Taylor, Paul A. 1999. Hackers. Routledge.

1 *Them and us*

The hack

It is an interesting fact that most scientific research and speculation on deviance concerns itself with the people who break rules rather than with those who make and enforce them. If we are to achieve a full understanding of deviant behavior, we must get these two possible foci of inquiry into balance. We must see deviance, and the outsiders who personify the abstract conception, as a consequence of a process of interaction between people, some of whom in the service of their own interests make and enforce rules which catch others who, in the service of their own interests, have committed acts which are labelled deviant. ... It is, of course, possible to see the situation from both sides. But it cannot be done simultaneously. That is, we cannot construct a description of a situation or process that in some way fuses the perceptions and interpretations made by both parties involved in a process of deviance. We cannot describe a 'higher reality' that makes sense of both sets of views. We can describe the perspectives of one group and see how they mesh or fail to mesh with the perspectives of the other group: the perspectives of rule-breakers as they meet and conflict with the perspectives of those who enforce the rules, and vice versa. But we cannot understand the situation or process without giving full weight to the differences between the perspectives of the two groups involved.

(Becker 1963: 163, 173)

The key focus of this work is not just the computer underground in isolation, but rather upon the *them and us* conflictory relationship that exists between the computer security industry and the computer underground. In order to understand a social group labelled as *deviant* one needs to pay due attention to its ongoing interaction with those labelling it and not just attempt to research the group being labelled as deviant:

> We can construct workable definitions either of particular actions people might commit or of particular categories of deviance as the world (especially, but not only, the authorities) defines them. But we cannot make the two coincide completely, because they do not do so empirically. They belong to two distinct, though overlapping, systems of collective action. One consists of the people who co-operate to produce that act in question. The other consists of the people who co-operate in the drama of morality by which 'wrongdoing' is discovered and dealt with, whether that procedure is formal or quite informal.
>
> (Becker 1963: 185)

It is this conflict between the computer underground and those opposing groups who seek to stigmatise it as deviant that makes hackers an intriguing exemplar of how social practices dynamically emerge within technological environments.

The contested term

In its original technological sense, the word 'hacker', coined at MIT in the 1960s, simply connoted a computer virtuoso. That's still the meaning enshrined in the 1994 edition of the New Hacker's Dictionary, which defines such a person as someone 'who enjoys exploring the details of programmable systems and how to stretch their capabilities; one who programs enthusiastically, even obsessively'.

(Roush 1995: 1)

> The word hack doesn't really have 69 different meanings. ... In fact, hack has only one meaning, an extremely subtle and profound one which defies articulation. Which connotation is implied by a given use of the word depends in similarly profound ways on context. ... Hacking might be characterized as 'an appropriate application of ingenuity'. Whether the result is a quick-and-dirty patchwork job or a carefully crafted work of art, you have to admire the cleverness that went into it. An important secondary meaning of hack is 'a creative practical joke'. This kind of hack is easier to explain to non-hackers than the programming kind. Of course, some hacks have both natures.[1]

Before looking in detail at the rhetorical conflicts that have occurred between hacking's supporters and opponents, we turn to the act itself and the semantic debate that surrounds it. I seek to highlight the slippery nature of the term and emphasise that there is no one single, uncontested description of hacking. The fact it has disputed meanings and connotations for different groups is addressed in terms of group boundary formation within computing. I trace the evolution in the meaning of the term and show it to be part of a complex social process in which certain computer users have become marginalised within the wider computing community. Whether such marginalisation is justified or not is perhaps a moot point given the potentially serious implications it may have for the computers that now saturate our society, an issue I will return to in the concluding chapter.

The meaning of the term, *hacking*, has gone through several changes from its

original dictionary definition: of 'cut or chop roughly; mangle: cut (one's way) through thick foliage etc.: manage, cope with': to its present definition of: 'gain unauthorised access (to data in a computer)' [The Concise Oxford Dictionary, eighth edition]. It has also evolved from the MIT days of the 1950s onwards when it was first used in the context of computing. The phrase was originally used to denote the highly skilled but largely playful activity of academic computer programmers searching for the most elegant and concise programming solution to any given problem (Levy 1984). It has since been increasingly associated with its present-day connotation of illicit computer intrusion.

The origins of the phrase, *hacking*, relate to the problems encountered with programming the early cumbersome and huge computers such as the IBM 704, described by Levy as a 'hulking giant' (Levy 1984: 25). These valve-based machines were notoriously unreliable, a factor that, combined with the relative immaturity of programming methods, led to solutions to any particular computing problem being rather haphazardly constructed (thus meeting the phrase's first connotation of something being fashioned roughly: being *hacked together*). In addition, the baroque complexity and unmanageability of early software systems can also be associated with hacking's connotations of 'managing or coping with' and 'cutting through thick foliage'. The key themes from the various definitions of hacking relate to: exploration; obsession; and ingenuity/creativity. The potentially exploratory and obsessive elements of hacking are explored in the next chapter; at this point we will concentrate upon the ingenuity and creativity said to lie behind the bona fide hack.

The hack

> Bobby was a cowboy, and ice was the nature of his game, ice from ICE, Intrusion Countermeasures Electronics. The matrix is an abstract representation of the relationship between data systems. Legitimate programmers jack themselves into their employers' sector of the matrix and find themselves surrounded by bright geometrics representing the corporate data. Towers and fields of it ranged in the colorless nonspace of the simulation matrix, the electronic consensus-hallucination that facilitates the handling and exchange of massive quantities of data. Legitimate programmers never see the walls of ice they work behind, the walls of shadow that screen their operations from others, from industrial-espionage artists and hustlers like Bobby Quine. Bobby was a cowboy. Bobby was a cracksman, a burglar, casing mankind's extended electronic nervous system, rustling data and credit in the crowded matrix, monochrome nonspace where the only stars are dense concentrations of information.
>
> (Gibson 1986b: 197)

The basis of hacking culture is unsurprisingly 'the hack'. The hack did, and still does in various quarters, refer to the performing of a neat programming trick.

Despite its present predominant connotations of illicit computer break-ins, within hacking circles it is more widely defined as an attempt to make use of any technology in an original, unorthodox and inventive way. The main bone of contention in these differing interpretations is the extent to which the ingenuity of the hack should be made subordinate to its legality. Whilst this debate will be pursued in depth later, the hack is initially presented here in its widest sense in order to assess any potential commonality that may exist between all its illegal, mischievous and legitimately ingenious forms.

Turkle (1984) provides a thorough delineation of the main elements of hacking. She conflates the wider definition of illicit hacking with the general mentality of those who hack in its sense of seeking to manipulate any technology for unorthodox means. She refers to *the hack* as being: 'the holy grail. It is a concept which exists independently of the computer and can best be presented through an example using another technology complex enough to support its own version of hacking and hackers' (Turkle 1984: 232). The example she uses is that of phone-phreaking[2] and one of its main adherents, John Draper, alias *Captain Crunch*[3]. The hack, in this instance, refers to such technological stunts as having two phones on a table; talking into one and hearing your voice in the other after a time-delay in which the original call has first been routed around the world.

Turkle interpreted this type of hack in the following manner:

> Appreciating what made the call around the world a great hack is an exercise in hacker aesthetics. It has the quality of [a] magician's gesture: a truly surprising result produced with ridiculously simple means. Equally important: Crunch had not simply stumbled on a curiosity. The trick worked because Crunch had acquired an impressive amount of expertise about the telephone system. That is what made the trick a great hack, otherwise it would have been a very minor one. Mastery is of the essence everywhere within hacker culture. Third, the expertise was acquired unofficially and at the expense of a big system. The hacker is a person outside the system who is never excluded by its rules.
>
> (Turkle 1984: 232)

The main characteristics of a hack are thus:

1. **Simplicity**: the act has to be simple but impressive.
2. **Mastery**: the act involves sophisticated technical knowledge.
3. **Illicitness**: the act is 'against the rules'.

The ubiquitous hack and *the kick*

It is important to note that a key aspect of Turkle's analysis is the notion that the essential attributes of a hack can be found in relation to artefacts other than

computers. In keeping with the perspective of some hackers she highlights the eclectic pragmatism with which hackers characteristically approach all technologies. Hacking has traditionally involved such diverse activities as lock-picking and model-railway maintenance (and the accompanying tinkering with gadgetry that this involves).[4] Hackers themselves express the wide range of their potential targets:

> In my day to day life, I find myself hacking everything imaginable. I hack traffic lights, pay phones, answering machines, micro-wave ovens, VCR's, you name it, without even thinking twice. To me hacking is just changing the conditions over and over again until there's a different response. In today's mechanical world, the opportunities for this kind of experimentation are endless.
>
> (Kane 1989: 67–9)

The heterogeneous range of technological targets considered 'hackable' is described by R., a Dutch hacker, who argued that hacking is not just about computer break-ins but should be defined so that it does not:

> only pertain to computers but 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're using the technology in a way that it's not supposed to be used. Now that also pertains to telephones, if you're going to use your telephone to do various things that aren't supposed to be done with a telephone, then that's a hack. If you are going to use your skills as a car mechanic to make your motor do things it's not supposed to be doing, then that's a hack. So, for me it's not only computers it's anything varying from locks, computers, telephones, magnetic cards, you name it.
>
> (R., Utrecht interview)

Hackers' brushes with the criminal system have led to vivid illustrations of the ubiquitous nature of their activity and the extent to which it consists of an ability to adapt to the circumstances one finds oneself in. There is, for example, Kevin Poulsen's account of his time in prison:

> 'I've learned a lot from my new neighbors', Poulsen, the quintessential cyberpunk ... who describes hacking as performance art, said from behind the glass of the maximum security visitor's window. 'Now I know how to light a cigarette from an outlet and how to make methamphetamine from chicken stock'.
>
> (Fine 1995: website)

The phone network was the archetypal system for the early precursors of hackers, the *phone-phreaks*, the Internet providing the next complex technical

system ripe for exploration. In addition to such examples of hands-on hacking, which involve ingenious manipulations of whatever artefacts are at hand, hacking can also refer more abstractly to the 'system' one is confronted with. A US hacker using the sobriquet, *Agent Steal*, for example, published an article from Federal Prison entitled: 'Everything a hacker needs to know about getting busted by the feds', the theme of which centres around the notion that the legal system, like any other system, is there to be hacked:

> The criminal justice system is a game to be played, both by prosecution and defense. And if you have to be a player, you would be wise to learn the rules of engagement. The writer and contributors of this file have learned the hard way. As a result we turned our hacking skills during the times of our incarceration towards the study of criminal law and, ultimately, survival. Having filed our own motions, written our own briefs and endured life in prison, we now pass this knowledge back to the hacker community. Learn from our experiences ... and our mistakes.
>
> (Petersen 1997: website)

Two Dutch hackers, Rop Gongrijp[5] and M.,[6] in relating some of their activities illustrate how broad the desire to technologically explore can be. M. claimed to have physically explored the subterranean tunnels and elevator shafts of Amsterdam including Government nuclear fall-out shelters (Utrecht interview). Gongrijp, similarly, related how he had entered the out-of-bounds areas of buildings such as banks by pretending to accompany legitimate tour groups and then took the first opportunity to wander off on his own, assessing the security of the site and then somewhat cheekily informing the security staff of that assessment. The 'technology', which is the subject of their curiosity in these cases, simply being the architecture and security features of buildings that they found interesting. Gongrijp described in a further example of the heterogeneity of hacking, how 'the Wageningen agricultural university a couple of years ago had a couple of students doing a project enhancing the genes of marijuana plants, to me that's gene-hacking, it's more than science, it's just somebody gets a kick out of it'.[7] He argued that hacking is a frame of mind, a sort of intellectual curiosity that attaches itself to more than just one type of technology or technological artefact: 'for me a hacker is more all-round than to some people, I think a hacker is not a real hacker unless he has a basis in two or three skills, not just hacking Unix systems but also a little bit of something else, electronics, audio hacking or something general' (Amsterdam interview).

This heterogeneity of hacking's targets fuels *the kick* gained from satisfying the primary urge of technological curiosity:

> in the early days of say the uses of electricity and how to generate it, were first developed, I think Tesla and all the people who were playing with it then were as much hackers as most computer hackers are now, they are

playing on the frontier of technology and all those hefty experiments were not only done for science, they were done because they got a kick out of it.

(Gongrijp: Amsterdam interview)

The *kick*, thus gained, crucially depends upon an element of inventiveness that serves to distinguish 'true' hacks from those that could be labelled as acts of *Nintendo Perseverance*, that is to say, hacks who exhibit large amounts of concentration and dedication rather than ingenuity. Methods of hacking entry may become widely publicised by means of the various branches of the hacker grapevine, for example, electronic and paper-based specialist magazines, or even word-of-electronic-mouth. From such sources, hacking 'cook-books' of prepackaged instructions result. Those that predominantly, or exclusively, use such sources of information for the illicit use of a technology could be labelled hackers since they fulfil the main requirement of the pejorative definition of hacking: the illicit use of a technology. The Dutch hackers I spoke with, however, were keen to differentiate themselves from such people, by imparting their concept similar to Turkle's description of the Holy Grail type hack.

Using the example of phone-phreaking phone calls Gongrijp illustrates this distinction between a technical and a 'true' 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, leaves it regardless. He's a stupid ignoramus, yeah? The second situation is another hacker reads this and thinks, 'hey, this is an idea, let's expand on this'. So what he does is go to a phone box, he cuts the wire, puts a magnetic switch in between, puts the magnetic switch up against the case, closes the door again and whenever he wants to make a free phone call, he puts a magnet on top, makes the wires disconnect, and he has a free phone call, goes away, takes the magnet away and everybody else has to pay. Now he's more of a hacker straight away, it's not a simple black and white thing.
>
> (Gongrijp: Utrecht interview)

Chris Goggans, a US hacker, makes a distinction between hackers and what he terms computer criminals. He says:

> People have been trying to come up with these 'hacker-cracker knick-knack paddywacker' tags, but here's the difference: a hacker is someone who is interested in computer systems and networks and wants to take them to whatever possible reach they can go. A cracker is someone who breaks software copy protection.
>
> (Goggans: email interview)

A computer criminal, meanwhile, at least according to one definition has a specific goal of targeting someone's mail or research, or going after other information considered proprietary' (Lange 1996: 3). Thus in the definition favoured by self-styled 'real' hackers a true hack should involve an element of originality reflected in the unorthodox subversion of any given technical situation. There are various forms a hack can take, and a hacker tends to be defined not just by what he does but by how he does it. Gongrijp, for example, mischievously pointed out to me, as we walked through an Amsterdam housing estate, startlingly vivid yellow paint on road over-pass supports. He explained that it was indelible anti-graffiti paint and observed wryly that people could cause havoc if they used such paint for graffiti purposes (Amsterdam interview).

Criminal activities of hackers

Alongside the more contestable categories of hacking activity with their own purported ethic and *kick* there are some more straightforwardly criminal variants of technological endeavour that should perhaps be acknowledged early on. Whilst most of the emphasis placed upon criminal types of motivation for hacking comes from figures within the computer security industry, conventional criminality was also recognised by several of the hackers I spoke to, one of whom, D., whilst claiming it was only to see if it could be done, demonstrated on the table of the café in which the interview took place his prototype magnetic credit-card copier:

> By the way, this is the card-copier, I'm proud of it. [So what does it copy?] Everything. [Everything with a magnetic strip?] Yeah, I'll let you hear how a credit-card sounds, the trick is you take two cards, you slide them through here at the same time, yeah well it gives the same sound but then it copies from this one to this one, you can also use this for credit cards, there's a different sound, I can hear what kind of card it is through the ear-phones.
>
> (D.: Utrecht interview)

Similarly, whilst interviewing at a hacker group's flat in Amsterdam I was also shown their latest prototype touch-tone dialler that they were in the process of miniaturising further, and which was being used as a means of phreaking free phone calls by emulating electronically the switching tones of the international digital phone systems:

> Well, I can show you something, this device, this chip, is also available in a very small package, it will fit into this whole thing [a small touch-tone dialler case]. This whole prototype will be in here [large sandwich board of electronics], he [a colleague] is working on the board now. What this basically does is, it's a touch-tone dialler that has extra features which mean you can make tones which are called C5 to control the phone system and to tell phone switches in other countries that they should complete calls without

charging you for it, so with this system you can make free phone calls, and it's all going to be in a little dialler this big, it's pretty nifty ... you can have it make these tones and try things at different times, there's all these protocols for in-band telephone signalling in there, it's fully programmable. ... We make our phone calls with this type of technology so it doesn't cost anything.

(G.: Amsterdam interview)

Whereas G. and his colleagues were not, or would not admit to being, interested in the potential commercial aspects of this activity, D. was much more forthcoming. When I asked him about monetary reward being a possible motivating factor behind hacking, he related how:

A friend of my brother ... is only concerned with the money he gets for it [and] all kinds of schemes he has to make things. Free phone calls, there's a lot of business in it. They sell cards, copy cards and things like that. Car phones: they change the chip with the ID of the car phone, things like that.

(D.: Utrecht interview)

He then proceeded to give more details of his own personal involvement in a scheme aimed at funding an excessively large phone bill that had been accumulated as a product of his hacking exploits:

The first system we attacked was the Spanish telephone system, it was about seven years ago, we didn't have a meter to check the costs, later we found that when we called Spain, there was one special tone which activated the computer and we had a phone bill of 10,000 guilders, so we made little boxes, blue boxes, and me and my brother went to Spain with the boxes. Well, we first sent the taxi driver to pick up the boxes and then waited to see if the taxi driver came back without the police and then we took the boxes and sold them to all kinds of people, dealers of cars and such like, it was very hard to deal with the Spanish people because they can't get money from the banks very easily, they have to show where the money is going, per box we asked 1,500 guilders, so after ten boxes we paid the bill and got back to Holland.

(D.: Utrecht interview)

D. believes that there is the possibility that hacking expertise will become more widely used by criminal elements in society:

If you keep it illegal then I think in the future there will be more people who will be interested in it, really malicious people, right now there aren't so many people who want to sell it to espionage or companies or whatever, but I think in the future there will be more people, you always see people who are interested but they don't have the means to hack themselves. There was

a hackers' party, the 'galactic hackers' party' in Amsterdam and we were trying to make free phone calls and always someone behind you, some foreigner from Egypt 'free phone calls, free phone calls'. The only thing he could say in Dutch was 'free phone calls', and they offer a lot of money to make free phone calls and stuff: often companies if they want to know something else about other companies – like a friend of mine had an account that would check out all companies, they were offered money to check out other companies but when they wouldn't do it, they would get in trouble.

(D.: Utrecht interview)

R., another Dutch hacker, also gave his perspective on monetary-induced hacking. In an attempt to quantify a perhaps inevitably vague area, I asked him to give me a percentage figure for the number of hackers that hack for monetary gain. He replied:

No, you can't say it in percentage, I'd guess it's about five persons in the whole of Holland that do it for the money. For instance I had a hack and somebody wanted to publish it, he gave me money for it. Now, did I do it for the money? No, not initially, initially I did it for the kick, not because it was illegal but for the kick. Okay, so I earned a little money with it, big deal, I didn't do it for the money, and another reason is convenience, pure convenience. It is very convenient if you can make free phone calls, it is absolutely convenient if you can pull copies off magnetic cards, it is very easy if you can get your TV at home without a de-scrambler, things like that. And it's not a kick, it's not a thrill, it's not that it's illegal, it's just pure convenience.

(R.: Utrecht interview)

One group in the early 1990s that was much more criminal-minded, and recognised as such by G., D. and R., were known as the *Amiga Kids*, after the computers they used most. When discussing viruses D. described how:

There are a lot of viruses in the Amiga world. That's one of the groups they have to get rid of, the Amiga Kids, that's a real pain in the arse. Also for hackers, if we hack a system and they find out about it, like making free phone calls, they spread it. It's incredible, those guys are really destructive, because when they use something they use it for software, we use it occasionally for hacking or making calls but they use it twenty-four hours a day for software, they'll do anything for software, they use and abuse credit cards and things like that. Anything for software, and a few of them, I know, are the ones that write viruses to combat other groups, to put viruses in the programs of other groups, I hate those guys. Yeah, here in Utrecht there are a lot of these groups and they card a lot of stuff, you know carding? Using credit cards to get stuff, but illegally. They wear Rolexes, little kids on the street with Rolexes around their wrists it's incredible.

(D.: Utrecht interview)

Whilst the hackers that formed the basis of this study were at pains to disassociate themselves from such groups, they recognised the potential for hacking-related activities to branch into criminal activity. A hacker called Maelstrom related how:

> In 1989 a local friend put up a world headquarters BBS for the West German group Red Sector Inc. They were into writing Amiga demos, and were one of the top ten groups in the world, which got us a lot of interesting and well-known callers. We obtained a voice mailbox and put up a codeline on it, which was very popular for a long time. RSI made me an offer: if I would give them stolen AT&T calling-card numbers to enable them to call the USA, they give me all the hardware I needed to have the ultimate computer system. I was offered computers, high-speed modems, hard drives, and software ... the only catch was their method. Using CBI or TRW's computer, some people use credit-card numbers to steal merchandise, and by having stolen stuff sent to West Germany, they were able to escape detection when the theft was discovered since the post office there didn't keep records. This was against my morals, and I dropped out of the scene for a while.
>
> (Maelstrom: email interview)

Finally, for obvious reasons, it was difficult to look in any depth at hacking conducted solely for criminal or monetary purposes, or even to check the absolute validity of claims such as D.'s above. What I did see of the above instances seemed to be real methods of fraud, and the hackers I spoke with, with the exception of the Zoetermeer group, all had knowledge of each other and seemed to verify each other's claims and accounts. Hacking with criminal intent or for monetary gain of some sort appeared, from my interviews in Holland at least, to be conducted on the fringes/margins of mainstream hacking and then only in order to fund their activity rather than for express monetary gain. The pressure to commercialise their activity may, however, be increasing as techniques become more widely desired by traditional criminal groups.

2 Hacking culture

The hacking generations

> The 'original' hackers were computer professionals who, in the mid-sixties, adopted the word 'hack' as a synonym for computer work, and particularly for computer work executed with a certain level of craftmanship. ... Then in the seventies, assorted techno-hippies emerged as the computerized faction of the counterculture of the day. ... What characterized the second wave hackers was that they desperately wanted computers and computer systems designed to be useful and accessible to citizens. ... Finally, in the second half of the eighties the so-called cu emerged, appropriated the terms 'hacker' and 'hacking' and partly changed their meaning. To the computer underground, 'to hack' meant to break into or sabotage a computer system, and a 'hacker' was the perpetrator of such activities.
>
> (Hannemyr 1997: 2)

In the most seminal piece of work on hackers to date Levy (1984) describes three generations of hackers who exhibited to various degrees qualities associated with the hacking's original connotation of playful ingenuity epitomised by the earliest hackers, the pioneering computer *aficionados* at MIT's laboratories in the 1950s and 1960s. These *aficionados* formed the first generation of hackers defined as those who were involved in the development of the earliest computer-programming techniques. The second generation are defined as those involved in bringing computer hardware to the masses with the development of the earliest PCs. The third generation refers to the programmers who became the leading lights in the advent of computer games architecture. The phrase *hacker* is now almost exclusively used to describe an addition to this schema: the fourth generation of hackers who illicitly access other people's computers.

To the fourth generation of hackers can also arguably be added a new group: the *microserfs* identified by Douglas Coupland in his novel of the same name.[1] This generation represents the co-optation of hacker skills by commercial computing. Whilst there were still elements of this commercial acumen in hacking's second and third generations, they kept the positive connotations of the hacker sobriquet because their activity still retained the pioneering qualities