A sociology of hackers

Tim Jordan and Paul Taylor

Abstract

Illicit computer intruders, or hackers, are often thought of as pathological individuals rather than as members of a community. However, hackers exist within social groups that provide expertise, support, training, journals and conferences. This article outlines this community to establish the nature of hacking within 'information societies'. To delineate a 'sociology of hackers', an introduction is provided to the nature of computer-mediated communication and the act of computer intrusion, the hack. Following this the hacking community is explored in three sections. First, a profile of the number of hackers and hacks is provided by exploring available demographics. Second, an outline of its culture is provided through a discussion of six different aspects of the hacking community. The six aspects are technology, secrecy, anonymity, membership fluidity, male dominance and motivations. Third, an exploration of the community's construction of a boundary, albeit fluid, between itself and its other, the computer security industry, is provided. This boundary is constructed through metaphors whose central role is to establish the ethical nature of hacking. Finally, a conclusion that rejects any pathologisation of hackers is offered.

Introduction[1]

The growth of a world-wide computer network and its increasing use both for the construction of online communities and for the reconstruction of existing societies means that unauthorised computer intrusion, or hacking, has wide significance. The 1996 report of a computer raid on Citibank that netted around $10 million indicates the potential seriousness of computer intrusion. Other, perhaps more whimsical, examples are the attacks on the CIA

world-wide web site, in which its title was changed from Central Intelligence Agency to Central Stupidity Agency, or the attack on the British Labour Party's web-site, in which titles like 'Road to the Manifesto' were changed to 'Road to Nowhere'. These hacks indicate the vulnerability of increasingly important computer networks and the anarchistic, or perhaps destructive, world-view of computer intruders (Miller, 1996; Gow and Norton-Taylor, 1996). It is correct to talk of a world-view because computer intrusions come not from random, obsessed individuals but from a community that offers networks and support, such as the long running magazines *Phrack* and *2600*. A present there is no detailed sociological investigation of this community, despite a growing number of racy accounts of hacker adventures.[2] To delineate a sociology of hackers, an introduction is needed to the nature of computer-mediated communication and of the act of computer intrusion, the hack. Following this the hacking community will be explored in three sections: first, a profile of the number of hackers and hacks; second, an outline of its culture through the discussion of six different aspects of the hacking community; and third, an exploration of the community's construction of a boundary, albeit fluid, between itself and its other, the computer security industry.[3] Finally, a conclusion that briefly considers the significance of our analysis will be offered.

In the early 1970s, technologies that allowed people to use decentred, distributed networks of computers to communicate with each other globally were developed.[4] By the early 1990s a new means of organising and accessing information contained on computer networks was developed that utilised multi-media 'point and click' methods, the World-Wide Web. The Web made using computer networks intuitive and underpinned their entry into mass use. The size of this global community of computer communicators is difficult to measure[5] but in January 1998 there were at least 40 million (Hafner and Lyons, 1996; Quarterman, 1990; Jordan, 1998a; Rickard, 1995; Quarterman, 1993). Computer communication has also become key to many industries, not just through the Internet but also through private networks, such as those that underpin automated teller services. The financial industry is the clearest example of this, as John Perry Barlow says 'cyberspace is where your money is'. Taken together, all the different computer networks that currently exist control and tie together vital institutions of modern societies; including telecommunications, finance, globally distributed production and the media (Castells, 1996; Jordan, 1998a). Analysis of the community which attempts to illicitly use these networks can begin with a definition of the 'hack'.

Means of gaining unauthorised access to computer networks include guessing, randomly generating or stealing a password. For example, in the Prestel hack, which resulted in the Duke of Edinburgh's mail-box becoming vulnerable, the hacker simply guessed an all too obvious password (222222 1234) (Schifreen, hacker, interview). Alternatively, some computers and software programmes have known flaws that can be exploited. One of the most complex of these is 'IP spoofing' in which a computer connected to the Internet can be tricked about the identity of another computer during the process of receiving data from that computer (Felten *et al.*, 1996; Shimomura, 1996; Littman, 1996). Perhaps most important of all is the ability to 'social engineer'. This can be as simple as talking people into giving out their passwords by impersonating someone, stealing garbage in the hope of gaining illicit information (trashing) or looking over someone's shoulder as they use their password (shoulder surfing). However, what makes an intrusion a hack or an intruder a hacker is not the fact of gaining illegitimate access to computers by any of these means but a set of principles about the nature of such intrusions. Turkle identifies three tenets that define a good hack: simplicity, the act has to be simple but impressive; mastery, however simple it is the act must derive from a sophisticated technical expertise; and, illicit, the act must be against some legal, institutional or even just perceived rules (Turkle, 1984: 232).[6] Dutch hacker Ralph used the example of stealing free telephone time to explain the hack:

> It depends on how you do it, the thing is that you've got your guys that think up these things, they consider the technological elements of a phone-booth, and they think, 'hey wait a minute, if I do this, this could work', so as an experiment, they cut the wire and it works, now *they're hackers*. Okay, so it's been published, so Joe Bloggs reads this and says, 'hey, great, I have to phone my folks up in Australia', so he goes out, cuts the wire, makes phone calls. He's a stupid ignoramus, yeah? (Ralph, hacker, interview)

A second example would be the Citibank hack. In this hack, the expertise to gain unauthorised control of a bank was developed by a group of Russian hackers who were uninterested in taking financial advantage. The hacker ethic to these intruders was one of exploration and not robbery. But, drunk and depressed, one of the hackers sold the secret for $100 and two bottles of vodka, allowing organised criminals to gain the expertise to steal $10 million (Gow and

Norton-Taylor, 1996). Here the difference between hacking and criminality lay in the communally held ethic that glorified being able to hack Citibank but stigmatised using that knowledge to steal. A hack is an event that has an original moment and, though it can be copied, it loses its status as a hack the more it is copied. Further, the good hack is the object in-itself that hackers desire, not the result of the hack (Cornwall, 1985: vii).

The key to understanding computer intrusion in a world increasingly reliant on computer-mediated communication lies in understanding a community whose aim is the hack. It is this community that makes complex computer intrusion possible and a never ending threat, through the limitless search for a good hack. It is this community that stands forever intentionally poised both at the forefront of computer communications and on the wrong side of what hackers see as dominant social and cultural norms.

Computer underground: demographics

Analysing any intentionally illicit community poses difficulties for the researcher. The global and anonymous nature of computer-mediated communication exacerbates such problems because generating a research population from the computer underground necessitates self-selection by subjects and it will be difficult to check the credentials of each subject. Further methodological difficulties involved in examining a self-styled 'outlaw' community that exists in cyberspace are indicated by the Prestel hacker.

> There used to be a hacking community in the UK, the hackers I used to deal with 8 or 9 years ago were all based in North London where I used to live and there were 12 of us around the table at the local Chinese restaurant of a Friday night . . . within about 20 minutes of me and my colleague Steve Gold being arrested: end of hacking community. An awful lot of phone calls went around, a lot of discs got buried in the garden, and a lot of people became ex-hackers and there's really no-one who'll talk now (Schifreen, hacker, interview).

Demographic data is particularly difficult to collect from an underground community.[7] However, some statistics are available. Following presentation of these, an in-depth exploration of the hacking community on the basis of qualitative research will be pre-

sented. After investigating the US police force's crackdown on the computer underground in the early 1990s, Sterling estimated there were 5,000 active hackers with only around 100 in the elite who would be 'skilled enough to penetrate sophisticated systems' (Sterling, 1992: 76–77). For the same period, Clough and Mungo estimated there were 2,000 of 'the really dedicated, experienced, probably obsessed computer freaks' and possibly 10,000 others aspiring to this status (Clough and Mungo, 1992: 218).[8] Though no more than an indication, the best, indeed only, estimates for the size of the hacking community or computer underground are given by these figures.

Another means of measuring the size of the computer underground is by its effects. Though this cannot hope to indicate the actual number of hackers, as one hacker can be responsible for extensive illicit adventures, measuring the extent of hacking allows one indication of the underground's level of activity. Three surveys are available that generate evidence from the 'hacked' rather than hackers: the 1990 UK Audit Commission's survey, the 1993 survey conducted as part of this research project, and the 1996 War Room Research, information systems security survey.[9] Results from all three sources will be presented, focusing on the amount of hacking.

The 1990 UK Audit Commission surveyed 1,500 academic, commercial and public service organisations in the United Kingdom. This survey found 5% of academic, 14% of commercial and 11.5% of public service organisations had suffered computer intrusion (Audit Commission, 1990). A survey was conducted as part of this research project (hereafter referred to as the Taylor survey) and received 200[10] responses, of which 64.5% had experienced a hack, 18.5% a virus only and 17% no detected illicit activity (Taylor, 1993). The 1996 WarRoom survey received 236 responses from commercial USA firms (Fortune 1,000 companies) of which 58% reported attempts by outsiders to gain computer access in the 12 months prior to July 1996, 29.8% did not know and 12.2% reported no such attempts. The types of intrusions can be categorised as 38.3% malicious, 46.5% unidentifiable as malicious or benign and 15.1% benign[11] (WarRoom, 1996).

The level of hacking activity reported in these surveys varies greatly between the Audit Commission on the one hand and the Taylor and WarRoom surveys on the other. A number of possibilities explain this. The lower level of hacking comes from a survey of UK organisations, while Taylor was over half from the USA and a

third UK and WarRoom was solely USA. This might suggest a higher level of hacking into USA organisations, though this says nothing about the national source of a hack. Second, the Audit Commission survey has a much larger sample population and consequently should be more reliable. However, third, the WarRoom and Taylor surveys stressed the confidentiality of respondents. This is a key issue as organisations show a consistently high level of caution in reporting hacks. The WarRoom survey found that 37% of organisations would only report computer intrusion if required by law, that 22% would report only if 'everybody else did', that 30% would only report if they could do so anonymously and only 7% would report anytime intrusion was detected (WarRoom, 1996). From this perspective the Audit Commission survey may have under-reported hacking because it did not place sufficient emphasis on the confidentiality of responses. Fourth, the Taylor and WarRoom surveys were conducted later than the Audit Commission survey and may reflect rising levels of or rising awareness of hacking. Unfortunately, there is no way of deciding which of these factors explain the differences in reported levels of hacking.

The available statistics suggest the computer underground may not be very large, particularly in the number of elite hackers, but may be having a significant effect on a range of organisations. If the Taylor and WarRoom surveys are accurate nearly two-thirds of organisations are suffering hacks. To grasp the nature of hackers requires turning to the qualitative fieldwork conducted in this project.

Internal factors: technology, secrecy, and anonymity, membership fluidity, male dominance and motivations

> To find 'hacker culture' you have to take a very wide view of the cyberspace terrain and watch the interactions among physically diversified people who have in common a mania for machines and software. What you will find will be a gossamer framework of culture. (Marotta, hacker, interview)

The 'imagined community' that hackers create and maintain can be outlined through the following elements: technology, secrecy, anonymity, boundary fluidity, male dominance and motivations. Community is here understood as the collective identity that mem-

bers of a social group construct or, in a related way, as the 'collective imagination' of a social group. Both a collective identity and imagination allow individuals to recognise in each other membership of the same community. The computer underground, or at least the hacking part of it, can be in this way understood as a community that offers certain forms of identity through which membership and social norms are negotiated. Even though some of these forms are externally imposed, the nature of Internet technology for example, the way these forms are understood allows individuals to recognise in each other a common commitment to an ethic, community or way of life. This theorisation draws on Anderson's concept of the imagined community and on social movement theories that see movements as dispersed networks of individuals, groups and organisations that combine through a collectively articulated identity. Anderson names the power of an imagined identity to bind people, who may never meet each other, together in allegiance to a common cause. Social movement theories grasp the way movements rely on divergent networks that are not hierarchically or bureaucratically unified but are negotiated between actors through an identity that is itself the subject of much of the negotiation (Jordan, 1995; Diani, 1992; Anderson, 1991). These perspectives allow us to grasp a hacking community that can use computer mediated communication to exist world-wide and in which individuals often never physically meet.[12]

Technology

The hacking community is characterised by an easy, if not all-consuming, relationship with technology, in particular with computer and communications technology.

> We are confronted with . . . a generation that has lived with computers virtually from the cradle, and therefore have no trace of fear, not even a trace of reverence. (Professor Herschberg, academic, interview)

Hackers share a certain appreciation of or attitude to technology in the assumption that technology can be turned to new and unexpected uses. This attitude need not be confined to computer mediated communication. Dutch hacker Dell claimed to have explored the subterranean tunnels and elevator shafts of Amsterdam, including government fall-out shelters (Dell, hacker, interview), while

Utrecht hacker Ralph argued hacking 'pertains to any field of technology. Like, if you haven't got a kettle to boil water with and you use your coffee machine to boil water with, then that in my mind is a hack, because you are using technology in a way that it's not supposed to be used' (Ralph, hacker, interview). It is the belief that technology can be bent to new, unanticipated purposes that underpins hackers' collective imagination.

Secrecy

Hackers demonstrate an ambivalent relationship to secrecy. A hack demands secrecy, because it is illicit, but the need to share information and gain recognition demands publicity. Sharing information is key in the development of hackers, though it makes keeping illicit acts hidden from law enforcement difficult. Hackers often hack in groups, both in the sense of physically being in the same room while hacking and of hacking separately but being in a group that physically meets, that frequents bulletin boards, on-line places to talk and exchanges information. It is a rare story of a hacker's education that does not include being trained by more experienced hackers or drawing on the collective wisdom of the hacking community through on-line information. Gaining recognition is also important to hackers. A member of the Zoetermeer hacking group noted 'Hacking can be rewarding in itself, because it can give you a real kick sometimes. But it can give you a lot more satisfaction and recognition if you share your experiences with others. . . . Without this group I would never have spent so much time behind the terminals digging into the operating system' (Zoetermeer, hackers, interview). A good hack is a bigger thrill when shared and can contribute to a hacker gaining status and access to more communal expertise. For example, access to certain bulletin boards is only given to those proven worthy.

A tension between the need to keep illicit acts away from the eyes of police and other authority figures but in front of the eyes of peers or even the general public defines hackers' relationship to secrecy. No hack exemplifies this more than a World-Wide Web hack where the object is to alter an internationally accessible form of public communication but at the same time not be caught. In the case of the Labour Party hack, the hacker managed to be quoted on the front page of UK national newspapers, by ringing up the newspapers to tell them to look at the hack before it was removed, but also kept his/her identity secret. A further example is that many hackers take trophies in the

form of copied documents or pieces of software because a trophy proves to the hacking community that the hacker 'was there'. The problem is that a trophy is one of the few solid bases for prosecuting hackers. Ambivalence toward secrecy is also the source of the often-noted fact that hackers are odd criminals, seeking publicity. As Gail Thackeray, one-time police nemesis of hackers, noted 'What other group of criminals . . . publishes newsletters and hold conventions?' (Thackeray, cited in Sterling, 1992: 181).[13]

Anonymity

The third component of the hacking community is anonymity. As with technology what is distinctive is not so much the fact of online anonymity, as this is a widely remarked aspect of computer-mediated communication (Dery, 1993: 561), but the particular understanding of anonymity that hackers take up. Anonymity is closely related to secrecy but is also distinct. Secrecy relates to the secrecy of the hack, whereas anonymity relates to the secrecy of a hacker's offline identity. Netta Gilboa notes one complex version of this interplay of named and hidden identity on an on-line chat channel for hackers.

> Hackers can log into the #hack channel using software . . . that allows them to come in from several sites and be on as many separate connections, appearing to be different people. One of these identities might then message you privately as a friend while another is being cruel to you in public. (Gilboa, 1996: 102–103)

Gilboa experienced the construction of a number of public identities all intended to mask the 'real' identity of a hacker. A second example of this interplay of anonymity and publicity is the names or 'handles' hackers give themselves and their groups. These are some of the handles encountered in this research: Hack-Tic (group), Zoetermeer (group), Altenkirch (German), Eric Bloodaxe, Faustus, Maelstrom, Mercury, Mofo. Sterling notes a long list of group names – such as Kaos Inc., Knights of Shadow, Master Hackers, MAD!, Legion of Doom, Farmers of Doom, the Phirm, Inner Circle I and Inner Circle II. Hackers use names to sign their hacks (sometimes even leaving messages for the hacked computer's usual users), to meet on-line and to bolster their self-image as masters of the hack, all the while keeping their offline identity secret.[14]

Membership fluidity

The fourth quality of the hacking community is the speed at which membership changes. Hacking shares the characteristics ascribed to many social movements of being an informal network rather than a formally constituted organisation and, as such, its boundaries are highly permeable (Jordan, 1995; Diani, 1992). There are no formal ceremonies to pass or ruling bodies to satisfy to become a hacker. The informal and networked nature of the hacking community, combined with its illicit and sometimes obsessional nature means that a high turnover of hackers occurs (Clough and Mungo, 1992: 18). Hackers form groups within the loose overall structure of the hacking community and these may aspire to be formally organised, however the pressures of law enforcement means that any successful hacking group is likely to attract sustained attention at some point (Quittner and Slatalla, 1995).

> People come and go pretty often and if you lay off for a few months and then come back, almost everyone is new. There are always those who have been around for years . . . I would consider the hacking community a very informal one. It is pretty much anarchy as far as rule-making goes. . . . The community was structured only within the framework of different hacking 'groups'. Legion of Doom would be one example of this. A group creates its own rules and usually doesn't have a leader . . . The groups I've been in have voted on accepting new members, kicking people out, etc. (Eric Bloodaxe, hacker, member of Legion of Doom, interview)

Gilboa claims that the future of hacking will be a split between life-long hackers, often unable to quit because of police records and suspicion, and 90% of hackers who will move on 'when they get a job they care about or a girlfriend who sucks up their time' (Gilboa, 1996: 111). A more prosaic, but equally potent, reason why the hacking community's membership is fluid is given by hacker Mike 'if you stop, if you don't do it for one week then things change, the network always changes. It changes very quickly and you have to keep up and you have to learn all the tricks by heart, the default passwords, the bugs you need' (Mike, hacker, interview). The sheer speed at which computer communications technology changes requires a powerful commitment from hackers.

Male dominance

The fifth component of hacking culture is male dominance and an associated misogyny. Research for this project and literature on hackers fails to uncover any significant evidence of female hackers (Taylor, 1993: 92). Gilboa states 'I have met more than a thousand male hackers in person but less than a dozen of them women' (Gilboa, 1996: 106). This imbalance is disproportionate even in the field of computer mediated communication (Spertus, 1991: i). A number of factors explain the paucity of women generally in the computer sciences: childhood socialisation, where boys are taught to relate to technology more easily than girls; education in computers occurs in a masculine environment; and, a gender bias towards men in the language used in computer science (Spertus, 1991; Turkle, 1984; Taylor, 1993: 91–103). With these factors producing a general bias towards males in relation to computers, the drive towards the good hack exacerbates this as it involves a macho, competitive attitude (Keller, 1988: 58). Hackers construct a more intensely masculine version of the already existing male bias in the computer sciences.

> When Adam delved and Eve span . . . who was then the gentleman? Well, we see that Adam delves into the workings of computers and networks and meanwhile Eve spins, what? Programmes? Again, my wife programmes and she has the skills of a hacker. She has had to crack security in order to do her job. But she does it as her job, not for the abstract thrill of discovering the unknown. Even spins. Females who compute would rather spend their time building a good system, than breaking into someone else's system. (Mercury, hacker, interview)

Whether Mercury's understanding of differences between men and women is accurate or not, the fact that he, and many other hackers, have such attitudes means the hacking community will almost certainly feel hostile to women. Added to these assumptions of, at best, separate spheres of male and female expertise in computing is the problem that anonymity often fuels sexual harassment. 'The fact that many networks allow a user to hide his real name . . . seems to cause many males to drop all semblance of civilisation. Sexual harassment by email is not uncommon' (Freiss, hacker, interview). Gilboa, a woman, recounts an epic tale of harassment that included hackers using her on-line magazine as a 'tutorial' example of how to

charge phone calls to someone else, taking over her magazine entirely and launching a fake version, being called a prostitute, child molester and drug dealer, having her phone calls listened to, her phone re-routed or made to sound constantly engaged and having her email read. One answer to Gilboa's puzzlement at her treatment lies in the collective identity hackers share and construct that is in part misogynist.

Motivations

Finally, hackers often discuss their motivations for hacking. They are aware of, and often glory in, the fact that the life of a dedicated hacker seems alien to those outside the hacking community. One result of this is that hackers discuss their motivations. These are sometimes couched as self-justifications, sometimes as explanations and sometimes as agonised struggles with personal obsessions and failures. However, whatever the content of such discussions, it is the fact of an ongoing discourse around the motivation to hack that builds the hacking community. These discussions are one more way that hackers can recognise in each other a common identity that provides a collective basis for their community. A number of recurring elements to these discussions can be identified.

First, hackers often confess to an addiction to computers and/or to computer networks, a feeling that they are compelled to hack. Second, curiosity as to what can be found on the world-wide network is also a frequent topic of discussion. Third, hackers often claim their offline life is boring compared to the thrill of illicit searches in online life. Fourth, the ability to gain power over computer systems, such as NASA, Citibank or the CIA web site, is an attraction. Fifth, peer recognition from other hackers or friends is a reward and goal for many hackers, signifying acceptance into the community and offering places in a hierarchy of more advanced hackers. Finally, hackers often discuss the service to future computer users or to society they are offering because they identify security loopholes in computer networks. Hackers articulate their collective identity, and construct a sense of community, by discussing this array of different motivations.

> I just do it because it makes me feel good, as in better than anything else that I've ever experienced . . . the adrenaline rush I get when I'm trying to evade authority, the thrill I get from having written a program that does something that was supposed

> to be impossible to do, and the ability to have social relations with other hackers are all very addictive . . . For a long time, I was extremely shy around others, and I am able to let my thoughts run free when I am alone with my computer and a modem hooked up to it. I consider myself addicted to hacking . . . I will have no moral or ethical qualms about system hacking until accounts are available to the general public for free . . . Peer recognition was very important, when you were recognised you had access to more. (Maelstrom, hacker, interview)

Maelstrom explores almost the whole range of motivations including curiosity, the thrill of the illicit, boredom, peer recognition and the social need for free or cheap access. By developing his own interpretation out of the themes of motivation, he can simultaneously define his own drives and develop a sense of community. It is this double movement in which individual motivations express the nature of a community, that makes the discussions of motivations important for hackers. Finally, the motivations offered by perhaps the most famous of all hackers, Kevin Mitnick, provides another common articulation of reasons for hacking.

> You get a better understanding of cyberspace, the computer systems, the operating systems, how the computer systems interact with one another, that basically was my motivation behind my hacking activity in the past. It was just from the gain of knowledge and the thrill of adventure, nothing that was well and truly sinister as trying to get any type of monetary gain or anything. (Mitnick, hacker, interviewer)

Internal factors: conclusion

These six factors all function largely between hackers, allowing them a common language and a number of resources through which they can recognise each other as hackers and through which newcomers can become hackers. These are resources internal to the hacking community, not because they do not affect or include non-hackers but because their significance is largely for other hackers. Put another way, these are the resources hackers use to discuss their status as hackers with other hackers, they are collectively negotiated within the boundaries of the hacker community. This raises the issue of how an external boundary is constructed and maintained. How do hackers recognise a distinction between inside and outside?

How do hackers adjust, reinvent and maintain such a distinction? This is the subject of the third and final section of this definition of the hacker community.

External factors: the boundary between computer underground and the computer security industry

Hackers negotiate a boundary around their community by relating to other social groups. For example, hackers have an often spectacular relationship to the media. Undoubtedly the most important relationship to another community or group is their intimate and antagonistic bond to the computer security industry (CSI). This relationship is constitutive of the hacking community in a way that no other is. Put another way, there is no other social group whose existence is necessary to the existence of the hacking community. Here is a sample of views of hackers from members of CSI.

> Hackers are like kids putting a 10 pence piece on a railway line to see if the train can bend it, not realising that they risk derailing the whole train. (Mike Jones, security awareness division, Department of Trade and Industry, UK, interview)
>
> Electronic vandalism. (Warman, London Business School, interview)
>
> Somewhere near vermin. (Zmudsinski, system engineer/manager, USA, interview)

Naturally, hackers often voice a similar appreciation of members of CSI. For example, while admitting psychotic tendencies exist in the hacking community Mofo notes:

> my experience has shown me that the actions of 'those in charge' of computer systems and networks have similar 'power trips' which need to be fulfilled. Whether this psychotic need is developed or entrenched before one's association with computers is irrelevant. (Mofo, hacker, interview)

However, the boundary between these two communities is not as clear as such attitudes might suggest. This can be seen in relation to membership of the communities and the actions members take.

Hackers often suggest the dream that their skills should be used by CSI to explore security faults, thereby giving hackers jobs and

legitimacy to pursue the hack by making them members of CSI. The example of a leading member of one of the most famous hacker groups, the Legion of Doom, is instructive. Eric Bloodaxe, aka Chris Goggans, became a leading member of the hacking community before helping to set up a computer security firm, Comsec, and later moving to become senior network security engineer for WheelGroup a network security company (Quittner and Slatalla, 1995: 145–147 and 160–160). On the CSI side, there have been fierce debates over whether hackers might be useful because they identify security problems (Spafford, 1990; Denning, 1990). Most striking, a number of CSI agencies conduct hacking attacks to test security. IBM employ a group of hackers who can be hired to attack computer systems and the UK government has asked 'intelligence agents' to hack its secure email system for government ministers (Lohr, 1997; Hencke, 1998).[15] In the IBM case, an attempt at differentiating the hired hackers from criminal hackers is made by hiring only hackers without criminal records (a practice akin to turning criminals who have not been caught into police) (Lohr, 1997). Both sides try to assure themselves of radical differences because they undertake similar actions. For example, Bernie Cosell was a USA commercial computer systems manager and one of the most vehement anti-hackers encountered in this study, yet he admitted he hacked

> once or twice over the years. I recall one incident where I was working over the weekend and the master source hierarchy was left read-protected, and I really needed to look at it to finish what I was doing, and this on a system where I was not a privileged user, so I 'broke into' the system enough to give myself enough privileges to be able to override the file protections and get done what I needed . . . at which point I put it all back and told the systems administrator about the security hole. (Cosell, USA systems manager, interview)

More famous is the catalogue of hacks Clifford Stoll had to perpetrate in his pursuit of a hacker, which included borrowing other people's computers without permission and monitoring other people's electronic communications without permission (Stoll, 1989; Thomas, 1990). Such examples mean that differences between the two communities cannot be expressed through differences in what they do but must focus on the meaning of actions. Delineating these meanings is chiefly done through ethical debates about the nature of

hacking conducted through analogies drawn between cyberspace and non-virtual or real space.

CSI professionals often draw analogies between computer intrusion and a range of widely understood crimes. These analogies draw on the claim that a computer is something like a bank, car or house that can be 'got into'. Using this analogy makes it easy to understand the danger of hackers, people who break into banks, schools or houses usually do so for nefarious purposes. The ethical differences between hackers and the CSI become clearly drawn. The problem with such analogies is that, on further reflection, hackers seem strange burglars. How often does a burglar leave behind an exact copy of the video recorder they have stolen? But this unreal situation is a more accurate description of theft in cyberspace because taking in cyberspace overwhelmingly means copying. Further, hacker culture leads hackers to publicise their break-ins, sometimes even stressing the utility of their break-ins for identifying system weaknesses. What bank robbers ring up a bank to complain of lax security? The simple analogy of theft breaks down when it is examined and must be complicated to begin to make sense of what hackers do.

> There is a great difference between trespassing on my property and breaking into my computer. A better analogy might be finding a trespasser in your high-rise office building at 3am and learning that his back-pack contained some tools, some wire, a timer and a couple of detonation caps. He could claim that he wasn't planting a bomb, but how can you be sure? (Cosell, USA systems manager, interview)

Cosell's analogy continues to draw on real world or physically based images of buildings being entered but tries to come closer to the reality of how hackers operate. However, the ethical component of the analogy has been weakened because the damage hackers cause becomes implied, where is the bomb?[16] Cosell cannot claim there will definitely be a bomb, only that it is possible. If all possible illegal actions were prohibited then many things would become illegal, such as driving because it is possible to speed and then hurt someone in an accident. The analogy of breaking and entering is now strong on implied dangers but weak on the certainty of danger. The analogies CSI professionals use continue to change if they try to be accurate. 'My analogy is walking into an office building, asking a secretary which way it is to the records room and making some

Xerox copies of them. Far different than breaking and entering someone's home' (Cohen, CSI, interview). Clearly there is some ethical content here, some notion of theft of information, but it is ethically far muddier than the analogy burglar offers. At this point, the analogy breaks down entirely because the ethical content can be reversed to one that supports hackers as 'whistle-blowers' of secret abuses everyone should know about.

> The concept of privacy is something that is very important to a hacker. This is so because hackers know how fragile privacy is in today's world. . . . In 1984 hackers were instrumental in showing the world how TRW kept credit files on millions of Americans. Most people had not even heard of a credit file until this happened . . . More recently, hackers found that MCI's 'Friends and Family' programme allowed anybody to call an 800 number and find out the numbers of everyone in a customer's 'calling circle'. As a bonus, you could also find out how these numbers were related to the customer . . . In both the TRW and MCI cases, hackers were ironically accused of being the ones to invade privacy. What they really did was help to educate the American consumer. (Goldstein, 1993)

The central analogy of CSI has now lost its ethical content. Goldstein reverses the good and bad to argue that the correct principled action is to broadcast hidden information. If there is some greater social good to be served by broadcasting secrets, then perhaps hackers are no longer robbers and burglars but socially responsible whistle blowers. In the face of such complexities, CSI professionals sometimes abandon the analogy of breaking and entering altogether; 'it is no more a valid justification to attack systems because they are vulnerable than it is valid to beat up babies because they can't defend themselves' (Cohen, CSI, interview). Here many people's instinctive reaction would be to side with the babies, but a moment's thought reveals that in substance Cohen's analogy changes little. A computer system is not human and if information in it is needed by wider society, perhaps it should be attacked.

The twists and turns of these analogies show that CSI professionals use them not so much to clearly define hacking and its problems, but to establish clear ethical differences between themselves and hackers. The analogies of baby-bashing and robbery all try to establish hacking as wrong. The key point is that while these analogies work in an ethical and community building sense, they do not work

in clearly grasping the nature of hacking because analogies between real and virtual space cannot be made as simply as CSI professionals would like to assume.

> Physical (and biological) analogies are often misleading as they appeal to an understanding from an area in which different laws hold. . . . Many users (and even 'experts') think of a password as a 'key' despite the fact that you can easily guess the password, while it is difficult to do the equivalent for a key. (Brunnstein, academic, Hamburg University, interview)

The process of boundary formation between the hacking and CSI communities occurs in the creation of analogies by CSI professionals to establish ethical differences between the communities and their reinterpretation by hackers. However, this does not exclude hackers from making their own analogies.

> Computer security is like a chess-game, and all these people that say breaking into my computer systems is like breaking into my house: bull-shit, because securing your house is a very simple thing, you just put locks on the doors and bars on the windows and then only brute force can get into your house, like smashing a window. But a computer has a hundred thousand intricate ways to get in, and it's a chess game with the people that secure a computer. (Gongrijp, Dutch hacker, interview)

Other hackers offer similar analogies that stress hacking is an intellectual pursuit. 'I was bored if I didn't do anything . . . I mean why do people do crosswords? It's the same thing with hackers (J.C. van Winkel, hacker, interview). Gongrijp and van Winkel also form boundaries through ethical analogy. Of course, it is an odd game of chess or crossword that results in the winner receiving thousands of people's credit records or access to their letters. Hackers' elision of the fact that a game of chess has no result but a winner and a loser at a game of chess whereas hacking often results in access to privileged information, means their analogies are both inaccurate and present hacking as a harmless, intellectual pursuit. It is on the basis of such analogies and discussions that the famed 'hacker ethic' is often invoked by hackers. Rather than hackers learning the tenets of the hacker ethic, as seminally defined by Steven Levy, they negotiate a common understanding of the meaning of hacking of which the hacker ethic provides a ready articulation.[17] Many see the hacker

ethic as a foundation of the hacker community, whereas we see the hacker ethic as the result of the complex construction of a collective identity.

The social process here is the use of analogies to physical space by CSI and hackers to establish a clear distinction between the two groups. In these processes can be seen the construction by both sides of boundaries between communities that are based on different ethical interpretations of computer intrusion, in a situation where other boundaries, such as typical actions or membership, are highly fluid.

Conclusion

The nature of the hacking community needs to be explored in order to grasp the social basis that produces hacking as a facet of computer networks. The figures given previously and the rise of the World-Wide Web hack, offering as it does both spectacular publicity and anonymity, point to the endemic nature of hackers now that world-wide computer networks are an inescapable reality. Hackers show that living in a networked world means living in a risky world. The community found by this research articulates itself in two key directions. First there are a number of components that are the subject of ongoing discussion and negotiation by hackers with other hackers. In defining and redefining their attitudes to technology, secrecy, anonymity, membership change, male dominance and personal motivations, hackers create an imagined community. Second, hackers define the boundaries of their community primarily in relation to the Computer Security Industry. These boundaries stress an ethical interpretation of hacking because it can be difficult to clearly distinguish the activities or membership of the two communities. Such ethics emerge most clearly through analogies used by members of each community to explain hacking.

Hackers are often pathologised as obsessed, isolated young men. The alien nature of online life allows people to believe hackers more easily communicate with machines than humans, despite hackers' constant use of computers to communicate with other humans. Fear of the power of computers over our own lives underpins this terror. The very anonymity that makes their community difficult to study, equally makes hackers an easy target for pathologising. For example, Gilboa's experience of harassment outlined earlier led her to pathologise hackers, suggesting work must be done exploring the

characteristics of hackers she identified – such as lack of fathers or parental figures, severe depression and admittance to mental institutions (Gilboa, 1996: 112). Similar interpretations of hackers are offered from within their community, 'All the hackers I know in France have (or have had) serious problems with their parents' (Condat, hacker, interview). Our research strongly suggests that psychological interpretations of hackers that individualise hackers as mentally unstable are severely limited because they miss the social basis of hacking. Gilboa's experience is no less unpleasant but all the more understandable when the male dominance of the hacking community is grasped.

The fear many have of the power of computers over their lives easily translates into the demonisation of those who manipulate computers outside of society's legitimate institutions. Journalist Jon Littman once asked hacker Kevin Mitnick if he thought he was being demonised because new and different fears had arisen with society becoming increasingly dependent on computers and communications. Mitnick replied 'Yeah . . . That's why they're instilling fear of the unknown. That's why they're scared of me. Not because of what I've done, but because I have the capability to wreak havoc' (Mitnick, cited in Littman, 1996: 205). The pathological interpretation of hackers is attractive because it is based on the fear of computers controlling our lives. What else could someone be but mad, if s/he is willing to play for fun on computer systems that control air traffic, dams or emergency phones? The interpretation of hackers as members of an outlaw community that negotiates its collective identity through a range of clearly recognisable resources does not submit to the fear of computers. It gains a clearer view of hackers, who have become the nightmare of information societies despite very few documented cases of upheaval caused by hackers. Hacking cannot be clearly grasped unless fears are put aside to try and understand the community of hackers, the digital underground. From within this community, hackers begin to lose their pathological features in favour of collective principles, allegiances and identities.

University of East London

Received 6 August 1997
Finally accepted 23 June 1998

Notes

1 Thanks to Sally Wyatt, Alan White, Ian Taylor and two anonymous referees for comments on this piece.

2 Meyer and Thomas (1989) and Sterling, (1992) provide useful outlines of the computer underground, while Rosteck (1994) provides an interesting interpretation of hackers as a social movement. Previous accounts lack detailed survey work.

3 This analysis draws on extensive fieldwork consisting of both a quantitative questionnaire (200 respondents) that outlines the extent and nature of hacking and 80 semi-structured interviews with hackers (30), computer security professionals (30) and other interested parties (20). A full methodology and list of interviewees is available in Taylor, (1993). All notes of the following form (Schifreen, hacker, interview) indicate that Schifreen was a hacker interviewed for this project.

4 It is of course impossible to provide an adequate history of computer networking here and would distract from the main purpose of present arguments. A summary and full references for such a history can be found in Jordan, (1998a).

5 See Jordan, (1998a) for a full discussion of methodologies for counting Internet users.

6 The concept of a 'hacker' has had several manifestations, with at least four other possibilities than a computer intruder. This paper is concerned solely with hacker in the sense of a computer intruder, though see Taylor, (1993) for further discussion (Levy, 1984; Coupland, 1995). It should also be noted that hacking makes most sense within a society in which knowledge has become extensively commodified and is subject to a process in which it can be extensively copied (Mosco and Wasco, 1988).

7 One indication of these difficulties is that the passage of the Computer Misuse Act 1990 in the UK meant it was difficult to persuade UK hackers to discuss their activities but a lack of comparable legislation in the Netherlands removed one barrier to several Dutch hackers allowing interviews to go ahead. For an extensive discussion of the difficulties and advantages of this research methodology, see Taylor, (1993: chapter 2). For a general discussion of such difficulties see Jupp (1989).

8 Professional security consultants, whose interests are best served by a large underground, have placed the number of hackers as high as 50,000 or 35,000 (Sterling, 1992: 77; Gilboa, 1996: 98).

9 A fourth survey exists, the 1991 UK National Computing Centre Survey, but investigates 'logical breaches' (disruption to computer systems) and only provides tangential evidence of hacking. We became aware of John Howard's work too late for inclusion in this analysis (Howard, 1997).

10 Academic (39.5%), commercial (41%), public service organisations (2.5%), other (14%) and some combination of the above (3%).

11 The following categories from the WarRoom survey were joined to create categories of clearly malicious, neither malicious nor benign, and clearly benign: malicious – manipulated data integrity (6.8), introduced virus (10.6), denied use of service (6.3), compromised trade secrets (9.8), stole/diverted money (0.3), harassed personnel (4.5); neither – installed sniffer (6.6), stole password files (5.6), trojan logons (5.8), IP spoofing (4.8), downloaded data (8.1), compromised email/documents (12.6), other (3.0); and, benign – probing/scanning of system (14.6), publicised intrusion (0.5). It is of course possible to argue that any intrusion is malicious and to dispute the division given above.

12 Much more, of course, could be said about the nature of community and the theories referred to here. To prevent this paper becoming a theoretical exposition of well-known work, the understanding of community will be left here.

13 Hackers do indeed hold conferences, such as HoHoCon, SummerCon, PumpCon and DefCon (Rosteck, 1994). See Littman, (1996: 41–44) for a description of such a conference.
14 Anonymity also enables some of the darker fears that emerge about hackers. Finding fearsomely named gangs of hackers running amok in supposedly secure systems can give rise to exaggerated fears, which hackers are often happy to live up to, at least rhetorically (Barlow, 1990).
15 Our research also leads us to believe that CSI uses teams of hackers to test security far more often than CSI professionals publicly admit.
16 Other CSI professionals offered similar analogies, such as finding someone looking at a car or aeroplane engine.
17 Steven Levy distilled a hacker ethic from the early, non-computer intruder, hackers. This ethic is often invoked by all types of hackers and Levy defines the tenets as: all information should be free; mistrust authority, promote decentralisation; hackers should be judged by their hacking, not by bogus criteria such as degrees, age, race or position; you can create art and beauty on a computer; and, computers can change your life for the better (Levy, 1984: 40–45).

References

Anderson, B., (1991), *Imagined Communities*, second edition, London: Verso.
Audit Commission, (1990), 'Survey of Computer Fraud and Abuse', Audit Commission.
Barlow, J.P., (1990), 'Crime and Puzzlement', *Whole Earth Review*, Fall 1990, 44–57.
Castells, M., (1996), *The Rise of the Network Society: the information age, volume 1*, Oxford: Blackwell.
Cherny, L. and Weise, E., (eds), (1996), *Wired Women: gender and new realities in cyberspace*, Seattle: Seal Press.
Clough, B. and Mungo, P., (1992), *Approaching Zero: data crime and the computer underworld*, London: Faber and Faber.
Coupland, D., (1995), *Microserfs*, London: HarperCollins.
deamon9/route/infinity, (1996), 'IP-Spoofing Demystified', *Phrack*, 7 (48), also available at http://www.geocities.com/CapeCanaveral/3498/.
Denning, P., (ed.), (1990), *Computers Under Attack: intruders, worms and viruses*, New York: Addison-Wesley.
Dery, M., (ed.), (1993), *Flame Wars*, London: Duke University Press.
Diani, M., (1992), 'The Concept of a Social Movement', *The Sociological Review*, 40 (1): 1–25.
Dreyfus, S., (1997), *Underground: tales of hacking, madness and obsession on the electronic frontier*, Kew: Mandarin.
Felten, E., Balfanz, D., Dean, D. and Wallack, D., (1996), 'Web-Spoofing: an Internet con game', *Technical Report 540-96*, Department of Computer Science, Princeton University, also at http://www.cs.princeton.edu/sip.
Gilboa, N., (1996), 'Elites, Lamers, Narcs and Whores: exploring the computer underground', in Cherny, L. and Weise, E. (eds), (1996), 98–113.
Goldstein, E., (1993), 'Hacker Testimony to House Sub-committee Largely Unheard', *Computer Underground Digest*, 5.43.
Godell, J., (1996), *The Cyberthief and the Samurai: the true story of Kevin Mitnick and the man who hunted him down*, New York: Dell.

Gow, D. and Norton-Taylor, R., (1996), 'Surfing Superhighwaymen', *The Guardian* newspaper, 7/12/1996, 28.

Hafner, K. and Lyons, M., (1996), *Where Wizards Stay Up Late: the origins of the Internet*, New York: Simon and Schuster.

Hafner, K. and Markoff, J., (1991), *Cyberpunk: outlaws and hackers on the computer frontier*, London: Corgi.

Harasim, L., (ed.), (1993), *Global Networks: computers and international communication*, Cambridge: MIT Press.

Hencke, D., (1998), 'Whitehall Attempts to Foil Net Hackers', *Guardian Weekly*, 26 April, 8.

Howard, J., (1997), 'Information Security', unpublished PhD dissertation, Carnegie Mellon University, available at http://www.cert.org.

Jordan, T., (1995), 'The Unity of Social Movements', *The Sociological Review*, 43 (4): 675–692.

Jordan, T., (1998a), *Cyberpower: a sociology and politics of cyberspace and the Internet*, London: Routledge.

Jordan, T., (1998b), 'New Space? New Politics: cyberpolitics and the Electronic Frontier Foundation', in Jordan, T. and Lent, A. (eds), (1998).

Jordan, T. and Lent, A., (eds), (1998), *Storming the Millennium: the new politics of change*, London: Lawrence and Wishart.

Jupp, C., (1989), *Methods of Criminological Research*, London: Unwin Hyman.

Keller, L., (1988), 'Machismo and the Hacker Mentality: some personal observations and speculations', paper presented to WiC (Women in Computing) Conference.

Levy, S., (1984), *Hackers: heroes of the computer revolution*, Harmondsworth: Penguin.

Littman, J., (1996), *The Fugitive Game: online with Kevin Mitnick, the inside story of the great cyberchase*, Boston: Little, Brown and Co.

Ludlow, P., (ed.), (1996), *High Noon on the Electronic Frontier*, Cambridge: MIT Press.

NCC, (1991), 'Survey of Security Breaches', National Computing Centre.

Meyer, G. and Thomas, J., (1989), 'The Baudy World of the Byte: a post-modernist interpretation of the Computer Underground', paper presented at the American Society of Criminology annual meeting, Reno, November 1989.

Miller, S., (1996), 'Hacker takes over Labour's cyberspace', *The Guardian* newspaper, 10/12/1996, 1.

Mosco, V. and Wasko, M., (eds), (1988), *The Political Economy of Information*, Wisconsin: University of Wisconsin Press.

Quarterman, J., (1990), *The Matrix: computer networks and conferencing systems worldwide*, Bedford: Digital Press.

Quarterman, J., (1993), 'The Global Matrix of Minds', in Harasim, L. (ed.), 1993, 35–56.

Quittner, J. and Slatalla, M., (1995), *Masters of Deception: the gang that ruled cyberspace*, London: Vintage.

Ross, A., (1991), *Strange Weather*, London: Verso.

Rosteck, T., (1994), 'Computer Hackers: rebels with a cause', honours thesis. Sociology and Anthropology, Concordia University, Montreal, also at http://www.geocities.com/CapeCanaveral/3498/.

Shimomura, R., (1996), *Takedown: the pursuit and capture of Kevin Mitnick, the world's most notorious cybercriminal – by the man who did it*, with John Markoff, London: Secker and Warburg.

Spafford, E., (1990), 'Are Computer Hacker Break-Ins Ethical?, Princeton University Technical Report, CSD-TR-994, Princeton.

Spertus, E., (1991), 'Why are there so few female computer scientists?', unpublished paper, MIT.

Sterling, B., (1992), *The Hacker Crackdown: law and disorder on the electronic frontier*, London: Viking.

Sterling, B., (1994), 'The Hacker Crackdown three years later', only published electronically, available at http://www.uel.ac.uk/research/nprg.

Stoll, C., (1989), *The Cuckoo's Egg: tracking a spy through the maze of counter-espionage*, New York: Simon and Schuster.

Taylor, P., (1993), 'Hackers: a case-study of the social shaping of computing', unpublished PhD dissertation, University of Edinburgh.

Thomas, J., (1990), 'Review of The Cuckoo's Egg', *Computer Underground Digest*, 1.06.

Turkle, S., (1984), *The Second Self: computers and the human spirit*, London: Granada.

WarRoom, (1996), '1996 Information Systems Security Survey', WarRoom Research, LLC, available at http://www.infowar.com/.

