempts: The theory and practise of resistance to everyday life.* Routledge.

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

Coleman, G. (2017). From Internet farming to weapons of the geek. *Current Anthropology*, *58*(S15), S91–S102.

Coleman, G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255–277.

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. In *Proceedings of the Internet Measurement Conference (IMC)* (pp. 50–64). ACM.

Cook, P. J., Harris, R. J., Ludwig, J., & Pollack, H. A. (2014). Some sources of crime guns in Chicago: Dirty dealers, straw purchasers, and traffickers. *J. Crim. L. & Criminology*, *104*, 717.

Cooke, E., Jahanian, F., & McPherson, D. (2005). The zombie roundup: Understanding, detecting, and disrupting botnets. *Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, 39–44.

Cortner, C. (2008). *The warez scene.* Retrieved 2020-02-26, from `https://people.uwec.edu/greener/phil308/TermPapers2/ChrisCortner-FinalRev-4-05-09.pdf`

Décary-Hétu, D., Dupont, B., & Fortin, F. (2014). Policing the hackers by hacking them: Studying online deviants in IRC chat rooms. In *Networks and network analysis for defence and security* (pp. 63–82). Springer.

Densley, J. A. (2014). It's gang life, but not as we know it: The evolution of gang business. *Crime & Delinquency*, *60*(4), 517–546.

Dubbell, J. (2015). Invisible labor, invisible play: Online gold farming and the boundary between jobs and games. *Vand. J. Ent. & Tech. L.*, *18*, 419.

Ferrell, J. (2004). Boredom, crime and criminology. *Theoretical Criminology*, *8*(3), 287–302.

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*. doi: 10.1177/1477370819887305

Grabosky, P. N. (1996). Unintended consequences of crime prevention. *Crime Prevention Studies*, *5*, 25-56.

Greenberg, A. (2020). *The confessions of marcus hutchins, the hacker who saved the internet.* Retrieved from `https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/`

Grier, C., Ballard, L., Caballero, J., Chachra, N., Dietrich, C. J., Levchenko, K., ... others (2012). Manufacturing compromise: the emergence of exploit-as-a-service. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (pp. 821–832).

Hagan, J., Hefler, G., Classen, G., Boehnke, K., & Merkens, H. (1998). Subterranean sources of subcultural delinquency beyond the American dream. *Criminology*, *36*(2), 309–342.

Hayward, K. J., & Fenwick, M. (2000). Youth crime, excitement and consumer culture: the reconstruction of aetiology in contemporary theoretical criminology. In *Youth Justice* (pp. 31–50). Cavendish.

Herley, C., & Florêncio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In *Economics of information security and privacy* (pp. 33–53). Springer.

Hodgkinson, S., & Tilley, N. (2007). Policing anti-social behaviour: Constraints, dilemmas and opportunities. *The Howard Journal of Criminal Justice*, *46*(4), 385–400.

Holt, T. J. (2007). Subcultural evolution? examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198.

Holt, T. J. (2019). Chapter 7: Cybercrime subcultures. In *The human factor of cybercrime.* Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. Routledge.

Holt, T. J., Brewer, R., & Goldsmith, A. (2019). Digital drift and the "sense of injustice": Counterproductive policing of youth cybercrime. *Deviant Behavior*, *40*(9), 1144–1156.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1–20.

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 *Proceedings of the 2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 33–40).

Hutchings, A., Clayton, R., & Anderson, R. (2016). Taking down websites to prevent crime. In *Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1–10).

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

Hutchings, A., & Holt, T. J. (2018). Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice & Criminology*, 75.

Hyslip, T. S., & Holt, T. J. (2019). Assessing the capacity of DRDoS-for-hire services in cybercrime markets. *Deviant Behavior*, *40*(12), 1609–1625.

Johnson, D. G., & Powers, T. M. (2005). Computer systems and responsibility: A normative look at technological complexity. *Ethics and Information Technology*, *7*(2), 99–107.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757–780.

Kamps, J., & Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science*, *7*(1), 18.

Karami, M., & McCoy, D. (2013). Rent to pwn: Analyzing commodity booter DDoS services. *USENOX ;login*, *38*(6), 20–23.

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).

Karanasiou, A. P. (2014). The changing face of protests in the digital age: on occupying cyberspace and Distributed-Denial-of-Services (DDoS) attacks. *International Review of Law, Computers & Technology*, *28*(1), 98–113.

Katz, J. (1988). *Seductions of crime: Moral and sensual attractions in doing evil*. Basic Books New York.

Kaufman, J. M. (2017). *Anomie, strain and subcultural theories of crime*. Routledge.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84.

Konte, M., Perdisci, R., & Feamster, N. (2015). ASwatch: An AS Reputation System to Expose Bulletproof Hosting ASes. In *ACM SIGCOMM Computer Communication Review.*

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy*, *4*(1), 33–39.

Ladegaard, I. (2019). "I pray that we will find a way to carry on this dream": How a law enforcement crackdown united an online community. *Critical Sociology*, *45*(4-5), 631–646.

Leslie, I. I. (2009). From idleness to boredom: on the historical development of modern boredom. In *Essays on boredom and modernity* (pp. 35–59). Brill Rodopi.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

Leukfeldt, R., & Holt, T. J. (2019). Examining the social organization practices of cybercriminals in the Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology*. doi: 10.1177/0306624X19895886

Leukfeldt, R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? an assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300.

Levitt, S. D., & Venkatesh, S. A. (2000). An economic analysis of a drug-selling gang's finances. *The Quarterly Journal of Economics*, *115*, 755–789.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Anchor Press/Doubleday Garden City, NY.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52–60.

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.

MacDonald, R., & Shildrick, T. (2007). Street corner society: leisure careers, youth (sub) culture and social exclusion. *Leisure Studies*, *26*(3), 339–355.

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, *2013*(6), 9–13.

Marlinspike, M. (2019). *36C3: The ecosystem is moving.* Retrieved 2020-02-26, from `https://www.youtube.com/watch?v=Nj3YFprqAr8`

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, *3*(5), 672–682.

Meyer, G. R. (1989). *The social organization of the computer underground* (Unpublished doctoral dissertation). Northern Illinois University.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives*, *23*(3), 3–20.

Möring, S., & Leino, O. (2016). Beyond games as political education – neo-liberalism in the contemporary computer game form. *Journal of Gaming & Virtual Worlds*, *8*(2), 145–161.

Noroozian, A., Koenders, J., Van Veldhuizen, E., Ganan, C. H., Alrwais, S., McCoy, D., & Van Eeten, M. (2019). Platforms in everything: analyzing ground-truth data on the anatomy and economics of bullet-proof hosting. In *28th USENIX Security Symposium* (pp. 1341–1356).

Ohm, P. (2008). The myth of the superuser: Fear, risk, and harm online. *UC Davis Law Review*(41), 1327–1402.

Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018). Characterizing Eve: Analysing cybercrime actors in a large underground forum. In *International symposium on research in attacks, intrusions, and defenses (RAID)* (pp. 207–227).

Pastrana, S., Thomas, D. R., Hutchings, A., & Clayton, R. (2018). CrimeBB: Enabling cybercrime research on underground forums at scale. In *Proceedings of the 2018 World Wide Web Conference* (pp. 1845–1854).

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

Raman, A., Joglekar, S., Cristofaro, E. D., Sastry, N., & Tyson, G. (2019). Challenges in the decentralised web: The Mastodon case. In *Proceedings of the Internet Measurement Conference (IMC)* (pp. 217–229). ACM. doi: 10.1145/3355369.3355572

Santanna, J. J., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). Booters – an analysis of DDoS-as-a-service attacks. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 243–251).

Sauter, M. (2013). 'LOIC will tear us apart': The impact of tool design and media portrayals in the success of activist DDoS attacks. *American Behavioral Scientist*, *57*(7), 983–1007.

Shakarian, J., Gunn, A. T., & Shakarian, P. (2016). Exploring malicious hacker forums. In *Cyber deception* (pp. 259–282). Springer.

Shammas, V. L., Sandberg, S., & Pedersen, W. (2014). Trajectories to mid-and higher-level drug crimes: Penal misrepresentations of drug dealers in Norway. *British Journal of Criminology*, *54*(4), 592–612.

Silva, S. S., Silva, R. M., Pinto, R. C., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks*, *57*(2), 378–403.

Smith, A. (1776). *An inquiry into the nature and causes of the wealth of nations*.

Smith, H. P., & Bohm, R. M. (2008). Beyond anomie: Alienation and crime. *Critical Criminology*, *16*(1), 1–15.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28-38.

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, *43*(3), 377–391.

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.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670.

Tajalizadehkhoob, S., Asghari, H., Gañán, C., & Van Eeten, M. (2014). Why them? Extracting intelligence about target selection from Zeus financial malware. In *Workshop on the Economics of Information Security*.

Thomas, D. R., Clayton, R., & Beresford, A. R. (2017). 1000 days of UDP amplification DDoS attacks. In *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 79–84).

Thomas, D. R., Pastrana, S., Hutchings, A., Clayton, R., & Beresford, A. R. (2017). Ethical issues in research using datasets of illicit origin. In *Proceedings of the Internet Measurement Conference (IMC)*. ACM.

Thomas, K., Crespo, J. A. E., Rasti, R., Picod, J. M., Phillips, C., Decoste, M., ... McCoy, D. (2016). Investigating commercial pay-per-install and the distribution of unwanted software. In *25th USENIX Security Symposium* (pp. 721–739).

Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., ... Vigna, G. (2015). Framing dependencies introduced by underground commoditization. In *Workshop on the Economics of Information Security*.

Thomas, R., & Martin, J. (2006). The underground economy: Priceless. *USENIX ;login*, *31*.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review*, *23*(1), 8–23.

Turgeman-Goldschmidt, O. (2011). Identity construction among hackers. *Cyber criminology: Exploring Internet crimes and criminal behavior*, 31–51.

Turkel, D. (2016). *Hackers are now offering 'customer support' to the victims they extort money from.* Retrieved 2020-02-26, from `https://www.businessinsider.com/ransomware-writers-offer-customer-support-to-victims-2016-1`

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Wang, A., Chang, W., Chen, S., & Mohaisen, A. (2018). Delving into Internet DDoS attacks by botnets: characterization and analysis. *IEEE/ACM Transactions on Networking*, *26*(6), 2843–2855.

Wasiak, P. (2019). Telephone networks, BBSes, and the emergence of the transnational 'warez scene'. *History and Technology*, *35*(2), 177–194.

Workman, M., Phelps, D. C., & Hare, R. C. (2013). A study of performative hactivist subcultures and threats to businesses. *Information Security Journal: A Global Perspective*, *22*(4), 187–200.

Xie, Y., Yu, F., Achan, K., Panigrahy, R., Hulten, G., & Osipkov, I. (2008). Spamming botnets: signatures and characteristics. *ACM SIGCOMM Computer Communication Review*, *38*(4), 171–182.

Yar, M. (2005a). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387–399.

Yar, M. (2005b). 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 Publications.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516–539.