doi:10.1093/bjc/azu061 BRIT. J. CRIMINOL. (2015) **55**, 125–145
Advance Access publication 14 September 2014

CRAFT(Y)NESS

An Ethnographic Study of Hacking

Kevin F. Steinmetz*

The idea of the 'hacker' is a contested concept both inside and outside the hacker community, including academia. Addressing such contestation the current study uses ethnographic field research and content analysis to create a grounded understanding of 'the hacker'. In doing so, hacking is revealed to parallel features found in craftwork, often sharing (1) a particular mentality, (2) an emphasis on skill, (3) a sense of ownership over tools and objects of labour, (4) guild-like social and learning structures, (5) a deep sense of commitment, (6) an emphasis on process over result, (7) a common phenomenological experience, and (8) tendencies towards transgression. The final result is that hacking is identified as a kind of transgressive craft or craft(y).

Keywords: hacking, hackers, ethnography, craft, transgression

Introduction

As various societies throughout the world become increasingly networked, concern correspondingly rises over potential threats to technological infrastructures. Of these threats perhaps those considered the most dire fall under the umbrella of technocrime.[1] In 2011, it was estimated that the annual cost of technocrime in the United Kingdom was approximately £27 billion (The Cost of Cyber Crime 2011). One report estimates that the cost of technocrime activity in the United States ranges from $24 to $120 billion annually with yearly costs ranging as high as $300 billion to $1 trillion globally (The Economic Impact of Cybercrime and Cyber Espionage 2013). The US Bureau of Justice Statistics estimates that, among 7,818 businesses surveyed, 67 per cent have experienced some form of technocrime or network attack (Rantala 2008). Despite problems and potential biases underpinning the estimations of technocrime incidences and harms, these numbers are associated with tremendous concern among businesses, policymakers, and the public. For many, the character behind these technocrimes is *the hacker*. It is with this figure that the current study is occupied.

Hacking has come to denote any person engaged in an array of high-tech trouble-making. Originally, the term hacker did not carry such a pejorative connotation (Levy 1984; Turkle 1984). Instead, the label has been transmogrified over time through social construction (Hollinger 1991; Halbert 1997; Taylor 1999; Skibell 2002; Yar 2013) to the point where hackers are now cast as the 'archetypal "cybercriminal"' (Wall 2007: 46). In actuality, such a narrow image of the hacker concerns the criminal element of a *subarea*

*Kevin F. Steinmetz, Department of Sociology, Anthropology, and Social Work at Kansas State University, 204 Waters Hall, Manhattan, KS 66506, USA; kfsteinmetz@ksu.edu.

[1] Based on the arguments of Leman-Langlois (2013), the term 'technocrime' has been chosen for use rather than 'cybercrime' to describe various types of technological malfeasance.

of hacking (often referred to as security hacking) and other technocriminals rather than the hacking community at large. The result of such obfuscation is that hacking has become a concept mired in disagreement both within and outside the hacking community (Taylor 1999).

In the literature, hackers have been described in a number of ways which extend beyond these distorted public perceptions, many of which are explicitly non-criminal. These include—but are not limited to—various kinds of open-source software programming and computer hardware manipulation (Levy 1984; Taylor 1999; Coleman 2013). As one hacker described in an interview, the criminal stereotype of the hacker may not be as prevalent in the hacking community as believed: 'they are a minority but they are a loud minority'. In this way, it is not a criminal element that characterizes hacking as a subculture. Rather, as articulated in this study, other cultural and phenomenological components seem more suited to describe the essence of the overarching hacker community.

Previous work in criminology has generated outstanding insights into hacker culture but most attention has been given—for understandable reasons—towards the areas of security hacking and related forms of technological malfeasance. Scholars have dedicated themselves towards analysing key components of security hacking including divisions among security hackers (crackers v. hackers, black v. white hats, etc.) (Wall 2007; Yar 2013), cultural/learning dynamics (Holt 2009; 2010), and different perspectives among computer security engineers towards such hackers (Taylor 1999), to name a few. While such efforts have contributed to the discipline's understanding of hacking, the result is that relatively little time has been devoted towards developing a robust conceptual understanding of hacking *sensitive to the broader subculture*. It is the contention of this analysis that scholarship would be enriched by research attuned to such a gap. In this manner, any conceptualization of hacking should be equally capable of describing generalities about security hacking *and* other kinds of hackers such as those dedicated towards open-source software programming (Coleman and Golub 2008; Söderberg 2008; Coleman 2013). Though great strides have been made in the area of hacking (and technocrime generally), the fear is that criminology may have moved beyond definitional issues prematurely—an oversight this analysis addresses.

To create a subculturally grounded understanding of *the hacker*, the current study uses ethnographic field research and content analysis. This endeavour is based in the cultural criminological enterprise of examining meaning and sense-making (Ferrell 2013). In this manner, the current study attempts to move beyond contested and taken-for-granted understandings to find the core of hacking. As such, this project is also one of phenomenological eidetic reduction, an approach concerned with isolating the eidos—essence—of a particular subject (Palermo 1978). The aim is to uncover those perceptual qualities which allow for the onlooker to distinguish the subject—in this case, hackers—from similar others. Additionally, similar to Becker's (1963) descriptions of marijuana users, the emphasis is not on whether a person *is* or *is not* a hacker but, rather, the features that one begins to embody in the *process of becoming a hacker*.

In challenging taken-for-granted notions and seeking the eidos of becoming a hacker, this study finds that hacking is a late-modern transgressive craft. The majority of this analysis focuses on the parallels between hacking and craftwork, drawing

primarily from the theoretical work of Richard Sennett (2008).[2] Such an undertaking builds from previous research framing crime as *work* (e.g. Letkemann 1973; Sutherland 1937; King and Chambliss 1984; Fagan and Freeman 1999; Adler 2003). These studies find that 'various dimensions of work [or other related occupational labels such as "professional"] appear to be as applicable, for the purposes of study, to the illegitimate as to the legitimate worker' (Letkemann 1973: 6).[3] To this end, the current study makes a unique contribution—the hacking essence orients around a specific kind of labour—*craft*. This study also finds that the hacking eidos involves the cultural criminological notion of *transgression* (Ferrell *et al.* 2008), which is also related to craftwork.

The organization for the current study is as follows. First, a brief review of the literature is presented. Second, the research methods used in this study—ethnographic field research and content analysis—are described. This analysis then turns to exploring the results of this study, finding that hacking is perhaps best thought of as a kind of late-modern technological craft. In particular, this study details eight components of hacking/craft which include: (1) a mentality, (2) an emphasis on skill, (3) a sense of ownership, (4) social and learning structures with parallels to guilds, (5) commitment, (6) an emphasis of means over ends, (7) a particular experience, and (8) an underlying transgressive edge. Finally, this study concludes with a definition of hacking useful as a foundation for scholars inside and outside of criminology.

A Petit Review of Hacking

In the literature, hackers have been described as interested in tinkering with and advancing hardware (Levy 1984; Taylor 1999) or software (Taylor 1999; Coleman 2013), engaged in politics through technological means (such as through 'hacktivism') (McKenzie 1999; Meikle 2002; Taylor 2005), and engaged in online thrill-seeking, trespassing, or creating various forms of malware (Jordan and Taylor 1998; Wall 2007). Springing from institutions like MIT in the late 1950s and 1960s (Levy 1984), hacking has emerged as a force driven by creativity, ambition, and technological development. It has simultaneously been a force of technological progress and concern for those trying to maintain stable computational infrastructures. Hacking proliferated with the advent of computer networks and, in particular, with the rise of bulletin board systems (BBSs) (Coleman 2013). Throughout its progression, hacking has involved creating and sharing code, figuring out new ways to solve problems, and probing/overcoming security systems. Hacking culture has also developed alongside technology (Jordan and Taylor 1998), been culturally transformative (Thomas 2002), and been interconnected with political economy (Söderberg 2008).

The literature is replete with descriptions of a cultural spirit interwoven with hacking. Perhaps the most popular characterization has been the idea of the *hacker ethic*—coined by Levy (1984) as a hands-on approach to technology valuing access to computers and code. Some authors have characterized the ethic as a departure from the Protestant Ethic towards a blurring between labour and leisure (Himanen 2001; Brown 2008).

[2] While Sennett (2008) uses the terms 'craftsmanship' and 'craftsman', the current study uses 'craftsperson' and 'craftwork' to avoid unnecessarily gendering the analysis. While the hacker community is predominantly male (Bachmann 2010), it is by no means *exclusively* male.

[3] References to crime as work or labour should not be confused with the related but separate concept of the 'criminal career' (Blumstein *et al.* 1986).

Coleman and Golub (2008) highlight the streak of liberalism underpinning hacker culture while Warnick (2004) describes hacking cultural perceptions as shaped by the ontological metaphor of 'the world is a computer'. Additionally, hacker culture is characterized by a sense of technological utopianism (Barbrook and Cameron 2001), that all problems in society can be solved through technological/engineering fixes.

As previously mentioned, confusion surrounds the term hacker. In particular, social construction has confounded understanding (Hollinger 1991; Halbert 1997; Taylor 1999; Skibell 2002; Yar 2013). Almost any time a computer crime is committed in the media, the violator is referred to as a *hacker* (Holt 2009; Turgeman-Goldschmidt 2011). Such a veiled perspective on hacking is disjointed from historical and subcultural understandings (e.g. Levy 1984; Coleman 2013). Further confusion has been wrought from recent events surrounding 'hacktivist' groups (McKenzie 1999; Meikle 2002), which has reinforced the negative perception that hackers are threats, further obfuscating the image of hacking.

While the previous literature is replete with incisive examinations of hacker culture (see Turkle 1984; Jordan and Taylor 1998; Taylor 1999; Thomas 2002; Turgeman-Goldschmidt 2005; Coleman and Golub 2008; Holt 2010; Coleman 2012; 2013; Steinmetz and Gerber 2014), there have been few which have sought to isolate a useful conceptual understanding of hacking. Many elucidate cultural features and dynamics which are part of hacker culture, but little attention has been given towards the specific question *what is a hacker*? Most acknowledge the contested nature of the term and then adopt one narrow definition and proceed with the analysis. The current seeks to further fill this conceptual void.

Method

Two different forms of data are combined in this study—ethnographic field research and content analysis. The current study is ethnographic in the sense that it 'rests on the peculiar practice of representing the social reality of others through the analysis of one's own experience in the world of these others' (Van Maanen 1988/2011: xiii). To express the participants' social realities towards hacking, both participant observation and semi-structured interviews are used in this study with the presentation of results drawing heavily from their own words. The researcher began attending public meetings for a hacker group (given the pseudonym Union Hack) in June 2012. Field sites included various restaurants, bars, and hackerspaces in which this group congregated. Additionally, the members of Union Hack encouraged participation at DEF CON 21—one of the largest hacking conventions in the world—which marked the end of formal data collection in August 2013. In this study, overt participant observation was used and was chosen for ethical (Bulmer 1982) as well as pragmatic reasons; hackers are often intelligent with access to resources. Deceit may unravel quickly. Approximately 137 hours and 20 minutes were spent in the field. Field exposure ranged anywhere from 40 minutes to 17 hours at a time.

In addition to participant observation data, 16 in-depth semi-structured interviews were conducted with 14 members of the group or their close affiliates. Informed consent was gathered and each participant was assigned a pseudonym to protect their confidentiality. Interviews ranged from 58 minutes to 5 hours and 4 minutes. With the exception of two, all interviews were audio-recorded and fully transcribed. Table 1 presents demographic information for the participants.

To broaden the data beyond Union Hack, the current study also employs ethnographic content analysis (Altheide 1987) of *2600: The Hacker Quarterly*—one of the 'first

significant hacker publications' (Thomas 2005: 604). In publication consistently since 1984, this 'zine' is written largely by hackers, for hackers.[4] Inclusion of such data is valuable because ethnographic content analysis 'is used to document and understand the communication of meaning, as well as verify theoretical relationships' (Altheide 1987: 86)—a venture of central importance in the current analysis.

The sample was drawn from 41 issues of *2600* ranging from the Spring 2002 issue to Spring 2012. Items included for analysis are articles, editorials, book reviews, and short stories. A total of 839 articles, 41 editorials, 8 short stories, and 2 reviews (collectively referred to as *items*) written by 611 different authors comprise the initial sample (Table 2). To generate the subsample for analysis, purposive sampling was used to find

Table 1 *Interviewee demographic information*[a]

Variable	Interviewees (%)
Age	
Mean	~35[b]
Range	23–61
Race/ethnicity	
White	13 (92.85)
Indian	1 (7.15)
Gender	
Male	13 (92.85)
Female	1 (7.15)
Marital status	
Single	6 (42.85)
Married	6 (42.85)
Divorced	2 (14.29)
Has children	4 (28.57)
Education	
High school	1 (7.15)[c]
In college	3 (21.14)
Some college	2 (14.29)
Associate's	1 (7.15)
Bachelor's	6 (42.85)
Master's	1 (7.15)

[a]These demographics roughly parallel Bachmann's (2010) demographic study.
[b]Some participants were reluctant to give their real age and only gave approximations.
[c]Of note, the participant with a high school diploma possesses an honorary doctorate.

Table 2 *Content analysis descriptive statistics*

Items	Full sample	Subsample
No. of items	893	193
Articles	839	163
Editorials	41	29
Reviews	2	0
Short stories	8	1
No. of authors	611[a]	143

[a]Some authors were included, which may be duplicates with slight variations on names like kaige and kaigeX. Omitting duplicates brings the number to 608.

[4] A 'zine' is a self-published magazine, typically with a small circulation amongst a niche population.

all items within the full sample (all 41 issues), which discussed the nature of hacking and hackers. The relevant items were then flagged and logged in an electronic dataset. This process resulted in the creation of a subsample for analysis, which consists of 193 articles, 29 editorials, and 1 short story by 143 different authors.

The coding approach adopted for the current study is *grounded theory* (Glaser and Strauss 1967). Grounded theory methods of analysis 'consist of flexible strategies for focusing and expediting qualitative data collection and analysis' and 'provide a set of inductive steps that successively lead the researcher from studying concrete realities to rendering a conceptual understanding of them' (Charmaz 2002: 675). Involved is an iterative, multi-level analytic approach geared towards developing themes and categories inductively, ideally resulting in a theoretical explanatory apparatus uniquely tailored to the data. The qualitative analysis software Atlas.ti was used to organize the field research data to facilitate coding while Excel 2010 was used for the content analysis data.

Hacking as Craft

In seeking the eidos, the results indicate hacking qualifies as a late-modern transgressive technological craft. Richard Sennett's (2008) theoretical work is used in this analysis to provide guideposts throughout to illustrate the connection between hacking and craft. Craft is 'the skill of making things well' (Sennett 2008: 8). Previous research has discussed criminal/deviant activity through an occupational lens (Sutherland 1937; Letkemann 1973; King and Chambliss 1984; Fagan and Freeman 1999; Adler 2003). Hacking is not discussed here as a mere vocation or occupation, however. Hacking should be understood as a particular type of skilled labour—craftwork.

Importantly, many of the cultural features of hacking described in previous academic literature and found in this study can be understood as materializing from the craft-life approach taken towards hacking—emerging from what Sennett (2008) describes as the relationship between the head and the hand. As Thomas (2002) explains, the culture of hacking develops in tandem with technological progress. Understanding hacking as craft gives us the theoretical tools to understand how this relationship manifests—through the dialectics between technological progress and direct work with technology. In this study, the hacking–craft relationship is described through eight features: (1) a particular mentality, (2) an emphasis on skill, (3) a sense of ownership over tools and objects of labour, (4) guild-like social and learning structures, (5) a deep sense of commitment, (6) an emphasis on process over result, (7) a common phenomenological experience, and (8) the politics of resistance/transgressive tendencies. Each feature is discussed in turn (Table 3).

The hacker mentality

The cultural mentality of hacking is a key feature of the hacker essence (interviewees = 14; 100 per cent; CA items = 124; 64.25 per cent). Five components comprise this mentality. The first is *curiosity*. Russell describes hacker curiosity by stating: 'So, to me, it's more like curiosity of… what can it do? What can I make it do to make my life easier?' Dr Zoltan (2008: 57) describes the core of hacking as 'exploration, led by curiosity'. Such curiosity is also indicative of hacking's relationship to craftwork: 'all of his

Table 3 *Components of being a hacker*[a]

Theme	Interviewees (%)	Articles (%)
The hacker mentality	14 (100)	124 (64.25)
Skill	13 (92.86)	33 (17.10)
Ownership	11 (78.57)	118 (61.14)
As guild	10 (71.43)	50 (25.91)
Commitment	10 (71.43)	25 (12.95)
Journey over destination	9 (64.29)	23 (11.92)
Experience	10 (71.43)	20 (10.36)
Hacking as transgression	13 (92.86)	86 (44.56)

[a]Frequencies from participant observation data are omitted because of the difficulty presented by creating distinct counts from these types of data.

or her [the craftsperson] efforts to do good-quality work depend on curiosity about the material at hand' (Sennett 2008: 120).

The second hacker mentality component is a *problem-solving orientation*. This orientation can be seen in many of the social elements of hacker culture. For example, DEF CON is rife with puzzles for its members to solve such as various games (like capture the flag, a security hacking challenge). Even the badges worn for admittance into the convention are puzzles because, as the badge designer—LosTboY—stated, a great way to get hackers to socialize is to present problems to solve. Such a problem-solving orientation is also deeply embedded in the act of craftwork (Sennett 2008).

Systematic and technical thinking comprise the third element of the hacker mentality. This component perhaps is the most apparent in its parallels to craftwork—the ability to approach a problem in a manner which is efficient and systematic. Harvey provides an example of this kind of thinking when he describes hacking as creating an efficient and technically sophisticated solution:

> I'm in the PHP configuration file, I'm dicking around with… [and I think] 'And you know what? I bet I can shave a couple cycles if I use this command instead of that command… or if I write a specialized function that does this this way as opposed to that.' I get all excited. And that, that is to me what hacking is.

The fourth component of the hacker mentality is thinking in a *creative and unconventional manner*. It is not enough to approach things in a logical and critical capacity but one has to be willing to think unorthodoxly. *2600* author Ninja_of_Comp (2011: 31) describes this creativity as 'outside the box' thinking that 'looks for different ways to solve a problem'. Interviewee Rick also describes hacking as a creative and unorthodox approach, relying on a metaphor which characterizes creativity as a means past restrictions:

> You've probably seen a jail with all those bars. Some people see the bars. Some people see the *spaces between the bars*. We always saw the spaces between the bars. And we're always baffled that other people didn't see the spaces between the bars…

In 'seeing the spaces between the bars', Rick highlights the importance of being able to see things in an unconventional way. Sennett (2008) describes the idea that craftsmanship often involves using tools designed for one purpose for alternative purposes in

which they were not initially designed—improvisation, a greatly valued ability amongst hackers, is an example of the value of creativity and unconventionality in craftwork. Additionally, the problem-solving orientation, systematic and technical thinking, and creative unorthodoxy combine together into what Sennett (2008: 30) refers to as 'practical creativity'.

The final element of the hacker mentality is an *orientation towards breaking and creating*—thinking about things in terms of their capacity to be taken apart, broken, fixed, and reconfigured. Aidan summarizes the breaking component of hacking by stating, '[Hacking is] basically taking it apart to see if you can put it back together again. I mean, it's tinkering… figuring out what makes it do what it does and… ways to break it'. The desire to take things apart and put them back together echoes the craftsperson's desire to fix things as a method of learning—'Put simply, it is by fixing things that we often get to understand how they work' (Sennett 2008: 199). While the act of simply repairing something and putting it back together is referred to as a *static* repair, *dynamic* repairs are a key part of hacking culture. Dynamic repairs 'will change the object's current form or function once it is reassembled' (Sennett 2008: 200).

Skill

Hacking is beyond computers, beyond intrusions, and beyond programming. Hacking is about the possession and development of *skill* (interviewees = 13; 92.86 per cent; CA items = 33; 17.10 per cent) (see also Turkle 1984; Taylor 1999; Holt 2010). Similarly, Sennett (2008: 20) states, '[a]ll craftsmanship is founded on skill developed to a high degree'.[5] Skill can be simply defined as 'a trained practice' (Sennett 2008: 37)—a definition which implies that skill is more a product of labour and development than raw talent. Regardless of the domain in which one hacks, the honing and exercising of skill is characteristic. Just as Sutherland (1937: 14) states that 'a thief is not a professional until he is proficient', a person is not a hacker until they are skilled. By and large, acts which do not stem from a degree of skill are not considered hacking. Rick describes, in detail, the amount of skill Steve Wozniak put into his work, notably describing it as 'magic':

> If you look at the Apple world and the shit Woz did, it was crazy. People cannot even grasp the shit he did. He basically made a color computer out of nothing. Almost magic. Just by changing timing and seeing what happened on the computer. I mean, he used, like, no chips.

In fact, the very process of becoming a hacker involves the development of skill and its recognition by others, similar to Sutherland's (1937: viii) description of professional thieves, 'No one is a professional thief unless he is recognized as such by other professional thieves'. In this vein, Farr (2008: 26) illustrates these dynamics among hackers:

> Most of the people in the room, however, are 'newbies'. … In a few Mondays, after getting a little experience with a soldering iron, a few code samples, a bit of encouragement, and a kit of their own, a few of these newbies will start contributing ideas and hacks of their own—and be recognized by their peers as fellow hackers.

[5] Other research focusing on deviance/crime as work has discussed the necessity of skill (e.g. Sutherland 1937; Letkemann 1973; Fagan and Freeman 1999).

Through the pursuit of challenges, implementation of intelligence, and exertion of effort, hackers come into their own—their status as hackers only increasing with the development and expression of their abilities. In this sense, as previously described, hacking is an act of becoming rather than a matter of 'is' or 'is not'. As one develops skill, they move closer to the culturally negotiated idea of 'hacker'. Drawing hard and fast distinctions between when a person is or is not a hacker based on skill is difficult as there is no measurable threshold. Rather, each hacker must culturally and situationally negotiate their position as a hacker through the possession, development, and implementation of skill.

Sennett (2008: 20) describes the relationship between craft and skill as one where, 'as skill progresses, it becomes more problem-attuned'. In this sense, there is a strong relationship between the development of skills for hackers and the problem-solving orientation previously described. Further, Sennett (2008: 26) states, 'the experimental rhythm of problem solving and problem finding makes the ancient potter and the modern programmer members of the same tribe'. Hacking involves not just a process of problem solving but, as skill increases, the ability to find problems to solve. Indeed, problem solving and problem finding are vital to the process of skill development (Sennett 2008).

Ownership

When an artisan pursues a craft, there is an intimately close relationship between the person, their tools, and the creation. Through time, commitment, and skill the artisan pours themselves into the object, leaving their mark upon it or, in some cases, a literal brand (Sennett 2008). As such, the craftsperson possesses a sense of *ownership* over the item, being completely unalienated in their labour. Involved is both a sense of ownership over the act of labour itself as well as over technology—the latter perhaps most familiar through hacker slang of 'owning' a machine by gaining control through bypassing security. Hackers, as artisans, take ownership of the items of their interests in multiple ways (interviewees = 11; 78.57 per cent; CA items = 118; 61.14 per cent). Such an emphasis can be seen through hacker assertions about the importance of being hands-on—similar to Levy's (1984) 'hands-on imperative'—and thoroughly knowing technology with an emphasis on modifying technology.

The breaking of restrictions—both technological and legal—on software and hardware is another way that hackers demonstrate ownership over technology. The presence of restrictions means a third party is asserting control on the relationship between hackers and technology. For instance, Rick describes going to hacker parties as a youth where the participants created methods for breaking software copy-protection mechanisms. Rick describes the rationality as such, '*The goal is to make your computer do what you want it to do. Not what somebody else wants it to do* [emphasis added]. . .The computer answers to me. Not… not to you'. In the narrative Rick provides, both technological and legislative restrictions—in the form of copy-protection methods and copyright law—were circumvented because both obstructed the relationship between themselves (hackers) and the computer: '*the goal is to make your computer do what you want it to do. Not what somebody else wants it to do.*' Such assertions about ownership also invoke notions of autonomy, independence, and freedom. These likely spring from liberalist underpinnings permeating hacker culture (Coleman and Golub 2008), which are particularly

evident around hackers involved in open-source software projects (Coleman 2013). As such, the closing of distance between a craftsperson/hacker, their tools, and objects of labour indicate a greater political struggle occurring within the very act of hacking—resistance against control and the value of autonomy.

Hacking as a guild: self-sufficiency and group learning

The hacking community can be viewed as a kind of guild (interviewees = 10; 71.43 per cent; CA items = 50; 25.91 per cent). After all, both guilds and hacking carry a 'collective agent' (Sennett 2008: 73), which manifests here as hacker groups and/or the broader hacker community. Craftspersons within guilds predominantly operated individualistically or in small groups, only to come together as a guild when necessary to control and develop the trade (Sennett 2008). Hackers operate in a similar manner, often engaging technology in isolation while also being social creatures with a desire to learn from and share information with others.

To start, the activity of hacking involves autonomy. As Miles points out, 'they tend to be self-started. Self-starters, self-learning.' Valnour (2009: 32) describes his experience in learning to hack, borrowing language from the Star Wars franchise, 'I was beginning to identify with the hacker world, but very much considered myself a padawan [apprentice] without a master. I am sure many of you can identify with me at that age'. In this sense, there is *some* truth to the stereotype of the hacker loner. Often hacking is a solitary activity involving long hours in front of a computer or other piece of technology to accomplish a task or learn. The individual is valued as demonstrated by the often libertarian or anarchistic flair in hacker politics (Barbrook and Cameron 2001; Jordan and Taylor 2004; Coleman and Golub 2008). This emphasis on the individual is similar to trades where the craftsperson is centre (particularly compared with mass-production settings).

In a guild, however, the individual does not operate in a vacuum. Often training is conducted on the basis of mentorship between a master and an apprentice. Additionally, the artisan will learn, teach, and work within the context of the guild. Hackers have similar dynamics that are modified in the age of the Internet. In this sense, the direct relationship between hackers' work with technology and technological progress mediates and influences social interactions as well (Thomas 2002). Such social mechanisms are important as learning to hack in isolation can be difficult. As Russell describes, sometimes, 'you are too ignorant to know what you don't know. So, you can't really form the questions. So, you don't know what to ask to advance'. In short, social learning is important for development as a hacker (Holt 2010).

Like the master–apprenticeship relationships in guilds, various forms of apprenticeship can be found in the hacker community. First, one-on-one mentorship relationships can occur. Danny describes some of his earliest experiences in his hacker education involving a friend he met online. This friend showed him how to engage in various hacking-related behaviours, such as 'dropping dox'—an act which involves breaking through an individual's perceived sense of anonymity by uncovering personal details about them, often ending with the delivery of documents or 'dox' to the target. Hacker apprenticeship can also occur in a broader group setting. Reflecting on a time before Web 2.0, Rick described his first encounter with a hacker group. He indicated that his learning accelerated when he was among others capable of teaching him various tricks of the trade such as bypassing early forms of software copy protections.

Finally, the Internet and other computer networks serve as late-modern mechanisms for vicarious apprenticeship. Rick, Harvey, and Miles described learning about computers and hacking by accessing early BBSs where individuals would upload text files from which other hackers or would-be hackers would learn. Danny, Keith, and Gilbert described learning from Internet message boards or other repositories such as happyhacker.net. In this way, hackers write material to be accessible by other hackers, thus providing an indirect form of community mentorship reminiscent of guild trade books (Sennett 2008). Additionally, some of these digital localities are sources for others to ask questions in lieu of more direct mentorship relationships where they often are given the answers they seek or are told to RTFM or 'read the fucking manual' (see also Holt 2010).

Much like guild systems, hackers also stratify the community by skill level. In a guild, crafts are organized in terms of apprentices, journeymen, and masters (Epstein 1998; Sennett 2008). As a person progresses in skill, they move up the ranks. In the hacking community, a similar stratification method is present. At the lowest skill level there are 'script kiddies', 'newbies' or 'n00bs'. As one progresses in skill, one comes nearer to being a hacker. Someone can be considered a 'master' when they reach the 'next level' (as described by Susan) or 'elite' (Thomas 2002) and create an original, clever, and creative hack that required tremendous skill to execute.

Commitment

To become a master craftsman, one needs to be devoted to their trade (interviewees = 10; 71.43 per cent; CA items = 25; 12.95 per cent). Sennett (2008: 9) describes this as 'commitment'. Commitment has been found to be important for work in other criminological areas (Letkemann 1973; Fagan and Freeman 1999). Similarly, hackers are characterized by a deep commitment towards hacking. Susan summarizes such devotion as, 'The thing about hackers is they love to learn' and 'what it means to hack is to just take an interest in how things work'. Roger describes hackers as, 'tech savvy, geeky people with big passionate interests'. Further, he recognizes that it takes a lot of work and skill to become a hacker but, perhaps equally important, enthusiasm matters as well: 'I think it takes actually a lot of study and a lot of homework and a lot of enthusiasm.' *2600* author mirrorshades (2005: 50) describes hacker commitment in the following terms, 'I do what I do because I love computers… What I do goes beyond interest, beyond hobby, beyond obsession.' In this way, hackers are 'caught up in an intense need to master—to master perfectly—their medium' (Turkle 1984: 207).

The journey, not the destination

As previously stated, hacking is not about technology or the challenges therein *per se*, but about the process of hacking itself—of overcoming an obstacle (interviewees = 9; 64.29 per cent; CA items = 23; 11.92 per cent). As Sennett (2008: 9) describes, '[c]raftsmanship names an enduring, basic human impulse, the desire to do a job well for its own sake'. Similarly, as Susan states, 'hacking is about the journey and the process', not the destination. The process of hacking, according to Aidan, concerns '*getting* [emphasis added] to that end result versus the end result itself… the journey being more important than

the destination and all that'. Hacking, like craft, is considered to be embedded in the process of accomplishing a goal or overcoming a challenge rather than the challenge itself. Such descriptions of hacking parallel Turkle's (1984: 201) description of hacking, reinforcing the connection between hacking and this dynamic of craftwork: 'What is different for many hackers is that the means–ends relationship is dropped. The fascination is with the machine itself. Contact with the tool is its own reward'.

The hacker experience and craftwork

The deviant experience itself—with all of its emotional passions and perils—is a viable and important domain for inquiry (Katz 1988; Hayward 2004; Ferrell *et al.* 2008). Such an endeavour is dedicated towards moving beyond the 'background' factors of criminality to the 'foreground' thus illuminating the significance of the very experience of crime and deviance (Katz, 1988; Hayward, 2004). The current analysis includes an investigation of the emotional experience of hacking as vital towards understanding the hacking eidos. In doing so, similarities were found with the emotional experiences of craftwork (interviewees = 10; 71.43 per cent; CA items = 20; 10.36 per cent). The analysis is divided into two separate subsections. The first is a discussion of what it feels like to engage in the *process of hacking* followed by an investigation into the sensations experienced upon *completing a hack*.

The process of hacking

The participants in this study describe the emotionality underpinning the process of hacking in two distinct ways. The first involves tedium and frustration. While the initial interest in the project is often present, the endeavour can become tedious: 'Sure, some of it can be automated, some of it can be scripted, but a lot of it is just really tedious and repetitive' (Keith). Frustration also is often evident as Susan illustrates: 'Trying to figure out how something works and not getting the right answer is a little bit like being tortured'.

Tedium is a result of the often mundane parts of overcoming a challenge while frustration often comes from experiencing failure. Willingness to fail, however, is important for development as a craftsperson (Sennett 2008). The frustrations experienced in the process of hacking may encourage advancement and adaptation in the act of craftsmanship, 'Intuition begins with the sense that what isn't yet could be. How do we sense this? In technical craftsmanship, the sense of possibility is grounded in feeling frustrated by a tool's limits or provoked by its untested possibilities' (Sennett 2008: 209–10).

Frustration and boredom, however, are not the only sensations experienced while hacking. If one manages to endure and find a rhythm, the emotional payoff can be profound—resulting in the experience of *flow*, a concept pioneered by positive psychologists (Csikszentmihalyi 1975) and previously used by criminologists (Hayward 2004). Flow:

> involves intense and focused concentration on the activity; action and awareness merge together; the person loses self-consciousness and is no longer aware of self; there is a sense of control over the action; the sense of time is distorted; and the activity is intrinsically rewarding. (Ko and Donaldson 2011: 148)

Flow-inducing activities, in this sense, are said to be 'autotelic' (Csikszentmihalyi 1975) in that they are 'enjoyable but highly intense pastimes' (Hayward 2004: 183). Many

of the hackers in this study describe the process of hacking in a manner consistent with flow—a finding which resonates with Hayward's (2004) connection of flow and late modernity as, arguably, few activities are as characteristic of late modernity as hacking. Both Jensen and Pete even invoke the term flow in their descriptions, as Pete demonstrates:

> In psychology there's a concept called *flow*. And they say that a human being is at his happiest when they are at flow. Like a complete flow state. And when I get into those modes—which I guess would be a hacker mentality mode—my flow is extremely high. It's… you know those moments when you get so focused you lose track of time? You look up and you are like, 'holy crap, look at the time!'

Further, he describes such a state as associated with happiness, even if prolonged exposure to such a state can be exhausting, echoing the work of Csikszentmihalyi. Likewise, KC (2011: 27) describes hacking as a kind of meditation which results in an experience much like flow, 'Every hacker meditates in a similar fashion. Every time you lose yourself in a project for hours on end, you're meditating… the outside world gets shut out, allowing your brain to focus squarely on the task at hand'. Here, and represented in similar descriptions of time loss and drive, the process of flow is tied to hacking.

In addition, flow has ties to skill. To enter a flow state a person has to have their skills challenged (Csikszentmihalyi *et al.* 2005). McGonigal (2011: 40–1) states that, 'Flow was typically the result of years, if not decades, of learning the structure of an activity and strengthening the required skills and abilities'. Sennett (2008) makes similar connections with the experience of craftwork. As one hones their skill and expertise, that person becomes more engrossed in the rhythm of their labour, prolonging one's attention span for the activity (Sennett 2008). The process of flow is tied to the ability to maintain focus for prolonged periods of time—to become engrossed in one's work. As hacking emphasizes skill so heavily, one can see how flow and hacking would occur in tandem.

Sennett (2008) further describes the development of skill in craftwork in a manner similar to flow in the process of glass making: 'she lost awareness of her body making contact *with* the hot glass and became all-absorbed in the physical material as the end in itself'. He continues by stating, 'If I may put this yet another way, we are now absorbed *in* something, no longer self-aware, even of our bodily self. We have become the thing on which we are working' (Sennett 2008: 174). As such, the process of becoming wholly engrossed in an activity—as is necessary to achieve a flow state—is part of craftwork as well. In both cases, happiness is linked to work which is challenging, intrinsically rewarding, and even playful (Sennett 2008; McGonigal 2011).

Completing a hack

Separate from the process of hacking, however, is the emotional experience involved in completing a hack. In particular, the emotions encountered range from a sort of general pleasure to almost a jubilant euphoria. John had difficulty summarizing how it felt to complete a project. He could only summarize the feeling as, 'It feels pretty good… Whenever I accomplish something, it feels pretty good. So… good.' He then goes on to describe it as an 'a-ha!' moment accompanied by a 'sense of accomplishment you get from understanding something'.

Providing a more detailed account, hacker Pete describes hacking in the following manner, focusing primarily on finishing a hack:

[emphatically] Oh, man… It feels good. It's… I used to comment that 'you know what I love about hacking? It's the ability to create. It isn't necessarily just the high of breaking into something. It's the ability to be able to be creative on how you got in in the first place… And I… I posted once on my Facebook that there is no drug on this planet that a teenager can take that replaces the feeling you get from being… Your best moments in creativity. And that's how it feels. It's a rush. It feels good.

Pete describes hacking as containing a 'rush' and that it 'feels good'. He also associates a particular 'high'—equating the process of hacking with taking drugs and associating that with the desire to do more hacking.

Some accounts describe accomplishing a hack as liberating—akin to being released from a prison. Sairys (2004: 46–7) describes the process of breaking through network restrictions in such a manner:

At this point, the network was at our disposal, and even though there was nothing we wanted from all those folders, it was sure nice to know that they were available to us. It was like being released from a prison.

Susan describes completing a hack in a similar manner, 'So, when you finally figure it out… It's like… someone let you out of your cage. And you're like… I'm free.' In both of these cases, the catharsis of accomplishing a task feels like one is being freed—a release. The implication here is that when working towards a goal, the hacker feels beholden to the task and even trapped by it until the job is done.

In the process of hacking, one is confronted with tedium and frustration that, if things align properly, result in a positive flow experience. When one is in a flow state and completes their task, another intense emotional experience may occur resulting in positive feelings, like those previously described. McGonigal (2011) describes this as *fiero*, the Italian term for 'pride':

Fiero is what we feel after we triumph over adversity. You know it when you feel it—*and* when you see it. That's because we almost all express fiero in exactly the same way: we throw our arms over our heads and yell (McGonigal 2011: 33).

Miles describes the achievement of a hacking goal as 'epic win', drawing from the work of McGonigal (2011). He describes the emotional experience of completing a hack as:

It's a success thing.… You know, you've won.…You'll learn something and it becomes… that moment of epiphany which is sort of a… a transient nirvana… When you figured out that, you just get this rush of, you know, kind of endorphins, you know, to varying degrees. *You know, it's a win. You won the big game* [emphasis added].… You know, whatever. It feels good. You gain knowledge from it. You get this happy feeling through acquiring knowledge. You get happy feelings from being able to solve a problem.

Importantly, fiero occurs upon completion of some sort of challenge—a problem was overcome. In many ways then, considering cathartic and euphoric descriptions of hacking provided previously, accomplishing a good/challenging hack provides the sensation of fiero.[6]

Hacking as transgression

The final comparison between hacking and craftwork is their transgressiveness (interviewees = 13; 92.86 per cent; CA items = 86; 44.56 per cent). Transgression is a lived experience laden with emotion, a cultural manifestation, and a political act of subversion

[6] Turkle (1984) has previously commented on the relationship between the sensations of gaming and those of hacking.

and resistance (Ferrell *et al.* 2008). Previous work has discussed craftwork as transgressive by flying in the face of the modern politics of routinization and bureaucratization (Ferrell 2004). While hacking comprises a variety of activities spanning different types of technology and legality, it is always transgressive through its emphasis on resisting and transcending social boundaries. In this vein, Coleman (2012) has noted that the history of hacking is laden with the politics of resistance. Additionally, such subversion is also consistent with Nikitina's (2012) characterization of hackers as a sort of creative trickster.

Though the persistent theme of transgression comprises the focus of this section, the reader may unduly gain the impression that such behaviour is 'negative' in line with the socially constructed perceptions of hacking. Instead, it should be remembered that hacking can consist of activities ranging across the moral spectrum—a tendency which, once again, unites hacking and craftwork. The same cultural process and practice of craftwork yielded penicillin as well as the atomic bomb (Sennett 2008). Likewise, hacking can be applied to something as benign as open-source programming or as harmful as stealing a person's life savings (not all who do either of these activities are hackers, however). In this way, the essence of hacking and craftwork is amoral in that both stand 'in Pandora's shadow and can step out of it' (Sennett 2008: 11). Regardless of morality, however, the transgressive edge persists.

Hacking as subversive

In the public eye, hacking is automatically associated with criminal computer activity. As previously stated, however, many hacking activities exist which are not criminal such as open-source programming (Coleman 2013). Even the activities which are *usually* considered criminal are not always illegal. For example, if a hacker breaks into a network system he/she owns, it is often legal. Even in the case of legal hacking, however, the particular activities still often have a transgressive quality or are embedded with the politics of resistance and subversion. When working with technology and software, as Danny states, 'if you have to break a few things, you know, that's okay…. especially rules'.

Of course, rules are not the only things that hacking can violate. Expectations are also a goal to break in hacking. As Harvey states: 'Hacking has to have that going-outside-what-people-think-you-should-be-doing.' Regarding software and hardware, designers are said to not only create technology, but also create expectations for what can and should be done—expectations hackers delight in violating. Additionally, as previously described, hacking involves breaking and reconfiguring things. Part of this breaking process also involves doing new and creative things: 'hacking is doing stuff you generally are not supposed to be doing or…. You are finding new ways of doing something' (Aidan). In this sense, hacking means moving past designer expectations for systems and reinventing what can be done. Previous research has also found a connection between hacking and using machines unconventionally (Jordan and Taylor 2004).

Open-source software programming comprises a controversial section of the hacking community. Some members (including some who were interviewed in this study) assert that open-source programming is not hacking while others insist otherwise. For those who claim it is not, the reasons given are typically that it does not involve breaking. For

instance, Aidan discussing open-source software programmers, 'Open source projects are inherently open so there's no reason to hack them if they are open'.

But for those who do consider open-source software hacking, the grounds for such are exploration, creation, and defying expectations or even subverting convention. Open-source software hackers are those pushing at the edges of what can be done with programming. This sense also heralds back to the understanding of what it meant to be a hacker in the early days of the MIT Tech Model Railroad Club (Levy 1984). Open-source software programming may also be considered transgression and, thus, hacking because its philosophical logic is out of resistance to proprietary software and, in many instances, the capitalist notion of intellectual property. The very notion of programming in a manner which is (1) not for monetary gain and (2) open and available for others flies in the face of traditional intellectual property arrangements (see also Söderberg 2008).

Hacking and the criminal rush

As stated previously, hacking is not always illegal. When a law violation is committed, the criminal component is sometimes thought of as incidental: 'I mean the crime was always incidental' (Harvey). In this sense, the criminal act is a stepping-stone on the way to solving a problem or completing a project. Sometimes, however, the criminal component of an act can be seductive (Katz 1988). In this way, 'just as skilled craft work produces idiosyncratic designs unimaginable within the repetitions of the assembly line' (Ferrell 2004: 297–8), the thrills sought by hackers break away from otherwise mundane and 'safe' uses for computational technology.

For hackers, this seduction seems to largely concern the notion of trespass. To communicate the rush of breaking in and illicitly trespassing into a computer system, Danny compares hacking to another subcultural practice: Urban Exploration. He states, 'I mean that kind of first got me interested in this sort of thing. Because there's an adrenaline rush to knowing you are somewhere where you shouldn't be.' Previous research similarly describes excitement as a key motivating factor in hacking: 'When hackers are asked what motivates them to write free code or crack computer systems their answers are many and diverse. A recurrent theme, however, is the thrill they get from doing it' (Turgeman-Goldschmidt 2005; Söderberg 2008: 2).

Arriving at a Definition

Similar to previous criminological analyses (Letkemann 1973; Sutherland 1937; King and Chambliss 1984; Fagan and Freeman 1999; Adler 2003), the current analysis examines hacking as *labour* or *work*. Where previous work has attempted to isolate common themes which unify hacking, such as a hacker ethic (Levy 1984; Himanen 2001; Brown 2008), the central argument advanced in this analysis is that hacking comprises a kind of craft. Both hacking and craftwork consist of similarities across mentality, an emphasis on skill, ownership, commitment, similar social-learning structures, an emphasis on process over results, and experiential similarities. Additionally, both hacking and craftwork are stitched together through the politics of resistance and transgression—though hacking may be more flagrant in its transgressive tendencies. In moving towards a conceptual understanding of hacker, then, perhaps a more succinct understanding is that

hacking is a transgressive craft. Craft, however, has two different meanings that are both applicable. On the one hand, craft is a skill-based productive activity. On the other, craft is guileful subversive behaviour and the term can be used to describe a person as 'crafty'. Hacking embodies craft in both respects. In this manner, the eidos of hacking can be distilled into a single term: hacking is *craft(y)*.

Understanding the complexity behind the concept of hacker indicates that simplistic definitions which identify hacking as any illegal computer intrusion are lacking. In addition, because hacking can encompass so many activities beyond computer network intrusions, website defacements, or other forms of computer-mediated criminal activity, the use of the term 'hacking' as short-hand for these crimes is inappropriate. The suggestion made here is that it would be more practically and academically suitable to describe these acts by more specific labels such as *intrusion*, *illicit access*, *exfiltration*, *cracking*, *network obstruction*, *website defacement*, *carding*, *phishing*, etc. Any of these activities can be performed by people who are not hackers as described in this study. Describing any of these activities as hacking only confounds the issue as there often exists the possibility that the act is committed by a deviant/criminal who is not a part of hacking culture. For instance, relatively anyone can pick up a computer security/intrusion tool and attempt to break into a computer network. An entire industry of penetration testing has risen up to try to secure networks—not all of those who participate in this industry are hackers. In the literature, some consider activities as mundane as accessing a person's Facebook account without permission to be hacking (e.g. Marcum et al. 2014).[7] Considering the array of possibilities to acquire access—pre-made scripts, for example—this view of hacking is rendered questionable based on the results from the current study. The terms *intrusion* or *illicit access* may be more appropriate as it may not take a hacker in the sense described here to perform such an act. Such terminology is also preferable because these terms may "not come with the emotional and ideological baggage that comes with the term 'hacking"' (Wall 2007: 53). Continual use of the term divorced from its subcultural roots may in fact *contribute* to this 'emotional and ideological baggage' as well as act as a kind of conceptual colonization of the term from the subculture in which it originates.

Viewing hacking as craft is useful because hacking is more than an act or behaviour—it's a cultural practice tied to work. The very notion of hacker is intimately linked to the material relationship between labour and the mind (or the development of cultural identity). Additionally, because of the transgressive edge present, hacking presents a kind of craft with the politics of resistance running through to the core—resistance against convention, norms, expectations, and even law. Just as Sennett (2008) declares the spectre of harm looms over craftwork, the spirit of transgression flows through hacking. In this way, both hacking and craft 'are never innocent' (Sennett 2008: 294).

Similar to many other ethnographic studies, limitations confront the findings explicated here. Of particular note, this study sacrifices breadth for depth and, despite the cohesiveness found in data, the results may not be generalizable. With this point acknowledged, this study attempted to connect the results to outside literature and observations to validate the findings beyond the scope of this study. In addition, the ethnographic content analysis data used also add additional heft to the results, though generalizability is still left wanting. Regardless, future studies should further probe and refine the results presented here.

[7] I would like to thank an anonymous reviewer for helping identify this vital point of clarity.

Future research should also continue to investigate hacking and other areas of deviance in their relationships to work and labour. Many of these activities involve the development of various skills and bodies of knowledge. They are not mere acts or behaviours—they are connected to greater constellations of social and personal developments. Understanding how the 'hands-on' components of technological deviance interconnect with the developmental and social dynamics involved is a necessary venture. For instance, the features described here could be useful in understanding other deviant/illicit forms of work such as marijuana growth (Boylstein and Maggard 2013), methamphetamine production (Weisheit 2008), robbery and other forms of thieving (Sutherland 1937; Letkemann 1973; Tunnell 2006). Such a perspective may be invaluable for understanding the relationship between these activities as forms of work and their associated subcultures—building from Sennett's (2008) descriptions of the relationship between the head and the hand. Through understanding labour and craft as transgressive, such a perspective also allows connections to be made to broader social structures and processes.

Additionally, the results from this study can provide a foundation for future research in other contemporary debates in criminology and technocrime. Future research should consider the construction of the hacker as a deviant or criminal *other* and how society arranges its response accordingly—perhaps examining how public notions of the hacker detach themselves from subcultural understandings to create various tensions between hackers and social response agencies perhaps in a fashion similar to Becker's (1963) discussion of marijuana users and moral entrepreneurs. The understanding of hacking advanced here may also serve as a springboard to advance the debate on incorporating security hackers into various institutions (like law enforcement) and industries (such as banks). Understanding hacking from this perspective and, more importantly, that there are qualitative differences between hackers who engage in malfeasant behaviours and other technocriminals may be useful for consideration in future research and debates in technocrime and deviance studies.

Acknowledgement

The author would like to thank Jurg Gerber, Dennis Longmire and Howard Henderson for their support and insights throughout the research process. Kenneth Tunnell and Maria Koeppel must also be thanked for reviewing a previous draft of this manuscript. Thanks also go to the reviewers who provided constructive comments and criticisms. Finally, a tremendous debt of gratitude is also owed to the members of Union Hack who made this research possible.

References

Adler, P. A. (2003), 'Wheeling and Dealing: An Ethnography of an Upper-Level Drug Dealing and Smuggling Community', in D. Harper and H. M. Lawson, eds, *The Cultural Study of Work*, 452–62. Rowman & Littlefield Publishers, Inc.

Altheide, D. L. (1987), 'Ethnographic Content Analysis', *Qualitative Sociology*, 10: 65–77.

Bachmann, M. (2010), 'Deciphering the Hacker Underground: First Quantitative Insights', in T. J. Holt and B. H. Schell, eds, *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, 105–26. IGI Global.

Barbrook, R. and Cameron, A. (2001), 'California Ideology', in P. Ludlow, ed., *Crypto Anarchy, Cyberstates, and Pirate Utopias*, 363–88. MIT Press.
Becker, H. S. (1963), *Outsiders: Studies in the Sociology of Deviance*. The Free Press.
Blumstein, A., Cohen, J., Roth, J. A. and Visher, C. A. (1986), *Criminal Careers and 'Career Criminals'*. National Academy Press.
Boylstein, C. and Maggard, S. R. (2013), 'Small-Scale Marijuana Growing: Deviant Careers as Serious Leisure', *Humbolt Journal of Social Relations*, 35: 52–70.
Brown, J. (2008), 'From Friday to Sunday: The Hacker Ethic and Shifting Notions of Labour, Leisure, and Intellectual Property', *Leisure Studies*, 27: 395–409.
Bulmer, M. (1982), 'When is Disguise Justified? Alternatives to Covert Participant Observation', *Qualitative Sociology*, 5: 251–64.
Charmaz, K. (2002), Qualitative Interviewing and Grounded Theory Analysis', in J. F. Gubrium and J. A. Holstein, eds, *Handbook of Interview Research: Context and Method*, 675–94. Sage.
Coleman, G. (2012), 'Phreakers, Hackers, and Trolls and the Politics of Transgression and Spectacle', in M. Mandiberg, ed., *The Social Media Reader*, 99–119. NYU Press.
Coleman, G. E. (2013), *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press.
Coleman, G. E. and Golub, A. (2008), 'Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism', *Anthropological Theory*, 8: 255–77.
Csikszentmihalyi, M. (1975), *Beyond Boredom and Anxiety*. Jossey-Bass Publishers.
Csikszentmihalyi, M., Abuhamdeh, S. and Nakamura, J. (2005), 'Flow', in A. Elliot and C. S. Dweek, eds, *Handbook of Competence and Motivation*, 598–608. Guilford Press.
Epstein, S. R. (1998), 'Craft Guilds, Apprenticeship, and Technological Change in Preindustrial Europe', *The Journal of Economic History*, 58: 684–713.
Fagan, J. and Freeman, R. B. (1999), 'Crime and Work', *Crime and Justice*, 25: 225–90.
Farr, N. (2008), 'The Hacker Perspective', *2600: The Hacker Quarterly*, 25: 26–8.
Ferrell, J. (2004), 'Boredom, Crime and Criminology', *Theoretical Criminology*, 8: 287–302.
—— (2013), 'Cultural Criminology and the Politics of Meaning', *Critical Criminology*, 21: 257–71.
Ferrell, J., Hayward, K. and Young, J. (2008), *Cultural Criminology: An Invitation*. Sage.
Glaser, B. G. and Strauss, A. L. (1967), *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Publishing Company.
Halbert, D. (1997), 'Discourses of Danger and the Computer Hacker', *The Information Society*, 13: 361–74.
Hayward, K. (2004), *City Limits: Crime, Consumer Culture and the Urban Experience*. Taylor & Francis.
Himanen, P. (2001), *The Hacker Ethic: A Radical Approach to the Philosophy of Business*. Random House, Inc.
Hollinger, R. (1991), 'Hackers: Computer Heroes or Electronic Highwaymen?', *Computers & Society*, 21: 6–17.
Holt, T. J. (2009), 'Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers', in F. Schmalleger and Michael Pittaro, eds, *Crimes of the Internet*, 336–55. Pearson Education, Inc.
—— (2010), 'Becoming a Computer Hacker: Examining the Enculturation and Development of Computer Deviants,' in P. Cromwell, ed., *In Their Own Words: Criminals on Crime: An Anthology*, 5th edn, 109–23. Oxford University Press.

Jordan, T. and Taylor, P. (1998), 'A Sociology of Hackers', *The Sociological Review*, 46: 757–80.
—— (2004), *Hacktivism and Cyberwars: Rebels with a Cause*. Routledge.
Katz, J. (1988), *Seductions of Crime: Moral and Sensual Attractions in Doing Evil*. Basic Books.
KC. (2011), 'The Hacker Perspective', *2600: The Hacker Quarterly*, 28: 26–7.
King, H. and Chambliss, W. J. (1984). *The Box-Man: A Professional Thief's Journey*. John Wiley & Sons.
Ko, I., and Donaldson, S. I. (2011), 'Applied Positive Organizational Psychology: The State of the Science and Practice', in S. I. Donaldson, M. Csikszentmihalyi and J. Nakamura, eds, *Applied Positive Psychology: Improving Everyday Life, Health, Schools, Work, and Society*, 137–54. Routledge.
Leman-Langlois, S. (2013), *Technocrime, Policing, and Surveillance*. Routledge.
Letkemann, P. (1973), *Crime as Work*. Prentice-Hall, Inc.
Levy, S. (1984), *Hackers: Heroes of the Computer Revolution*. Penguin Group Inc.
Marcum, C. D., Higgins, G. E., Ricketts, M. L. and Wolfe, S. E. (2014). 'Hacking in High School: Cybercrime Perpetration by Juveniles', *Deviant Behavior*, 35, 581–91.
McGonigal, J. (2011), *Reality is Broken: Why Games make us Better and How They Can Change the World*. Penguin.
McKenzie, J. (1999), '!nt3rh4ckt!v!ty', *Style*, 33: 283–99.
Meikle, G. (2002), *Future Active: Media Activism and the Internet*. Routledge.
Mirrorshades. (2005), 'I Am Not a Hacker', *2600: The Hacker Quarterly*, 22: 50.
Ninja_of_Comp. (2011), 'Hacking is in the Blood', *2600: The Hacker Quarterly*, 28: 31.
Nikitina, S. (2012), 'Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture', *The Journal of Popular Culture*, 45: 133–52.
Palermo, J. (1978), 'Apodictic Truth: Husserl's Eidetic Reduction Versus Induction', *Notre Dame Journal of Formal Logic*, 19: 69–80.
Rantala, R. R. (2008), *'Cybercrime Against Businesses, 2005'*. Bureau of Justice Statistics.
Sairys. (2004), 'A Lesson on Trust', *2600: The Hacker Quarterly*, 21: 45–7.
Sennett, R. (2008), *The Craftsman*. Yale University Press.
Skibell, R. (2002), 'The Myth of the Computer Hacker', *Information, Communication & Society*, 5: 336–56.
Söderberg, J. (2008), *Hacking Capitalism: The Free and Open Source Software Movement*. Routledge.
Steinmetz, K. F. and Gerber, J. (2014), 'The Greatest Crime Syndicate Since the Gambinos': A Hacker Critique of Government, Law, and Law Enforcement', *Deviant Behavior*, 35: 243–61.
Sutherland, E. H. (1937), *The Professional Thief*. University of Chicago Press.
Taylor, P. A. (1999), *Hackers: Crime in the Digital Sublime*. Routledge.
—— (2005), 'From Hackers to Hacktivists: Speed Bumps on the Global Superhighway?', *New Media & Society*, 7: 625–46.
'The Cost of Cyber Crime: A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office'. (2011). Detica.
The Economic Impact of Cybercrime and Cyber Espionage (2013). Center for Strategic and International Studies.
Thomas, D. (2002), *Hacker Culture*. University of Minnesota Press.
Thomas, J. (2005), 'The Moral Ambiguity of Social Control in Cyberspace: A Retro-Assessment of the 'Golden Age' of Hacking', *New Media & Society*, 7: 599–624.

Tunnell, K. D. (2006), *Living off Crime*, 2nd edn. Rowman & Littlefield.
Turgeman-Goldschmidt, O. (2005), 'Hackers' Accounts: Hacking as a Social Entertainment', *Social Science Computer Review*, 23: 8–23.
—— (2011), 'Identity Construction Among Hackers', in K. Jaishankar, ed., *CyberCriminology: Exploring Internet Crimes and Criminal Behavior*, 31–51. CRC Press.
Turkle, S. (1984), *The Second Self: Computers and the Human Spirit*. Simon & Schuster.
Valnour. (2009), 'Revenge is a Dish Best Served Cold', *2600: The Hacker Quarterly*, 26: 32.
Van Maanen, J. (1988/2011), *Tales of the Field: On Writing Ethnography*, 2nd edn. University of Chicago Press.
Wall, D. S. (2007), *Cybercrime: The Transformation of Crime in the Information Age*. Polity.
Warnick, B. (2004), 'Technological Metaphors and Moral Education: The Hacker Ethic and the Computational Experience', *Studies in Philosophy and Education*, 23: 265–81.
Weisheit, R. (2008), 'Making Methamphetamine', *Southern Rural Sociology*, 23: 78–107.
Yar, M. (2013), *Cybercrime and Society*, 2nd edn. Sage.
Zoltan. (2008), 'Hacking Music', *2600: The Hacker Quarterly*, 25: 57.