Taylor, Paul A. 1999. HACKERS Routledge

Introduction

The following sections in this introduction expand upon the theme of the sensationalistion of hacking referred to in the Preface. This is done to provide a context for the subsequent analysis of hacking and is necessary groundwork for an exploration of the social processes at work in the depiction of hacking by both its opponents and proponents.

Fear, ignorance and vulnerability: hyping hacking

> The cops, and their patrons in the telephone companies, just don't understand the modern world of computers, and they're scared. 'They think there are masterminds running spy-rings who employ us,' a hacker told me. 'They don't understand that we don't do this for money, we do it for power and knowledge.' Telephone security people who reach out to the underground are accused of divided loyalties and fired by panicked employers. A young Missourian coolly psychoanalyzed the opposition. 'They're overdependent on things they don't understand. They've surrendered their lives to computers.'
>
> (Sterling 1991: 4)

Whilst the allegedly criminal aspects of hacking alone would seem enough to create a media interest in the activity, it also contains a mysterious technological element manifested in the lay person's uninitiated awe of computers' complexities and capabilities.[1] Despite the possible existence of reasons for us to welcome their maverick spirit, hackers also serve to remind us of our technological vulnerability/ignorance. This has been manifested in the problems experienced by law enforcement officials and legislators in their encounters with the computer underground and are perhaps merely smaller-scale illustrations of some of the wider problems society encounters as it attempts to assimilate new information technologies into existing social structures. There have been various cases of alleged over-reactions to computer security incidents by law enforcement agents. A legal example is provided by the E911 case whereby a member of the hacker group Legion of Doom, Craig Neidorf, was accused of threatening the safety of residents

throughout the US by having copied a document containing details of the telephone emergency 911 system. When the case came to trial the federal prosecutors were embarrassed when it was proved by the defence team that the allegedly sensitive document valued at $80,000 was in fact available to the general public for $13.[2]

The authorities' often dramatic response to hackers and their activities was perhaps most vividly manifested in the series of police raids on the homes of hackers code-named 'Operation Sun Devil' by gun-carrying US law enforcement officers. Officers were accused of over-reacting to the physical threat posed by hackers in their homes by entering with their guns drawn and of removing excessive amounts of computing equipment unrelated to their specific investigations. Whilst such a response can be interpreted as exhibiting displaced fear it is also viewed by some as deliberate strategy that fulfils a pragmatic function:

> Where the target of the raids is an individual, usually at his or her own home, this simple approach to raid and seizure is ... entirely appropriate and very effective. Hackers and paedophiles in particular are used to dealing with people and problems by means of remote connections; suddenly to be faced with by a veritable army of (in the US, gun carrying) officers is usually sufficient to persuade total – indeed, often *abject* – co-operation.
>
> (Barrett 1997: 157 [emphasis in the original])

A British perspective on allegedly over-zealous law enforcement is provided by the father of the 16-year-old London-based hacker, Richard Pryce, who was accused of hacking into the systems of US military bases:

> It was around 7 p.m. and I was watching TV when about eight cars pulled up and people started banging on the door. When I answered it, the officers came filing in ... there were so many of them, I thought he must have killed someone. They burst into his room and pulled his hands away from his computer keyboard. They then stripped his room. When I went up the stairs he was sitting there in shock while they were ripping up his floor-boards. They searched his room for 5 hours.
>
> (Sterling 1991: website)

Similarly, with reference to the case of Kevin Poulsen,[3] his attorney, Paul Meltzer, argued: 'It's ludicrous, it's absurd. ... They can't decide if they've got a kid playing in his garage or Julius Rosenberg'.[4] Meltzer said he was 'very disturbed by the inability of federal prosecutors to distinguish between assault with a deadly weapon and assault with a computer. I mean, c'mon, the guy's non-violent' (Fine 1995). Poulsen's own words are also instructive:

> The trouble began before I was released. I planned on living with my parents when I got out of prison, until I could find employment and live on my own. My probation officer anticipated this months before my release-date, and visited my parents. He was shocked to find that they had recently purchased an IBM compatible computer, and he warned them that they must get rid of it before I moved in. They didn't have a modem, mind you, but as a notorious hacker I might easily fashion a modem out of ordinary household appliances. ... It got even more interesting when I was released. When I reported to my P.O., he explained to me that, not only could I not use any computer, with or without a modem, but that *I couldn't be in the same room as a computer.* ... Judge Real declined to second-guess the decisions of the probation officer, and specifically rejected the contention that I should be allowed to obtain employment that allows access to computers without modems, noting, 'Who knows what a computer can do?'
>
> (Poulsen undated-a: website)

Justin Petersen, (alias *Agent Steal*) reinforces the claim that there is an apparent culture and knowledge gap between hackers and the legal authorities. Petersen spent forty-one months in Federal Prison for hacking into a bank's computer and transferring funds. Whilst serving his sentence he met up with Chris Lamprecht (alias *Minor Threat*), another hacker. He describes how:

> The prison officials were terrified of us. They became obsessed as they read our mail, screened our magazines, listened to our phone calls, and sent informants to try and infiltrate our little group of technophiles. The only conclusion they could come to was that they had no idea what we were up to. When the computer at the prison industries plant crashed, Chris was promptly fired from his job there. It wasn't his doing, but unbridled paranoia spreads far and wide among bureaucrats.
>
> (Petersen 1997: website)

This general fear and ignorance of the authorities towards the abilities of hackers is further evident from Chris Lamprecht's experience of the court system. His judge, Sam Sparks, stipulated in his sentencing that:

> Upon release from imprisonment ... for a term of three years, the defendant cannot be employed where he is the installer, programmer, or trouble shooter for computer equipment; may not purchase, possess or receive a personal computer which uses a modem; and may not utilize the Internet or other computer networks.
>
> (cited in Thieme 1996: 21)

From the perspective of the computer underground:

> Doesn't Sparks know that anyone with a few dollars can buy a social security number in the data marketplace? Besides, good hackers are equally adept at 'social engineering.' If Lamprecht talks someone out of their social security number, should we cut out his tongue? In short, does the judge have a clue as to how life is led these days? Lamprecht's former boss, Selwyn Polit of

> ODT, laughed when asked about the case. 'They're dead scared of him because of the computer stuff,' he said. 'They treat him differently because they think if he just thinks about computers, he can do magical things.' Unfortunately, Lamprecht's statements feed these projections. He plays enthusiastically to the 'evil hacker genius' image.
>
> (Thieme 1996: 21–2)

A cultural gap is again evident in the fate of a young bulletin board operator in New Brunswick in 1985, held liable for the material posted by other users. His arrest, in 1985, led Jeffrey Fogel of the ACLU to use a forceful analogy[5] in order to claim that the youth was unfairly singled out: 'He has an electronic bulletin board and arresting him and seizing his computer amounts to seizing a printing press', Fogel said. 'It would be like if someone put a stolen credit card number in a newspaper classified. Would you close down the newspaper?' (PR Newswire 1985). Frustration from the computer underground at the perceived inappropriateness of the establishment's fear-induced responses is exhibited in the way in which metaphors are reappropriated in order to reinforce their own rhetorical points:

> Denying a criminal access to computer networks is like breaking his fingers for writing a hold-up note and forbidding him to use a pen. When the crime has nothing to do with computers or networks in the first place, it's like putting him into a sensory-deprivation tank simply to punish him.
>
> (Thieme 1996: 21)

Hacking's predominantly non-physical character and its accompanying air of mystery tends to heighten its potential for creating fear and anxiety. Its anonymity mixed with its illicit nature makes it easier for the media to portray the actions of hackers, who are rarely seen in the flesh, in such forms as 'electronic stalkers'. According to the convicted hacker, Kevin Poulsen: 'Criminal cases involving suspected unauthorized computer access, or "hacking", are frequently subject to wild, unsubstantiated, and often bizarre claims by prosecutors and investigators' (Poulsen undated-b). This claim of a tendency to over-dramatise would seem to be at least partially borne out by the ominous sounding subtitle of the book written about his exploits, *The Watchman*. This seemed designed to make a none-too-subliminal association with serial killing, being subtitled: *The Twisted Life and Crimes of Serial Hacker Kevin Poulsen.*

Hackers who hype

> It was no longer enough to break into computer systems, now it was essential to break into the limelight of national media attention, as well.
>
> (Hawn 1996: 2)

The hyperbole and mystery surrounding hacking is not always something that hackers passively suffer. They also make use of the immaterial anonymity of cyberspace in order to heighten the effects of the various on-line personae they adopt. On occasion they can revel in exaggeratedly malevolent poses: 'Cyberspace is a new world and in it the hacker is a datalord, a baudrate barbarian who takes what he wants' (Marotta 1993: 3). Under the cover of anonymity hackers project threatening personalities to the outside world and media facilitating the subsequent over-reactions of the police and legal establishment. Hacking groups generally choose colourful names such as 'Bad Ass Mother Fuckers, Chaos Computer Club, Circle of Death, Farmers of Doom'[6] and this can create a self-fulfilling prophecy in terms of the authorities' response. Anonymity allows hackers to indulge in extravagant role-playing whereby they form a dangerous underground movement with revolutionary credentials:

> Since we are engaged in Revolutionary War in Cyberspace ... Our Guerilla Warfare Operating Area, (GWOA), is the Internet. ... Our greatest tactical advantages are the speed of light and non location specificity. ... One small voice in Cyberspace becomes global interpersonal communication at the speed of light as the net grows geometrically. Global interpersonal communication is the greatest tool for world peace our species has ever known. We have the technology to achieve virtual collective consciousness on a planetary scale. The potential of the Electronic Revolution is awesome. Instead of electing an aristocracy whose choices are packaged by mass media marketing to govern us, we have the ability to transcend the physical limitations of deceptive appearance, and illuminate the truth of being through the digitized reflection of intelligence.
>
> (Davis undated: website)

Barlow (1990), questions the actual malevolence of such poses with reference to a group of hackers who had previously frightened him with a similar sort of aggressive email posturing. When he actually came face to face with two of the hackers they:

> were well scrubbed and fashionably clad. They looked to be as dangerous as ducks. But ... as ... the media have discovered to their delight, the boys had developed distinctly showier personae for their rambles through the howling wilderness of Cyberspace. Glittering with spikes of binary chrome, they strode past the klieg lights and into the digital distance. There they would be outlaws. It was only a matter of time before they started to believe themselves as bad as they sounded. And no time at all before everyone else did.
>
> (Barlow 1990: 48)

Aided by the choice of deliberately provocative handles, the eventual outcome of the hyperbole caused through anonymity is the danger that hackers become victims of their own hype. Barlow's experience is a direct illustration of

Becker's observation: 'Treating a person as though he were generally rather than specifically deviant produces a self-fulfilling prophecy. It sets in motion several mechanisms which conspire to shape the person in the image people have of him' (Becker 1963: 34). Similarly, Thieme notes in relation to the New Brunswick arrest of a bulletin board operator cited earlier that 'the case illustrates not only the great gulf fixed between those who use the Net and those who don't, but also how the image of hackers as "evil geniuses" can distort the perception and judgement of those who play into the image – as well as those who fear and misunderstand it' (Thieme 1996: 21). The result of this distortion of judgement can be profound:

> Before I first met with the computer hacker and convicted felon who goes by the handle of Minor Threat, I am warned. 'You have no idea what these people can do,' says a reporter who's familiar with the digital underground. She tells me Minor Threat and his hacking buddies are cyber sociopaths who get off on mangling credit histories, tampering with telephone lines, invading email accounts, and crashing hard drives. 'They might mess with you just because they can,' she says. 'It's a power game.' ... So I am prepared to greet Darth Vader beind the razor wire of the federal correctional institute. ... Sitting in the waiting room amid drug dealers and armed robbers, he looks more like a refugee from a college chess tournament than a high-tech supervillain. Yet Lamprecht is serving a 70 month sentence ... many who know Lamprecht and the hacking subculture say that law enforcement officials are overreacting, spooked by the harm they perceive hackers can do as much as by actual misbehavior.
>
> (Heiman 1997: 70)

In my correspondence with Gisle Hannemyr, a Norwegian computer security officer, he took exception to the idea that the media is solely used by those seeking to stigmatise hackers:

> As you point out, the media prefers the sensational to the factual, and you seem to imply that the computer security industry is in cahoots with the media to create a designer enemy. To me, it looks as if the main conspiracy is between the press and the computer underground – not between the press and the computer security industry. Why this is, we can only speculate. It is easy to understand what the media gains from the relationship (stories that sell papers), but the motivation of the computer underground is more subtle. My guess is that it is part attention-seeking (if you can't be famous, you can at least be notorious) – plus that some individuals (Chris Goggans comes to mind) have managed to make substantial profits from their notoriety as computer underground heroes.
>
> (Hannemyr: email interview)

Life after the Cold War

> 'Massive networking makes the US the world's most vulnerable target', said William Studeman, former deputy director of the CIA. Jamie Gorelick, a former deputy attorney-general, was even more blunt in her address to a Senate hearing on the subject: 'We will have a cyber equivalent of Pearl Harbor'.
>
> (*Sunday Times* 17 May 1998: 26)

A specific historical and cultural context that arguably contributed to some of the responses to hacking identified above is the post-Cold-War *Zeitgeist* where new scapegoats are sought to apportion blame for widespread feelings of vulnerability. For example, in a 1994 report on global organised crime, the Center for Strategic and International Studies, an independent research centre formerly associated with Georgetown University, asserted that 'a despot armed with a computer and a small squad of expert hackers can be as dangerous and disruptive as any adversary we have faced since World War II' (cited in Roush 95: 4). Various media accounts make full use of the cold-war imagery in order to emphasise the vulnerabilities hacking throws into sharp relief. The UK Sunday tabloid newspaper, the *News of the World*, for example, provides the following account under the headline 'I had my finger on Doomsday button':

> Hunched in a cramped bedroom in his parents' terraced house, computer whiz-kid Mathew Bevan felt a creeping chill as he gazed at the image on the screen before him. Against all the odds – and using just a £400 High Street system – the 17-year-old had hacked into the American Air Force's FLEX project ... **F**orce **L**evel **Ex**ecution. With an awful realisation he watched his twitching index finger hover over the nuclear button. One twitch more, he says, and he might have launched a Peacekeeper missile with a 150 kilotons nuclear payload. Its maximum range is 12,000 kilometres. It guarantees total devastation within a 20-mile radius of impact. With that, Bevan could lay waste to whole cities, kill millions ... and start World War III. *For a few numbing seconds his Cardiff street was mission control for the apocalypse.*
>
> (*News of the World* 23 November 1997: 43 [emphasis in the original])

Whilst the significance of the above sentiments could be played down by reference to the sensationalistic excesses of tabloid journalism, not too dissimilar sentiments are encountered in a broadsheet newspaper's account of the US's vulnerability to hackers:

> President Bill Clinton will announce plans this week to build ramparts against a new and invisible enemy threatening to spread more chaos in America than any conventional terrorist attack. He will unveil defence measures unprecedented in the history of human conflict to protect America from the potentially devastating peril posed by cyber warfare, in

which computer systems controlling airports, hospitals, traffic lights, banks and even nuclear weapons could be destroyed creating havoc. It sounds like a science fiction fantasy. But it is already happening. This month the Pentagon reported 'a series of systematic attacks' on its computer systems in an incident considered so ominous that the President was told it could be the work of Iraq's Saddam Hussein. The prospect of Saddam hiring a computer hacker to try to cripple American computer systems fills defence experts with horror: by a strange paradox, America's technological superiority and consequent dependence on computers, leave it more vulnerable than most countries to cyber attack.

(*Sunday Times* 17 May 1998: 26)

The feelings of vulnerability experienced by otherwise extremely powerful groups are caused by the potent mix of the anonymity of one's opponent (and the exaggerated perceptions such anonymity may then give rise to) and the paradox that one's own apparent strength and superiority may in fact prove to be an Achilles' heel. This combination of factors is portrayed as the new threat, coming quickly after a Gulf War which illustrated the apparent unassailability of the US's conventional military capability:

> Making things even more difficult for American defence experts is not knowing who the enemy is. Whether they are disgruntled Americans, Hamas terrorists or pariah dictators such as Saddam, the attackers could wage cyber warfare undetected on any laptop computer from the Sinai desert to Singapore. Just as exasperating for the government would be deciding how to deploy its vast military. 'If you don't know who your enemy is, how can you retaliate?' said one expert. This makes cyber warfare the great equaliser, a cheap and effective weapon for any Third World rogue state or small terrorist organisation wanting to wage war against a superpower – and win. All they might need is a few million dollars to hire a handful of 'cyber mercenaries' capable of penetrating supposedly secure government systems.
>
> (*Sunday Times* 17 May 1998: 26)

One might expect that the use of Cold-War imagery and language would be restricted to those on the right of the political spectrum. However, in a book otherwise devoted to analysing the Internet as an extension of Western imperialist practices, somewhat reactionary language is used to describe the role of those opposing the dominant system:

> Cellular phone ... hackers can tap into any conversation and trace anyone almost anywhere. ... Online terrorism is not too far away and most of the early proponents of this sick art are hackers. While some hackers will be causing increasing havoc, other hackers will be tracking them down.
>
> (Sardar 1996: 23)

> The disturbing prospect is that opposition to the microcybernetic consumerist dictatorship will then find its only effective location deep underground, in the hands of zealots or fanatics who are content to destroy without bothering to dialogue. And microcybernetic technology is particularly vulnerable to just such a sort of opposition; as we have seen, hackers generally get caught only when they become brazen; and a determined band of computer nihilists, endowed with patience as well as skill, could even now be ensconced deep in the system, planting their bugs, worms and bombs.
>
> (Ravetz 1996: 52)

The loss of the old certainties of the Cold War thus seems to affect Right and Left equally. The purported vulnerability to attack from outsiders used as part of Cold-War rhetoric is recycled here in the new context of the hi-tech world. The ability of phone-hackers to eavesdrop and trace people's whereabouts is implicitly placed on the same level of concern as that given to the 'microcybernetic consumerist dictatorship'. The ambivalence with which hackers are viewed addressed earlier in this chapter resurfaces here when hacking is emotively described as a 'sick art' whilst at the same time there is the explicit recognition of society's dependence upon such figures: 'while some hackers will be causing increasing havoc, other hackers will be tracking them down'.

Books and movies about hacking: specific examples of media coverage

> Popular media's fascination with things subversive and spectacular ... has the unfortunate side effect that it hides the 'other side' of hacking, the side that involves skilled craftsmen who believe that a computer is more than a means of production – it is, among many other things an instrument for creation, communication, mastery, artistic expression and political empowerment.
>
> (Hannemyr 1997: 2)

Given the above acknowledgement that hackers are not averse to sensationalising their activity, the widespread sensationalising of hacking by those seeking to marginalise and stigmatise hackers is, for a variety of reasons to be explored at length in the rest of this book, potentially debilitating for a society struggling to come to terms with the full ramifications of the information society and all the potentially profound changes that concept may signify for our everyday lives.[7] To illustrate briefly the media's role in sensationalising hacking, I describe below the non-fictional accounts of hacking and Hollywood's movie portrayals.[8]

Books

There is frequently in non-fictional accounts of hacking a rather curious mix of self-indulgent reliance upon seemingly trivial, tangential or simply mundane

details of different hacking episodes coupled with a simultaneous and frequent resort to hyperbolic description. Voluminous biographical details are provided on hackers and their dedicated but inevitably repetitive activities are described in exhaustive and somewhat exhausting detail. In *The Cuckoo's Egg*, for example, we are given various descriptions of the author's girlfriend and seemingly irrelevant details of their shared Californian lifestyle, in conjunction with a narrative suffused with recourse to references about the excitement of detective work and the underlying menace of KGB spying. In *Cyberpunk* the authors illustrate the use of hyperbolic imagery with their consideration of the issues at stake in the hiring of a hacker for security work: 'But hire such a mean-spirited person? That would be like giving the Boston Strangler a maintenance job in a nursing-school dormitory' (Hafner and Markoff 1991: 40). An overtly sensationalist tendency is evident in a sample of the titles and subtitles of some of the best-known recent books from the spate of non-fictional and journalistic accounts of hacking published in recent years:

The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage (Stoll 1989);
Cyberpunk: Outlaws and Hackers on the Computer Frontier (Hafner and Markoff 1991);
The Hacker Crackdown: Law and Disorder on the Electronic Frontier (Sterling 1992);
Approaching Zero: Data Crime and the Computer Underworld (Clough and Mungo 1992);
Takedown: The Pursuit and Capture of Kevin Mitnick the World's most Notorious Cybercriminal – by the Man who did it (Shimomura with Markoff 1995);
Masters of Deception: The Gang That Ruled Cyberspace (Quittner and Slatalla 1995);
The Fugitive Game: Online with Kevin Mitnick, the Inside Story of the Great Cyberchase (Littman 1996);
The Cyberthief and the Samurai: The True Story of Kevin Mitnick and the Man who Hunted him Down (Godell 1996);
Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier (Dreyfus 1997);
The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen (Littman 1997).

The movies

Various movies have used hacking for their subject matter including: *War Games*, *Sneakers*, *Die Hard II*, *The Net*, *Hackers* and *Johnny Mnemonic*. Whilst it is perhaps unsurprising that such a topical issue with particularly appealing subject matter (high technology, a subculture of apparently rebellious and anarchistic youths, the security of the nation, etc.) the movies' representations of hacking have had a disproportionately important influence upon the legislative response to the activity. Over-reliance upon fictional portrayals of hacking[9] by the authorities has contributed to helping to create a generally fearful and ignorant atmosphere surrounding computer security, which has in turn led to the charge to be fully analysed subsequently that hackers have become the victims of a somewhat hysterical witch-hunt:

> Anti-hacker hysteria had gripped the nation in 1990. Huge law enforcement efforts had been mounted against illusory threats. In Washington DC … a Congressional committee had been formally presented with the plot-line of a thriller movie – DIE HARD II, in which hacker terrorists seize an airport computer – as if this Hollywood fantasy posed a clear and present danger to the American republic. A similar hacker thriller, WAR GAMES, had been presented to Congress in the mid-1980s. Hysteria served no one's purposes, and created a stampede of foolish and unenforceable laws likely to do more harm than good.
>
> (Sterling 1991: 6)

That fictional movie portrayals of hacking have assumed the status of fact for key members of the establishment has rather obvious and worrying implications given their fundamentally unrealistic nature:

> A Hollywood thriller film about hackers – is very much part and parcel of the Hollywood thriller film tradition. Hollywood is not in the business of journalism or social analysis; Hollywood is in the mass entertainment business. I hope you wouldn't think that Hollywood gangsters or Hollywood cops bear much coherent resemblance to the quotidian daily lives of actual gangsters and actual cops. Nevertheless, cops go to cop films and gangsters go to gangster films, and sometimes gangsters (like George Raft) even become actors. Sometimes cops (like Joseph Wambaugh) become authors whose work is filmed. Criminals tend to be unrealistic and not very bright, so a lot of them have found compelling role models in deeply unrealistic screen portrayals of dashing, snappily-dressed criminals. Teenagers are also easily star-struck, so the film WAR GAMES was a major factor in the mid-80s boom of teenage computer-hacking. But to go to a typical hacker movie and think that the thrilling cyber-derring-do on the screen is a factual portrayal of the bleak, voyeuristic tedium of actual hacking – well, don't do that. It would be silly.
>
> (Sterling: email interview)

Hackers themselves would seem to concur with Sterling's evaluation of the factual accuracy of hacker movies:

> In the recent round of "Netsploitation" films, the worst offender was most likely *Hackers*. When we got the press photos we couldn't believe that Hollywood would actually think that hackers look like that. We have never seen any hacker on rollerblades. In fact, we have never seen a hacker break sweat.
>
> (Newton undated: website)