Hacking:The Performance of Technology?

***Hacker Culture*, Douglas Thomas. Minneapolis: University of Minnesota Press, 2002. Pp. xxvii + 266. ISBN 0-8166-3345-2.**

The word "hacker" has an interesting double-meaning: one vastly more widespread connotation of technological mischief, even criminality, and an original, meaning amongst the tech-savvy as a term of highest approbation. Both meanings, however, share the idea that hackers possesses superior ability to manipulate technology according to their will (and, as with God, this superior ability to exercise will is a source of both a mystifying admiration and fear). This book mainly concerns itself with the former meaning. To Thomas this simultaneously mystified and vilified, elusive set of individuals exemplifies "the performance of technology" (p. xx), showing the way in which "the cultural, social and political history of the computer...is fraught with complexity and contradictions" (p. ix). In fact he claims that hacking is more a cultural than a technological phenomenon, citing Heidegger's, "[t]he essence of technology is not anything technological" (p. 56).

In part one of the book, "The Evolution of The Hacker", Thomas claims *secrecy* to be the defining issue of "hacker culture". Society has an ambivalent, contradictory relationship to secrecy, which the pranks of hackers highlight in paradoxical and/or 'supplementary' ways. For instance, "[s]ecrets can preserve an institution's identity, but...they can also prevent a hacker from being identified" (p. xi). Hackers play with these contradictions (the hacker "both deploys

and disturbs the notion of the secret" (p. 189)). Thomas seeks a "genealogy of secrecy" in the Foucauldian sense.

To this end, Thomas retells much of hacking's history, from its little-known origins in phone "phreaking", through the hacker Eden of the 1960s. During this period (still fondly remembered by many participants) in the computer labs of MIT, Cornell and Harvard information and equipment were shared and it was accepted that any person had the right to tinker with anything that they could improve (such that, "[i]n a perfect hacker world...anyone pissed off enough to open up a control box near a traffic light and take it apart to make it work better should be perfectly welcome to..." (p. 15)). Thomas notes the irony, however, that much of the funding for these wonderfully free and creative communities derived from the military. The 1970s saw the birth of proprietary software and the beginning of the end of hackers' freely sharing files, tools and information, all of which corporations began to assert ownership of. This moment is perhaps epitomised in Bill Gates' famed cease-and-desist "Open Letter To Hobbyists" regarding sharing of his Altair BASIC. Thomas suggests that the "old school" of hackers capitulated to much of this enclosure of the hacking commons, causing the next hacker generation to mix anger with admiration for them. (Not all of the old school *did* capitulate however, a notable exception is Richard Stallman's Free Software Foundation and its unique "copyleft" licence, a discussion of which would have complicated Thomas' argument.)

Thomas credits two events with causing the concept of the hacker to jump into popular consciousness: the evocative 1983 movie "War Games", and the misguided release in 1988 by a college student of the infamously damaging Internet Worm. A major crackdown by law

enforcement agencies followed in the early 1990s, which led to a certain politicization of the hacker community. Thomas finishes by sketching some of today's issues, such as the split in the hacker community between so-called "white hats" (who protect systems and – allegedly – hack only with consent) and "black hats" (who do not).

As well as hacker history, Thomas explores hacker "language-games". Hackers famously play with spelling and the ASCII character set, writing words such as "3133+" ("elite"). This phenomenon bears a curious similarity with certain postmodernists' notorious semiotic play. Thomas draws materiality of the sign conclusions from this, arguing that hackers' letter-replacements are "not merely substitutions but translations", which remind one "first and foremost, that writing itself is a kind of technology" (p. 57). A somewhat formulaic nod to Plato's *Phaedrus* follows (p. 58).

In part two, "Hacking Representation", Thomas examines literature produced by hackers themselves, the way they are represented by nonhackers, and the complex interplay between the two. (For instance, hackers are "prone to precisely the same kind of overstatement and mischaracterisation of their activities that the media and government officials are" (p. 117)). Hackers are revealed in this section as superb wielders of irony. Firstly, the editors of the underground magazine *Phrack*, aware that their publication was assiduously studied by law-enforcement agencies and corporations, formally copyrighted their work, stating that it was available free of charge to "the amateur computer hobbyist", but that any "corporate, government, legal or otherwise commercial usage" was forbidden without "prior registration", at a fee of $100. Though many wrote in saying that they were planning to pay, "but don't tell

anyone", only one person ever did, which the editors delightedly sermonized about in the magazine. Thomas's analysis of this act is somewhat utilitarian. ("If *phrack* was to be watched or monitored, this agreement was designed to make sure that those who ran *phrack* could monitor the monitors" (p. 129). Editor Chris Goggan's own words, however, speak more of an intrinsically glorious act ("I named several people who were not only getting the magazine but in one case, they were spreading it around and, of course, none of them even contacted me for registration. I had a riot with it. It was a lot of fun" (p. 128-9)).

Secondly, when the Hollywood movie "Hackers" (widely scorned by the genuine article) appeared, some hackers defaced the "Hackers" website. The following new text appeared:

> Hackers, the new action adventure movie from those idiots in Hollywood, takes you inside a world where there's no plot or creative thought...When a seriously righteous hacker uncovers MGM's plot to steal millions of dollars, Dade and his fellow "throwbacks of thespianism"...must face off against hordes of hackers, call in the FBI,and ponder a sinister UNIX patch called a "Trojan". Before it's over, Dade discovers his agent isn't taking his calls any more, becomes the victim of a conspiracy and falls into debt. All with the aid of his VISA card. Want the number? (p. 167).

Again, Thomas's analysis of this hilarious piece of play is rather 'straight':

> There are two basic points of critique in this Web page hack. First, the hackers assert that the film is in some way unrepresentative of hacker culture...A second critique has to do with the very premise of the film. Those who hacked the web page argue that MGM...cannot make a film about hackers and global capitalism without implicating itself (pp. 167-8).

In Part Three, “Hacking Law”, Thomas explores “the juridical construction of the hacker”. The issue of the *punishment* of hackers, and its relationship to technology, is obvious grist to his Foucauldian mill. He notes “[t]he highly sexualized metaphors of penetration and ravaging (p. 177)” often used to describe hackers’ activity. Also, hackers would seem to trespass in the systems they penetrate, but in what sense? Despite the fact that they are not physically present in, say, the Pentagon’s mailserver, and even their virtual presence takes the form of a feigned on-line persona with a different name, “it is the hacker’s body that must be found, identified and ultimately prosecuted” (p. 185).

In this regard, Thomas tells the story of the hunt for the body of Kevin Mitnick, who was tracked down and arrested in 1995. Thomas notes how much focus was put by the press on Mitnick’s body. It was noted over and over that he had a weight problem. He was unilaterally diagnosed as having “an addiction” which led him to hack and he was ordered to attend 12-step meetings (p. 192). His body was also legally severed from all contact with computers, Sony Walkmans, even telephones (which led to him being put in solitary confinement for 8 months in an earlier jail sentence). Thomas suggests that much of the fierceness of such penalties arises from hackers’ being “made to stand in for an issue of great cultural anxiety” (p. 216), i.e. the increasing role of technology and attendant surveillance in everyone‘s life. This last section is possibly the most interesting of the book. Thomas seems to have thought deeply about the issues concerned. Also it is just a great (*albeit* tragic) story.

Much of the history and life of hackers recounted in this book has been told already (see, for instance, Bruce Sterling, *The Hacker Crackdown*). However to take a postmodernist perspective

on the phenomenon is novel and Thomas' treatment of many issues is very suggestive. Much of hackers' irony and intervention does indeed seem to embody a 'supplementary' logic not capturable by a purely analytic perspective. Ironically, however, Thomas himself in his presentation of "hacker culture" is relentlessly discursive. How would hackers themselves respond to this deployment of postmodernist theory? Is it possible that they might 'hack' it? The hacker spirit is curious in that despite being so apparently irresponsible, it is also robustly practical. Hackers accord respect to those who can manipulate technology according to their will, and gain the power that comes from that. They are quick to lampoon just about anything else. Thomas has done his homework, but the fact that he is not a programmer is evident in remarks such as, "Certain software is written to handle information in terms of a "buffer"." (p. 105). Whether there might be some perspective which could embrace postmodernist insights with respect to the logic of irony and intervention, and hackers' unparalleled understanding of how to actually do things with technology, and what might be able to be 'hacked' by someone who possessed such a perspective, is an interesting question.

CATHY LEGG.

Cycorp, University of Melbourne.