HACKING

DIGITAL MEDIA AND SOCIETY SERIES

TIM JORDAN

Hacking

Digital Media and Society Series

Mark Deuze, *Media Work*
Alexander Halavais, *Search Engine Society*
Robert Hassan, *The Information Society*
Tim Jordan, *Hacking*
Jill Walker Rettberg, *Blogging*

Hacking

Digital Media and Technological Determinism

TIM JORDAN

polity

First published in 2008 by Polity Press

Polity Press
65 Bridge Street
Cambridge cb2 1ur, UK

Polity Press
350 Main Street
Malden, ma 02148, USA

ISBN-13: 978-0-7456-5815-5

A catalogue record for this book is available from the British Library.

Typeset in 10.25 on 13 pt FF Scala
by Servis Filmsetting Ltd, Stockport, Cheshire
Printed and bound in Great Britain by MPG Books Ltd, Bodmin, Cornwall

the publisher has no responsibility for the websites and can make no guarantee that a site will remain live or that the content is or will remain appropriate.

Every effort has been made to trace all copyright holders, but if any have been inadvertently overlooked the publishers will be pleased to include any necessary credits in any subsequent reprint or edition.

For further information on Polity, visit our website:
www.polity.co.uk

Contents

Acknowledgements

Thanks to Andrea Drugan and her team who suggested looking at hacking in a series about digital media. Andrea and Jonathan Skerrett were very helpful during writing and production. Several anonymous reviewers offered suggestions which made significant improvements. I drew on years of discussion with far too many people to mention, thanks to all of them. Of course, all mistakes are my own.

To hacking, god knows what I owe in general, but specifically this was written using OpenOffice, operating system Ubuntu. For less specific but nonetheless more important support, thanks to Masters Lite at Clissold Swimming Club and the Ancient Shadows. For the most important things in life, thanks to Matilda and Joanna, though the adventure has been more mountainous while writing this book than I could have expected.

CHAPTER ONE

The Hack

Introducing hacking

The hack is a way of understanding what is possible, sensible and ethical in the twenty-first century. This overview of hacking will explain those who hack and their communities, because only by grasping hacking in the full sense of the people who hack and the social and cultural relations within which they live can we open up some important facets of twenty-first-century life. Further, only by exploring the norms and cultures found in this community will we open up a side to our existence that has arrived – whether we like it or simply put up with it or hate it – with the growing ubiquity of computers and the ever-expanding connections produced by computer networks.

Kevin Mitnick is a hacker, though some would demand he be called a cracker. He became famous for a number of activities: being held responsible for breaking the security on a US government computer security advisor's system, using a technique (IP-spoofing) that had not been documented before; for breaking into the corporations Fujitsu, Motorola, Nokia and possibly others, seeking software for mobile phones to try and secure his own systems; and, for being the hacker who was held in solitary confinement because someone claimed he could launch nuclear weapons by whistling phone tones down a phone line (Shimomura 1995; Littman 1996). Mitnick subsequently became a computer security consultant.

Linus Torvalds is a hacker. He became famous for leading the development of an operating system called Linux. This

complex software package began as a technical exercise for Torvalds, who wrote and released the core component (the kernel) of an operating system. Subsequently, Torvalds oversaw an expanding collective effort to write more and more components of it, until Linux emerged as a free, sophisticated operating system which is considered by many to be a technically significant rival to Microsoft's Windows operating system.

Torvalds and Mitnick exemplify the two core components of hacking: cracking, and free software and open source programming. Between these components are generated dynamics which create the particular characteristics of hacking, but these two are not the only components of hacking. We will explore how hacking is used to affect society though such things as cyberwar, cyberterrorism, hacktivism and cybercrime. We will also explore the way hacking is not solely about programming or using computers when we examine connections between Creative Commons, hackers who do not programme, the programming proletariat and hacking sub-cultures. Finally, all these various components will be drawn together to consider the meaning of hacking.

All these different hacking activities exist within a set of communal relations, each of which expresses a different aspect of hacking. I stress this embeddedness in life because the hack needs a social and cultural context. The hack does not breathe well in the abstract air of philosophy or ethics but rather lives intimately entwined with a number of communities or groups of hackers. The action of the hack is thus a material practice, it occurs within various collective ethics, norms and constraints embodied in wires, code, flesh and electricity. To introduce hacking, we can look at 'the hack' and then place this action in the context of its collective material practices. Having done so we will be able then to turn back and look at hacking, hackers and the hack

as a whole object, whose meaning for the twenty-first century we will then be able to examine.

Once I outline what an action has to be to have any hope of being considered a hack, I can then trace the hack in its material manifestations. This requires first examining the two key components of hacking; cracking (chapter 2) and the Free Software and Open Source movement (chapter 3). First, there are the crackers who break open your computer and sneak inside, for their own purposes. Second, there are the open so(u)rcerers who build digital freedoms through new infrastructures in the digital world. Following this we will be able to explore the complexity of hacking by adding in those who take the hack and apply it to society (chapter 4) dealing with such phenomena as war, crime, terrorism and political protest. Then we will be able to see some of the ways programming and hacking intertwine in hackers who do not programme or programmers who do not hack, as well as opening this out to see general symbolic cultures of hacking (chapter 5). Finally, the meaning of hacking can be explored allowing us to see the importance of understanding hacking for understanding the twenty-first century's obsession with information (chapter 6).

The essence of a hack

Before exploring what a hack means, two quick examples of a hack will be useful. These are not meant to capture the full picture of hacking but rather to offer specific instances. The '@' sign used in email addresses is a hack. When the first networks were being set up email was attached to several of them as a hack; that is, programmers simply wrote means of sending mail to each other into the software controlling the network without any direction or authorisation (Quartermain 1990; Hafner and Lyon 1996: 190-2; Abatte 2000). For example, Ray Tomlinson added a means of sending electronic mail using the ARPA network,

one of the most important forerunners of the Internet. He later answered the question ‘Why did you do it?’ by writing ‘Mostly because it seemed like a neat idea. There was no directive to “go forth and invent email” . . . A colleague suggested that I not tell my boss what I had done because email wasn’t in our statement of work. That was really said in jest’ (Tomlinson 2006). It could have been anything, but Tomlinson chose ‘@’ because, (1) it was a sign that did not appear in names; (2) some took ‘@’ to mean ‘at’; and (3) it was not in use on the computer systems he was thinking of (though it caused trouble for some other systems Tomlinson had forgotten about, which used ‘@’ to mean ‘erase line’) (Tomlinson 2006). Another key figure in the genesis of the Internet, Jon Postel, commented when he saw Tomlinson’s addition to ARPAnet, ‘Now, that’s a nice hack’ (cited in Hafner and Lyon 1996: 192).

In June 2007, the Pentagon removed access to the Internet from as many as 1,500 computers because they had discovered a hacker had gained illicit access to an unclassified email system. It was reported that the compromised system did not contain any military information and they were taken off line to repair the security breach. Then US Secretary of Defence Robert Gates noted that Pentagon systems were subject to hundreds of hack attacks a day (Modine 2007).

Here are two very different types of hackers: Tomlinson, who acts like an engineer, and the anonymous Pentagon cracker who acts like a bandit. They both raise the question: what moves individuals to push technology beyond what it is supposed to be doing? For many, being a hacker is about autonomy, politics and fun but above all it is about making a difference in the world that presents itself to them; whether that is breaking illicitly into computers or writing the software someone wants. Torvalds described his view of hacker motivations as being beyond survival.

> A ‘hacker’ is a person who has gone past using his computer for survival (‘I bring home the bread by programming.’) . . . That is how something like Linux comes about. You don’t worry about making that much money. The reason that Linux hackers do something is that they find it to be very interesting.
>
> (Torvalds 2001: xv)

Creativity and sharing figure large in Torvalds’ interpretation of hackers’ motivations. Erik Petersen – as a cracker he is a very different hacker to Torvalds – focuses in his explanation on a related but slightly different view when he was asked what it is in hacking that appeals to him: ‘It’s the control, the adrenaline, the knowledge, the having what you’re not supposed to have’ (cited in Littman 1996: 91).

The hackers Torvalds is thinking of seek something they want, something so far not implemented in a free, open operating system, and Petersen seeks hidden knowledge. The hack is the moment when a hacker gains access to these goods seemingly placed beyond him or her. The motivations are manifold; control, entertainment, adrenaline, political principles, and they all fuel the desire for access to something new, something previously unknown to the hacker.

Hackers of all sorts talk lovingly of the hack, often imbuing it with mystical properties. In a sense the hack is the way hackers touch the infinite, the way they imbue their actions with spiritual meaning and(or) change the world. This leads to an extension in which the hack has been so lovingly polished that it is at times hard to see how a hack is distinct from any creative action. Understood this way the hack need not be about computers and computer networks. Burrell Smith, an important figure in the creation of Apple’s Macintosh computer argued: ‘Hackers can do almost anything and be a hacker. You can be a hacker carpenter. It’s not necessarily high tech. I think it has to do with craftsmanship and caring about what you’re doing’ (cited in

Himanen 2001: 7). Put somewhat more practically, but making the same point, a hacker named Gonggrijp stated:

> 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 the 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?
>
> (Cited in Taylor 1999: 18)

Gonggrijp puts his finger squarely on the point that the hack needs to create something new. Gonggrijp and Smith both point to this moment of creation noting that it can sit outside of the computer networks and computers normally associated with hackers. We reach here an abstract definition of the hack, most clearly expressed in what was *The Hacker's Dictionary* and has become *The Hacker Jargon File*, an online resource tracking the language of hackers: 'Hacking might be characterised as an "appropriate application of ingenuity" ' (TJF 2006).

The writing of a programme to send electronic messages using the '@' was just such an ingenious application and while many disapprove of cracking, the Pentagon hacker obviously found an ingenious way of controlling military servers. This extension of hacking beyond the digital realm into any and all realms has been enthusiastically endorsed by some, who propound a hacker ethic as a new model for wildly divergent interests.

For example, Himanen sees hacking as a new approach to the philosophy of business. He argues that hackers represent a new 'work ethic', comparable to the Protestant work ethic that Weber argued underpinned the rise of capitalism. Himanen argues that the hacker work ethic is the spirit of the information or network society and consists of seven values: passion, freedom, social worth, openness, activity, caring and, the highest value, creativity. Himanen

argues this ethic is applicable across all forms of work (Himanen 2001). In contrast, Wark sees hackers as the new revolutionary class. He argues that the information society is a third stage of property relations following from property based on land, then on capital and now on information. These stages are not successive but accumulate, each with a ruling and a revolutionary class. Hackers in their pursuit of free creativity turn out to be, for Wark, the revolutionary class of the twenty-first century (Wark 2004).

These are rather opposing views of what hacking means; from network society's handmaiden to network society's nemesis. Wark calls himself a crypto-Marxist in opposition to Himanen's crypto-Weberianism, and accuses Himanen of aiding the ruling class by obfuscating the exploitations of network society (Wark 2004: 72 fn.). Yet despite this ideological divide, Wark and Himanen are united in defining the hack as something beyond a particular community whose primary concerns are with computers and computer networks. For Himanen, the highest and defining value of the hacker work ethic is creativity: 'creativity – that is, the imaginative use of one's own abilities, the surprising continuous surpassing of oneself and the giving to the world of a genuinely valuable contribution' (Himanen 2001: 141). For Wark:

> To hack is to differ . . . Hackers create the possibility of new things entering the world. Not always great things, or even good things, but new things. In art, in science, in philosophy and culture, in any production of knowledge where data can be gathered, where information can be extracted from it, and where in that information new possibilities for the world produced, there are hackers hacking the new out of the old.
>
> (Wark 2004: 3–4)

Both Himanen and Wark define hacking's essence as the ability to create new things, to make alterations, to produce differences. We might think of this as the abstract essence of the hack. Here we meet the nature of the hack in its plainest aspect yet we also reach a cul-de-sac, for this kind

of abstraction relates to everything and nothing. The hacker R argued that ‘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’ (cited in Taylor 1999: 16). But this is problematic, for if even the boiling of water in an unusual way is a hack then doing anything different is a hack. Any form of creativity for Himanen or any production of difference for Wark, is a hack. While finding a theoretical essence for the hack they have lost hackers and hacking. A cultural version of this freeing hacking from any relation to a specific technology or community is given by Thomas:

> we must regard technology as a *cultural* and *relational* phenomenon. Doing so, I divorce the question of technology from its instrumental, technical, or scientific grounding. In fact, I will demonstrate that tools such as telephones, modems, and even computers are incidental to the actual *technology of hacking*. . . . I argue that what hackers and the discourse about hackers reveals is that technology is primarily about mediating human relationships, and that process of mediation, since the end of World War II, has grown increasingly complex. Hacking, first and foremost, is about understanding (and exploiting) those relationships.
>
> (Thomas 2002: xx–xxi)

Again, hacking becomes everything. In Thomas’ case hacking does not even refer to the specificity of innovation or the production of difference but to the mediation of human relationships. Thomas’s point follows from the recognition that technologies are not asocial but, like everything else, mediated in and through social relationships. However, this should be merely a starting point; hacking will become the same as everything else if it is not developed to recognise the different relationships that produced different technologies that are characteristic of hacking. At the margins, hackers might call working on boiling water a hack but this is a margin that can only be understood from a basis in which hackers are engaged in the socially mediated technologies of computers and networked communication. For one last example, and to underline that the abstractness of a definition of hacking is

not restricted to theorists such as Wark, Himanen and Thomas but is felt by hackers, here is one more hacker expanding his horizons:

> In my day to day life, I find myself hacking everything imaginable. I hack traffic lights, pay phones, answering machines, micro-wave ovens, VCRs, 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.
>
> (Kane 1989: 67–9)

Such a view of the hack empties it of content except for such a general idea of change that the hack can become anything and everything. The objection to theories such as Wark's and Himanen's and to claims such as Kane's that I am making is that by re-interpreting a hack beyond computers and existing hacker communities, they have overgeneralised the nature of the hack and in so doing have trivialised it.

While the work we have looked at allows us to grasp something important about the hack – that it involves a moment when something new appears – we have also journeyed too far from real hackers and real hacks; we have joined in on a process of abstraction that reduces hacking to a miasma covering all social life. However, this journey has been important for two reasons. First, it allows me to distinguish this account of hacking from the overgeneralisations that permeate other accounts of hacking. Second, it means we have identified a particular moment in the creation of difference which must be present for a hack to occur. Now we need to take this creative moment and place the hack back into its social context.

The hack

At the moment we can hypothesise that the hack involves altering a pre-existing situation to produce something new; to hack is to produce differences. We can also be clear that this is too abstract and vague a description because it refers

to everything, from making toast to declaring war. An understanding based on the hack as a material practice implies both the materiality of bodies and technologies in addition to the community relations that permeate and surround such bodies and technologies. To develop such a grounded definition of the hack we can take forward the examples and discussion that have already been given, but it is also important to take up existing definitions of hacking that are based on sustained empirical engagement with the hack.

Sherry Turkle argued for a particular understanding of the hack which was later endorsed by Taylor, who produced one of the first extensive empirical studies of hackers (Turkle 1984: 232; Taylor 1999: 13–15). They agreed on three characteristics of the hack.

> Simplicity: the act has to be simple but impressive
> Mastery: the act involves sophisticated technical knowledge
> Illicitness: the act is ‘against the rules’.
>
> (Taylor 1999: 15)

The most important limitation of Taylor’s and Turkle’s definition is that it resulted from an examination of one of the subgroups of hacking: the cracking community. Accordingly, being illicit is highly valued but this is not necessarily as highly prized within the innovative cultures of free software and open source hackers. We can for the moment set aside being illicit as a core component of an all-encompassing definition of the hack, though we will come back to explore it in particular situations.

Taylor’s and Turkle’s work identifies an important element, which has also been implicit in the previous section. Mastery involves technical knowledge, revealing the assumption that a hack involves engagement with technology. We can take a core component of hacking to be not only producing many differences but producing these differences through engagement with some form of technology. We have seen