Cybercrime is (often) boring: infrastructure and alienation in a deviant subculture

Ben Collier, Richard Clayton, Alice Hutchings, Daniel Thomas

Abstract

The boredom and alienation produced by capitalist societies and countervailing forces of attraction and excitement are at the heart of the subcultural account of crime. The underground hacker subculture is no exception, commonly represented as based around exciting, technically skilled practices and high-profile deviance. However, the illicit economy associated with these practices has become industrialized, developing shared infrastructures that facilitate the sale of illicit services rather than skilled technical work. We explore how this shift in the nature of work has shaped the culture and experiences of this subculture. Developing a novel concept—the 'illicit infrastructure'—and drawing on an extensive analysis of empirical data from interviews and novel data sources such as forums and chat channels, we argue that as they industrialize, deviant subcultures can begin to replicate the division of labour, cultural tensions and conditions of alienation present in mainstream capitalist economies.

Introduction

Criminologists often frame organised and subcultural forms of crime as structured around alternative systems of financial, cultural, and social capital: social systems in competition with the mainstream (Blackman, 2014). These have significant explanatory merit – either from a cultural perspective, in understanding the experiences and identifications which bring people into these communities and bind them together (Hall and Jefferson, 1976), or as structural arguments about the effects of locking particular groups out of mainstream means of success (Shildrick and MacDonald, 2006). At the core of these are the ideas of alienation – from capital, status, labour, and mainstream value systems - and attraction – to countercultural values, excitement, money, and status in these alternative social systems and structures. However, these alternative systems are not static; they grow and evolve in much the same ways as mainstream economies. We investigate the changing economic structures, forms of work, and cultural context associated with the much-discussed underground hacker subculture to explore what happens when these alternative systems begin to scale up, developing a novel concept: the 'illicit infrastructure'. Drawing on an extensive analysis of empirical data from interviews and novel data sources such as forums and chat channels, we argue that as they industrialise, these illicit economies begin to replicate the division of labour, cultural tensions, and conditions of alienation present in the mainstream economy.

Both historical and recent work have drawn, much as scholarship on other illicit subcultures, on the roles played by boredom and excitement in involvement in the underground hacker subculture, with boredom providing a 'push factor' and excitement a 'pull factor' to involvement (Steinmetz et al., 2017). The pursuit of the 'hacker ethic', the thrill of online deviance, the joy of creative experimentation, and complex technological work have been key aspects of the criminological literature on illicit online hacker subcultures – the experiences and values which underpin the systems of cultural and social capital, and the linked technical practices which underpin their economies (Holt, 2007; Steinmetz, 2016). The actors whose motivations, behaviours, and decision-making are considered by criminologists tend as a result to be those involved in active, prominent roles: researching vulnerabilities, compromising systems, and performing key functions within cybercrime groups. However, these romantic notions of those involved in cybercrime ignore the often mundane, rote, and supportive aspects of the

work which have proliferated in the online illicit economies around hacking and the infrastructures on which they rely.

We begin by discussing the literature on the underground hacker subculture, focusing on the cultural values at its heart (particularly the lone figure of the 'hacker'), its structural features, and the specific criminalised activities with which they are commonly associated. We then explore how criminologists have generally theorised involvement in the hacker subculture, particularly the role played by boredom and alienation on one hand, and the exciting, sensuous experiences of hacking on the other. Subsequently, we set out our argument that the structure of this subculture is increasingly based around shared infrastructure for committing crime which is rented as a service. We develop a novel theorisation of 'illicit infrastructure' which we explore in the remainder of the piece. After outlining our empirical methods, we identify eight core features of illicit infrastructure, concluding with a discussion of these features in the context of broader criminological scholarship. We argue that the transformation in working practices engendered by the putting down of infrastructural roots of these illicit communities radically challenges their cultural foundations – far from solely being an initiator to involvement in illicit economies, the boredom and anomie associated with industrialised capitalist societies can also become routes of desistance when illicit communities begin to mimic these formations themselves.

Hacking and online illicit subcultures

Although cybercrime is a rather contested concept, used to describe an increasingly wide range of online harms (which can include everything from online harassment to state-sponsored espionage), we avoid engaging in this piece too deeply with criminology's competing taxonomies of online harm. Instead, we focus on a set of illicit online communities associated with the 'underground hacker' subculture, which is implicated in a particular set of forms of organised online harm which rely on specialist technologies and technical practices (Turgemann-Goldschmitt, 2011).

Hacking as an activity has a long and rich history, and itself comprises a range of different cultures and practices. Ethnographic studies of hacking conceive of it as a much wider and older set of ways in which humans have always interacted with technologies, emphasising practices of creative breaking, technical mischief, and repurposing (both social and technical) systems to produce outcomes unexpected by their designers (Coleman and Golub, 2008). More conventionally, it is associated with the creative subversion of information and communication technologies, a practice with its roots in the US research labs which developed early forms of networked computing. Embedded in the broader context of US counterculture in the 1960s, these technical communities gave rise to a fully-developed cultural identity and set of values – commonly known as the hacker ethic (Levy,1984). The foundations of hacker culture (as commonly conceived) prize hard technical mastery, creative repurposing of systems, a self-taught, anti-authoritarian approach, and reflexively technolibertarian politics (often subsumed or neutralised under the idea of broad-church participation). This is bound to strong currents of both techno-utopian and techno-dystopian visions of possible futures, in which advanced information and communication technologies possess both radical capacities for democratisation, free anonymous expression, and the redistribution of power to the masses, and simultaneously terrifying potentials for control, subjugation, and surveillance (Turgemann-Goldschmitt, 2011; Coleman, 2012).

A subset of hackers and hacker practices find their home in what Golub and Coleman (2008) refer to as the 'underground hacker' subculture – communities, often organised around online forums and chat channels, who adapt hacking practices for the commission of crime. It is on these communities which we focus in this article, as they form the link between hacking and hackers, and a subset of the activities which criminologists refer to as cybercrime. The picture of the criminal hacker, which still underpins much of the criminological conception of cybercrime, is often that of the 'lone wolf' depicted in popular culture (Ohm, 2008). In this mode, the hacker is a lone, romanticised figure with a hard mastery of technology, often highly intelligent, socially disconnected, and possessed of a libertarian politics of anti-authoritarian self-reliance. This vision of criminal hacking involves

individuals researching particular systems, building their own bespoke tools and developing substantial technical expertise (Levi, 1984). While far closer to myth than reality (as these subcultures are in fact organised around groups and communities) this picture has a powerful attraction and forms the cultural core of the underground hacker subculture, the apotheosis of their values of independence, self-teaching, anti-authoritarianism, and technical prowess (Turgemann-Goldschmitt, 2011).

In terms of organisation, the classic model of these communities has moved from a view which focuses solely on the highly-skilled individual actors who do the technical work in finding vulnerabilities in systems and developing tools to exploit them (Ohm, 2008) to a top-down, or concentric, view of large subcultures of 'script kiddies' clustered around small numbers of genuinely skilled individuals (Jordan and Taylor, 1998; Hutchings, 2014). Cultural capital in the underground hacker scene is still very much linked to the cultivation of technical prowess (sometimes known as 'l337', i.e. 'leet', or 'elite' status). A (very) small core of actors actually develop so-called 'exploits' by finding vulnerabilities in technical systems, a slightly wider group package them up within tools, which they monetise and distribute, a large group of 'skids' (low-skilled novices) use these tools 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 (Porcedda & Wall, 2019).

These tools can be used to a variety of ends, and communities of practice within the hacker underground have formed around particular typologies of online crime which these tools are designed to facilitate. For example, a broad range of tools allow users to infect other computers and enrol them into a network – often called a 'botnet'- which can be used to commit further crimes. Among other uses, these botnets can be used to mount 'Denial of Service attacks' which direct large amounts of computer traffic at a victim, knocking them (or the online service they run) offline. Further, an ecosystem of tools for distributing ransomware are bought and sold in these communities, allowing users to gain access to a victim's computer system and encrypt their files, demanding a fee to allow their access to be restored. RATs – or Remote Access Trojans – can allow various remote commands to be executed on a victim's system, including recording the webcam or stealing passwords and credit card details. Finally, a range of tools are bought and sold for avoiding detection by police or others, including hiding browsing traffic, concealing viruses in files from antivirus software, and erasing incriminating information from a victim's system once the attack is complete (Yar and Steinmetz, 2019).

These tools reduce the barrier to entry: although the community still depends on the skilled artisanal labour of the elite hackers at the centre, the majority of the technical practices involved are now more like lockpicking, involving learning to use sophisticated tools created by others (Jordan and Taylor, 1998). Despite this, the tool-sharing relationships in these subcultures work to maintain the overall values of the subculture – technical work is still prized above all, and although one may start as a 'script kiddie' using other people's tools, social status can be pursued through the progressive cultivation of technical skill, as people work up to creating their own exploits and tools and selling them to others.

Theorising involvement in hacker communities

A wide set of motivations have been posited to explain participation in these organised forms of online technical offending. These revolve around the pursuit of profit, social capital, and political goals (Holt, 2007; Yar & Steinmetz, 2019; Goldsmith & Wall, 2019). Criminological framing of involvement in the underground hacker subculture has generally mirrored broader subcultural criminology, resting on a dialectic between, on one hand, processes of alienation from mainstream social systems, and on the other, processes of attraction to deviant alternatives (Blackman, 2014). In this frame, more organised forms of offending can be understood as rooted in deviant subcultures – relatively stable cultural formations which exist in opposition to the mainstream which incorporate their own cultural values (or differently-realised versions of mainstream values), systems of social status, and ways of making money through illicit economies (Hall and Jefferson, 1976; Shildrick and Macdonal,

2006). Where people are blocked from accessing mainstream ways of attaining social or financial status, or alienated from the shared values of mainstream society, they seek out alternative systems into which they can better fit. Subcultural accounts of hacking generally depict involvement as occurring where young people, often with an interest in computing or technical skills, who are experiencing difficulties in socialising at school are attracted to online hacker communities where their skills, non-standard ways of learning, involvement in deviant behaviour and social mores are appreciated rather than condemned (Yar, 2005).

Boredom, long a productive concept in criminological scholarship, plays a crucial role in the subcultural account of crime. The role of boredom as a symptom of wider alienation is core to many criminological explanations of how people become involved in deviant subcultures, and hence in criminal offending. Ferrell (2004) argues that industrial capitalist societies produce such profound forces of alienation that, although boredom is not exclusive to capitalism, the individualist, entrepreneurial norms and values which it embodies and the forms of labour on which it relies give rise to particularly corrosive and oppressive forms of boredom. This 'anomic' boredom is conceived as a broad social phenomenon of deep dissatisfaction, the deprivation of personal fulfilment, a sense of social worthlessness, and disconnection from mainstream social values and narratives around personal success (Cohen & Taylor, 1976; Leslie, 2009; Kaufman, 2017). This boredom and dissatisfaction with conventional jobs, social roles and leisure activities drives people towards alternatives (Merton, 1938; Ferrell, 2004; Smith & Bohm, 2008) including deviant subcultures such as underground hacker communities, with some criminological research on hacker pathways explicitly finding a boredom a key aspect of involvement (Steinmetz, Shafer, and Green, 2017).

In concert with these forces of alienation from the mainstream are a range of forces of *attraction* which draw people into subcultural offending. Subcultures, which are often researched through vivid ethnographic accounts and depicted in exciting and charismatic forms in the popular media (Ferrel and Hamm, 1998), offer value systems, aesthetics, and identities which can appear far more glamorous and attractive than mainstream society. Katz (1988) additionally entreats us to consider the sensory and sensuous aspects of the experience of criminalised acts such as theft, vandalism, or violence, which can be exciting, risky, and enjoyable. The sensuous nature of hacking recurs in the criminological literature – either directly playing a role in initiation (Goldsmith and Wall, 2019) or as a wider cultural experience which holds hacker communities together (Steinmetz, 2016). Participation in hacking is therefore often explained through the pursuit of challenge and stimulation, (Levy, 1984). 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). 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 hacker literature conceptualises this through 'digital drift' – from playing online video games, to becoming involved in low-level, less technical forms of online crime at the fringes of hacker communities, to progressively more serious and technically sophisticated forms of offending (Holt et al, 2019).

Thus, subcultural accounts of involvement in illegal computer hacking have generally focused on its exciting and technically skilled aspects – true to the image of the charismatic deviant hacker subculture and the values of technical mastery around which it is based (Steinmetz et al., 2017). However, as we argue in this paper, as the underground hacking subculture and its associated economy have evolved, the reality of involvement increasingly looks rather different.

The industrialisation of hacking: Towards 'illicit infrastructure'

As these underground hacker communities have grown, the associated economies for buying and selling hacking tools (as described above) have tended towards role specialisation and a move towards a service economy. This development of a service economy, often referred to as 'cybercrime-as-a-service' has involved a move from a

tool-based economy to laying down more concrete infrastructures of technologies and shared services which can be re-purposed and rented out (Garg and Camp, 2015). This illicit infrastructure means that participation in these forms of crime is less a question of moderately- or low-skilled people buying tools which they can use to commit crime, and more a question of users purchasing these capacities as a service, for which they require no technical skill whatsoever. Actors do not need to buy and learn to use the tools themselves but can merely invoke them, allowing genuine scale to be achieved. 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 (Shamas et al., 2014). 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' (Hutchings, 2014; Leukfeldt et al, 2017). Instead, we argue that this is part of more partial, 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).

In this paper, we focus on three examples, corresponding to three distinct forms this infrastructural turn tends to take. The first involves the management of a large-scale technical infrastructure. An example of this is botnets – networks of infected computers. Rather than every individual having to set up and manage their own botnet, increasingly these are rented out to others by a small number of full-time providers, who need to advertise, maintain a network of hosting servers, respond to customer complaints, and launder their profits. These botnets power a range of services, including 'booter' or 'stresser' services –which allow customers to rent the power of these botnets to carry out Denial of Service attacks without having any technical ability of their own (Hutchings and Clayton, 2016). The second occurs where a service infrastructure emerges around a set of tools which require some awkward, complex, or otherwise difficult operation to work – such as for malware which allows the theft of banking credentials, where a market has grown for providers to set-up, configure, and maintain these for customers (Hutchings and Clayton, 2017). The third is more generic supportive infrastructure which solves a range of problems for a wide number of groups: for example, specialist forums which facilitate meeting others, cultivating trust and reputation, escrow services, and advertising; or hosting services, all of which again rely on substantial maintenance work by administrators (Bancroft, 2020).

To make sense of this industrialised landscape, we develop the concept of illicit infrastructure as a crucial aspect of the progression of deviant subcultures to more organised forms of offending. In doing so, we draw on Susan Leigh Star's (1999) infrastructure studies scholarship, which suggests further theoretical avenues for making sense of these illicit infrastructures. 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 smoothly facilitates their actions with minimal friction, and the reality of how it 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 community membership: 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, and it is built on a pre-installed base, making use of existing infrastructures (such as the Internet itself) as a platform on which to build further capabilities. Finally, 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 shared illicit infrastructures and how they change the character of work in cybercrime economies, guiding research to the 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 particular, Star directs the researcher of infrastructure to focus on the 'hidden work' which supports them – an approach which we take in this paper.

The service-based aspects of cybercrime economies, and the role played by specialisation, have been well-documented in the criminological and cybersecurity literature (Broadhurst et al. 2013; Manky, 2013; Lusthaus, 2018). This has tended to focus on the specialisation and compartmentalisation of cybercrime as a service economy whilst the way in which the infrastructure is actually run has generally been overlooked. 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. Steimetz (2016) has studied hacking through the lens of political economy but emphasises the skilled labour which typifies technical enthusiast communities. Instead, we focus on the industrialisation of the underground hacker subculture, and the new forms of work which are coming to predominate.

Methods

In exploring illicit infrastructures and the work which supports them, we draw on two main qualitative data sources. The first constitutes interviews with eleven 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.

Hutchings and Holt (2018) informed our strategies when interviewing participants involved in the administration and maintenance of 'booter' services. In total, eleven interview sessions 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. These give a fairly representative sample of booter administrators, including both small and large operations, though were limited to English-language services. 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.

The Cambridge Cybercrime Centre's CrimeBB database currently archives 25 underground cybercrime forums, with over 70M posts dating back as far as 2002. These have been collected using webscrapers, which 'crawl' a website or service and archive posts systematically, which are stored as conversational 'threads' or discussions which reflect how they appeared on the original bulletin board. Alongside these, it also collects and stores hundreds of public chat channels used by illicit services such as booters, which are more ephemeral lists of posts on these sites, much like the transcript of a WhatsApp conversation. These give us a unique window into the social life of underground hacker communities – as these are often publicly accessible, they include substantial discussion of the daily life, practices, beliefs, and experiences of providers and customers. 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; Thomas et al., 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.

Analysis of these data sources was conducted on an inductive, exploratory basis, with Star's infrastructural framework acting as a guide and a 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. We inductively coded our interview data, which yielded a set of initial findings and codes which were used to drive archival research on the webforum and chat channel data. These were searched using 'data science' approaches (including keyword search and text mining) to find relevant discussions – i.e. people talking about the practices and experiences of running illicit infrastructure. A sample of these threads and posts were harvested and coded inductively. This allowed us to explore a much wider dataset of social activity for evidence of the wider presence of the themes we found in our interviews, and hence to establish these as broader phenomena of relevance to theories of offending. 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.

Features of illicit infrastructural work: the life of a deviant system administrator

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. In analysing the hidden work which supports these infrastructures in further depth, we are particularly struck by the substantial quantity of maintenance and administrative work on which these infrastructures rely. This appears to be vital to their stability and capacity, but also to operate on rather different principles from the kinds of work generally understood to be important in hacker communities. We now draw on our empirical research, focusing on characterising this largely hidden administrative work, to draw out the links between the material demands of an infrastructural illicit economy, the experiences of doing this work, and the cultural system which holds these communities together. In doing so, we identify eight important features of deviant 'infrastructural work', which we now examine in further detail.

Supportive of broader illegal activity

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 existing Internet infrastructure (and generally following its topologies), and 'plugged-in' to other existing infrastructures, such as PayPal's payment systems, or the Bitcoin and 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 different use cases 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 (a network of infected machines) 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 cryptocurrency] 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.

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 follows Star's (1999) characterisation of infrastructure as smoothly facilitating user action, with the technical workings remaining invisible except when it breaks down – with 'transparency' relating to this invisible, taken-for-granted quality (rather than the visibility of the internal workings). 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, as can be seen below in discussions of 'booter' services which provide Denial of Service attacks to knock servers and home internet connections offline:

> Don't 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 00h 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 [a type of Denial of Service attack]. 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 – *Booter provider, posted on a chat channel*

Despite the rote nature of these kinds of work, they have generally not been automated because of these groups' lack of technical skill (they may be able to purchase the necessary technology but are generally unable to automate this administrative work). 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). For booter providers, whose income comes directly from consumers, this can be of particular importance to 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, we highlight the importance of usability for these infrastructures: for example, when the popular 'Zeus' malware for stealing banking credentials (as described above) was leaked publicly, many users found this powerful specialist tool hard to use (Hutchings & Clayton, 2017). This generated profitable supportive work in configuring and maintaining the software, which in combination with the leaked software 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, and keeping services stable is a key aspect of this supportive work.

Centralisation

The third feature of this kind of work is centralisation or 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. Thus economic factors 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 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 will 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 affect 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.

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 underground hacker 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 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.

> 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) – *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.

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 anti-abuse teams 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).

> 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.

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.

> 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. – *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 these half-hearted, unenforced, and often tongue-in-cheek warnings (which are often evident), the 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... 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]. – *Administrator post in a cryptomarket forum*

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 (or at least encourage) an agreed set of norms on the broader cybercrime economy. This 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 is crucial to managing trust, reputation, and, ultimately, the success of forums, markets, and other shared infrastructural services (Bancroft et al., 2020).

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).

Boredom

The final, and potentially most important, feature of this work is 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). 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*

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 deep boredom and disenchantment, once the low ceiling of social and financial capital which can be gained from this work is reached.

Discussion and concluding thoughts

For criminologists, the complex technical detail involved in understanding sophisticated communication technologies threatens to pose a barrier to making sense of the relationships between cultural and structural or technical aspects of online deviant subcultures. 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). This theoretical/methodological approach has allowed us to unearth a wealth of hidden work within cybercrime economies, and to bring to prominence the proliferation of forms of tedious supportive work in cybercrime economies. In this concluding section, we reflect on the implications for criminological research - in particular, on the role played by illicit infrastructure, boredom and alienation.

The tedious nature of much of the work involved in maintaining more organised forms of crime and the importance of supportive, mediating and administrative roles is a common feature in research on other illegal economies (Cook et al. 2014). In addition, this research also characterises the progression of these economies from excitement and experimentation to more business-like 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, with the attendant service economy largely focused around the provision of supportive technical infrastructure. The concept we develop – illicit

infrastructure – allows us to understand how this has transformed the nature of work, experiences, practices, and criminal phenomena in these communities. Infrastructure allows social phenomena to scale – rather than having to assemble tools, services, practices every time to achieve a result, it allows these to be taken for granted so that higher-level and greater-scale systems can be constructed. As we have argued, illicit infrastructure not only allows for more organised structural forms in illicit communities, but changes the nature of offending in a variety of ways: it diffuses risk, contributes to a narrower, more tightly-drawn set of norms which are more heavily policed, and shifts illegal practices towards maintenance and customer service.

In following Katz's (1988) focus on the sensuous experiences of criminalised activities and subcultures, and Star's (1999) focus on hidden infrastructural work we have explored a previously largely hidden form of illicit work and the lived experiences of the people who engage in it. Thus, our work frames boredom and its implication in illegal subcultures and economies rather differently from previous criminological scholarship. As opposed to understandings of involvement in crime as being born of boredom, (which put a focus on individual, low-level crime), we find that as the underground hacker subculture has developed into more organised and industrialised economies, the shift to shared illicit infrastructure has proliferated a range of tedious supportive forms of labour, much as in mainstream industrialised economies, with participation becoming less about charismatic transgression and deviant identity, and more about stability and the management and diffusion of risk. These new forms of labour are producing a rich and embodied experience of deep boredom potentially every bit as intense and characterful as the rush of excitement which Katz associates with crime, (and the excitement which the traditional picture of hacking associates with the more technical and creative work on which it focuses).

We therefore draw a connection between the structural organisation of an illicit economy and the cultural organisation of these communities. The infrastructural shift in the technological and practice-based underpinnings of these illicit markets has produced a concomitant shift in the nature of their labour practices, and hence in the experience of being part of the hacker subculture. Although the criminological literature generally theorises boredom, anomie, and alienation as driving involvement in deviant subcultures, in our study, we see deviant subcultures themselves producing forces of alienation which, when conceived within the criminal career, can lead to a novel route to desistance – boredom, disaffection, and burnout. This may be a crucial and under-considered aspect of how motivation is lost in criminal careers – that the entrepreneurial, competitive values and tedious industrialised work involved in more organised forms of crime may weaken the cultural bonds keeping people involved. This produces an interesting development to Wacquant's (2004) account of crime under capitalism: it may be that deviant subcultures are themselves no less vulnerable than mainstream social formations to the hypocrisies and contradictions within the 'civilising' cultural and organisational forms of entrepreneurial capitalism.

Our novel concept of illicit infrastructure reveals a crucial stage in the transition of subcultures to more organised forms of offending and more developed economies, fundamentally changing the nature of offending and permitting 'volume' crime. This work suggests further avenues for investigation, particularly, a renewed focus on crime as work, and on the roles played by infrastructure in supporting scale in illicit economies. There are some limitations to this study – we focused on communities in the underground hacker subculture, and where these illicit services are run by established organised crime groups, the 'hacker ethic' and attendant cultural forces may be less important in involvement. Additionally, this study elides the connections between these kinds of work and how people might move between them, suggesting the possibility for further longitudinal studies of pathways people take into, within, and out of these communities. As regards policy, our research suggests that efforts targeting this infrastructure (often termed 'whack-a-mole', as services that are shut down simply reappear elsewhere) may be more effective than previously thought, as they compound the tedious nature of these jobs. However, it remains for future research to consider how best to persuade those involved 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.

References

Bancroft, A., Squirrell, T., Zaunseder, A., & Rafanell, I. (2020). Producing Trust Among Illicit Actors: A Techno-Social Approach to an Online Illicit Market. *Sociological Research Online*, *25*(3), 456-472.

British Society of Criminology. (2015). *Statement of ethics*, 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

Blackman, S. (2014). Subculture theory: An historical and contemporary assessment of the concept for understanding deviance. *Deviant Behaviour*, *35*(6), 496-512.

Clement, M., & Mennell, S. (2020). Elias, ultra-realism and double-binds: Violence in the streets and the state. *European Journal of Criminology*

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

Coleman, E. G. (2012). *Coding freedom: The ethics and aesthetics of hacking*. Princeton University Press.

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.

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.

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.

Ferrell, J., & Hamm, M. S. (1998). *Ethnography at the edge: Crime, deviance, and field research*. Upne.

Garg, V., & Camp, L. J. (2015). Why cybercrime?. *ACM SIGCAS Computers and Society*, *45*(2), 20-28.

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

Hall, S., & Jefferson, T. (Eds.). (1976). *Resistance through rituals: Youth subcultures in post-war Britain* (Vol. 7). Psychology Press.

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.

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., 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., & 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.

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

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

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

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, 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.

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

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.

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

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

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).

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.

Shildrick, T., & MacDonald, R. (2006). In defence of subculture: young people, leisure and social divisions. *Journal of Youth Studies*, *9*(2), 125-140.

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

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.

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.

Turgeman-Goldschmidt, O. (2011). Identity construction among hackers. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, 31–51. CRC Press, New York

Wacquant, L. 2004. "Decivilizing and demonizing in the dark ghetto". In The sociology of Norbert Elias, Edited by: Loyal, S. and Quilley, S. Cambridge: Cambridge University Press

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

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