Editorial: Hacktivism

By Paul A. Taylor

Given increasing computer prevalence and the fact our political opponents are among the most wired in the world, it is foolish to ignore the computer. Rather, it is important to turn our attention toward the computer, to understand it, and to transform it into an instrument of resistance. For the luddites of the world who resist computers, consider using computers to resist. (Wray 1998: 1)

In Hackers: Crime in the Digital Sublime (Taylor 1999), I explored in detail the culture of computer hacking. One of the major themes of this study was the way in which connotations of the activity have evolved from the mischievous to the criminal. Technological curiosity and high-jinx was associated with the earliest hackers, but after numerous high profile cases of hacking incidents in the media, the present perception of hacking tends to have much more pejorative associations. An ongoing process of boundary formation was shown to lie behind this evolution in perceptions. The growing maturity of the computer industry and its effect upon the wider society meant that the initial tolerance towards the high levels of technological ingenuity and curiosity shown by hackers could no longer be maintained. Activities previously limited to the computer laboratories of MIT now had much wider potential implications and these needed to be circumscribed and controlled.

A brief examination of the various generations of hackers illustrates this change in the leeway given to hackers. We see how, whilst they contributed to the growth of the nascent computer industry, hackers, although maverick, were accepted as a legitimate part of society. More than merely accepted, they were in fact feted as technological pioneers on a new frontier, an image fuelled by the resonant trope of cyberspace as a new Wild West. Things changed dramatically for hackers, however, when the electronic equivalent of the Wild West became increasingly settled with a concomitant reduction in the space available for mavericks. The rising tide of “malicious hackers” or crackers can be viewed in terms of an active response to this increasingly marginal status. The acceptable bounds within which technological curiosity could be explored became an area of contestation for those seeking to maintain what was perceived to be the original hacker ethic (see below) and those striving to create new norms and ethics for the new informational environments created by the widespread dissemination of computers.

The nadir or “civilising” of the hacker ethic (depending upon your point of view) was documented in Douglas Coupland’s (1995)”factional” account of its apparent suffocation under the stock options and corporate lifestyle of Microsoft: hackers were replaced by microserfs. Resistance to this process, however, is evident from the rise of a new computer subculture: hacktivists. This group emerged in the mid-1990s to combine the technological curiosity of the original hacker ethic with a new political ethos. The tendency of hackers to focus upon technological systems has been re-engineered to include the political and social concerns surrounding global capitalism. Hacktivism thus simultaneously promises to return us to aspects of the original hacker ethic of the early hackers whilst also adding a significantly new and corrective political ethos to the predominantly technologically-focused culture of hacking.
Generations of Hackers

Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!

All information should be free.
Mistrust Authority – Promote Decentralisation

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.
Computers can change your life for the better.
(Levy 1984: 40-45)

The above manifesto is Levy’s description of the original hacker ethic which he describes as existing in its purest or least contested form in the following three main generations of hackers:
1. "True" hackers: these were the pioneering computer aficionados of the earliest days of computing who experimented with the capabilities of the large mainframe computers at such US universities as MIT during the 1950s and 1960s.
2. Hardware hackers: these were the computer innovators who, beginning in the 1970s, played a key role in the personal computing revolution which served to widely disseminate and dramatically decentralise computing hardware.
3. Game hackers: in the 1980s these were the creators of popular gaming software applications for the hardware developed by the previous generation.

To the initial hacker generations identified by Levy, can be added the following three:
4. Hacker/Cracker: from the mid 1980s to the present day both these terms are used to describe a person who illicitly breaks into other peoples’ computer systems. Hacker tends to be used by those within the computer underground or largely sympathetic to its values, whilst cracker tends to be used by those who oppose it.
5. Microserfs: in Douglas Coupland’s novel (1995) this is the phrase used to describe those programmers who whilst exhibiting various aspects of the hacker subculture nevertheless became co-opted into the corporate structure of Microsoft.
6. Hacktivists: the mid-1990s marked the merging of hacking activity with an overt political stance.

Generations 4 and 5 mark a significant evolution in the notion of the hacker ethic. From the 1980s onwards, various interested parties took part in a process of stigmatisation which labelled hackers as deviants and therefore unethical. In Hackers: Crime in the Digital Sublime (1999) I argue at length that such increasingly pejorative judgements were essentially contestable: to a large extent, the act of hacking had become classed as unethical not because the activity itself had substantially changed, but rather because of changes in the prevailing social climate. Despite such caveats, even those within the computer underground were sensitive to potential losses in the original hacker ethic. The widespread dissemination of computing equipment and the media’s sensationalisation of hacking led to: a loss of the early pioneer spirit; less concern with the need to safeguard the free status of information; more concern with gaining access to computing time or facilities; and an increased incidence in the number of destructive hacking incidents.

The overall effect of these factors meant that it became much harder to situate the fourth generation of the computer underground within an outward-looking hacker ethic of benign technological curiosity with its potential for social empowerment. The rise in the number of hackers and their coincidence with the broader political trends of Reaganism and Thatcherism led commentators such as Ross to bemoan their lack of oppositional ethical ethos to the extent that: “teenage hackers resemble an alienated shopping culture deprived of purchasing opportunities more than a terrorist network.” (Ross 1991:90) Corporate-friendly characteristics of hacker culture as “high productivity, maverick forms of creative work energy, and an obsessive
identification with online endurance (and endorphin highs)” [ibid: 90], were so successfully co-opted that they merely served to valorise “the entrepreneurial codes of silicon futurism.” (Ibid: 90) The key significance of hacktivism is the way in which it marks a retreat from such a pervasive intrusion of commodified values into the hacker ethic and a concomitant reassertion of more countercultural values.

Common Ground Between Hackers & Hacktivists

Wandering around the labyrinth of laboratories and storerooms, searching for the secrets of telephone switching in machine rooms, tracing paths of wires or relays in subterranean steam tunnels ... for some it was common behavior, and there was no need to justify the impulse, when confronted with a closed door with an unbearably intriguing noise behind it, to open the door uninvited. And then, if there was no one to physically bar access to whatever was making that intriguing noise, to touch the machine, start flicking switches and noting responses, and eventually to loosen a screw, unhook a template, jiggle some diodes and tweak a few connections ... things had meaning only if you found out how they worked. And how would you go about that if not by getting your hands on them? (Levy 1984: 17)

Whatever, the contestable differences between hacking and hacktivism may be, the two activities share the same fundamental characteristic of technological ingenuity. There are two key aspects to this ingenuity. Firstly, a major element of the hacker aesthetic is the deliberate re-appropriation of the original purposes of any technology. Secondly, the ubiquitous nature of this urge to re-appropriate encourages the hacker to look beyond the specific qualities of individual technologies and in turn to be manipulated and played with. It is this second aspect of the hacker ethic that hacktivism has most significantly adapted in order to facilitate its global political focus. We have seen earlier how curiosity was the key shared feature of the early hacker generations. From the beginning, however, such curiosity was inherently ambivalent. On the one hand, it was inextricably linked to a craving for access to technology in a physical form: curiosity did not remain isolated on an abstract intellectual plane, opportunities to exercise the hands-on imperative were highly valued. On the other hand, the “true” hacker combined, at times, in addition to the specific physical qualities of a particular technological artefact, an almost obsessive interest in the technological complexity of both abstract systems. This combination of interest in both abstract complexity and the physical manifestations of such complexity illustrates a key element of the hacking ethos that in recent times has tended to be overlooked: lost in the minutiae of the most important hacker artefact to date, the computer.

R., a Dutch hacker, expands upon the heterogeneous nature of hacking by arguing that the phrase should not:

Only pertain to computers but 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, 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. (cited in Taylor 1999: 16)

Although undoubtedly the most important hacker artefact to date, the computer is thus just one technological embodiment of a wider hacker commitment to the manipulation of technology in both general and specific forms. Hacking’s innate intellectual brand of explorative curiosity ultimately constitutes a craving to understand systems in both their abstract and grounded forms. Levy (1984) describes how a particular early MIT hacker, Peter Samson, embodied both forms of curiosity. His technological curiosity was effectively interchangeable between such vastly different scales as the labyrinth of MIT’s rooms and corridors and the bird’s nest of electrical wires underneath the layout table of its Tech Model Railroad Club where:
Underneath this layout was a more massive matrix of wires and relays and crossbar switches than Peter Samson had ever dreamed existed. There were neat regimental lines of switches, and achingly regular rows of dull bronze relays, and a long, rambling tangle of red, blue, and yellow wires – twisting and twirling like a rainbow-coloured explosion of Einstein's hair. It was an incredibly complicated system...

(Levy 1984: 21)

Historically, the desire to understand technology's systemic qualities has meant that the curiosity of hackers has been targeted at not only an eclectic range of physical artefacts but also social structures such as the legal system:

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 to 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.


It is this flexibility of expertise for both specific technologies and the general systems that incorporate them which forms the basis of hacktivism's novel approach to the problems of conducting political opposition to an economic and social system that works upon abstract imperatives, but which has very real effects. The apparently complete dependence of contemporary national governments and global capitalism upon complex communication networks has created room for a more deliberately focused political agenda to be added to the pro-systems but anti-authoritarian tendencies that have always existed within hacking. The huge recent growth in the number of such systems of communication networks has simultaneously increased the global commodification process and its vulnerability to dissenting forces.

Early hacker politics

These were the radical or guerilla hackers, who were destined to give the computer a dramatically new image and a political orientation it could never have gained from Big Blue [IBM] or any of its vassals in the mainstream of the industry. At their hands, information technology would make its closest approach to becoming an instrument of democratic politics.

(Roszak 1986: 138)

The political motivations of hacking were identifiable to varying degrees in the earlier generations but tended to be diluted by the more immediate and pressing concerns hackers had with first and foremost obtaining access to systems with a complexity commensurate with their technical knowledge. In an era of what Roszak calls “electronic populism,” hackers were both instrumental and inspirational figures. It can be seen from the ethical manifesto of the first generation of hackers cited above that a key issue of concern for the early hackers was the question of unlimited access to computing power and information. For the first and second generations, both the desire to hack, and the attempt to make technology more democratic and therefore accessible, were complementary facets of the hacker agenda. In the context of the radical US politics of the 1960s and 1970s, rather than opposing the ill-defined system, hackers were more pragmatically involved in promoting more widespread access to the computer systems behind the mega-system.

The political significance of this alliance between technological knowledge and evangelical leanings became more apparent when in May 1971, Abbie Hoffman played a leading role in the establishment of an underground newsletter entitled the Youth International Party Line (YIPL). In September 1973 YIPL changed its name to the Technological American Party (TAP) and its newsletters provided a raft of detailed technical information predominantly about how to phone-phreak (obtain free phone calls through the technical manipulation of the phone system) but in keeping with the previously cited heterogeneous conception of hacking, the newsletter also provided hacking information on a range of artefacts including burglar alarms, lock-picking, pirate radio and how to illegally alter gas and electric meters. TAP ceased publication in 1984, but its mantle was taken up in the same year with the launch of the
phone phreak/hacker magazine 2600 whose anti-Big Brother government bent was immediately indicated by the editor’s choice of the pseudonym Emmanuel Goldstein (the name of the protagonist of George Orwell’s 1984). At a similar time in Europe (1981) a German hacker group called the Chaos Computer Club (CCC) was established which sought to directly address the political implications of the original hacker ethic: “All information wants to be free”. Finally, in the 1980s aftermath of the Chernobyl nuclear accident, the CCC were active in the dissemination of alternative information about the severity of the incident and worked with the German Green Party in a joint evaluation of the Federal parliament’s introduction of new computer systems.

**Beating The System: Sixth generation hacktivists and the rise of online political protest**

Virtual politics ... should be founded on defying the neoliberal discourse of technology currently being fashioned by the virtual class. It is crucial to ensure that the political genealogy of technology, of virtual reality, of the reality of virtuality, is uncovered by numerous individuals, groups, classes, and new social movements. Indeed, without such excavations, the increasingly institutionalised neoliberal discourse of technology currently being promoted by the virtual class will rapidly become a source of immense social power. This is why concrete, corporeal, and ideological struggles over the nature and meaning of technology are so important in the realm of virtual politics ... It is time, then, to radically rethink, redefine and reinterpret the very meaning of technology, politics, and cybertulture in the age of the virtual class. (Armitage 2000: 1 & 4)

Hacktivism has built upon the nascent political agenda of hacking, and arisen in the context of an intellectual climate increasingly sensitive to the effects of globalisation. This sixth generation of hackers has arisen as a result of the convergence of two different trends: a) hackers have become more politically aware and b) activists have become more technologically knowledgeable. These two trends are reflected in the following two main types of hacktivist protest:

**a) Web hacks and computer break-ins**

Conventional hacking techniques are increasingly being applied to political targets whilst maintaining the sense of humorous mischief frequently associated with the computer underground. Thus in 1996 the Web site pre-election manifesto of the British Labour Party was altered from “The Road to the Manifesto” to “The Road to Nowhere” whilst in the US the Central Intelligence Agency’s Web site was changed so that it read “Central Stupidity Agency.” The hacker group Cult of the Dead Cow (CDC) have sought to combine a humorous with a hardened attitude to corporate power on the Net. Their various versions of the software package entitled “Back Orifice” targets computers attached to Microsoft Windows network systems and allows the software’s user to access the private files and emails of the Microsoft user. Back Orifice has been downloaded 128,776 times since late February 2000 and the CDC argue that it draws attention to the surveillance capabilities written into Microsoft software which allows system administrators access to the private information of users.

**b) Electronic Civil Disobedience**

Traditional forms of civil disobedience such as peaceful sit-ins have been replicated in cyberspace to create new forms of electronic civil disobedience. In 1998, for example, the hacktivist group the Electronic Disturbance Theatre coordinated a series of Web sit-ins in support of the Mexican anti-government group, the Zapatistas. This incident was perhaps most noticeable for its use of an automated piece of software revealingly called Flood Net. The Flood Net software once downloaded on to an individual’s computer automatically connects the surfer to a pre-selected Web site, and every seven seconds the selected site’s reload button is automatically activated by the software. If thousands of people use Flood Net on the same day, the combined effect of such a large number of activists will disrupt the operations of a particular site.
The most significant aspect of these two activities is the way in which they seek to merge hacking’s sophisticated knowledge of individual technological systems with a broader understanding of their overarching political systems. In so far as the advent of widespread computing has given rise to an increasingly hyperreal social environment, hacktivism offers at least some sort of provisional guidelines for simultaneous engagement with both social and technological systems that have ever-increasingly abstract forms.

**The Dot.communist manifesto and the unbearable lightness of being**

Constant revolutionizing of production, uninterrupted disturbance of all social relations, everlasting uncertainty and agitation, distinguish the bourgeois epoch from all earlier times. All fixed, fast-frozen relationships, with their train of venerable ideas and opinions, are swept away, all new-formed ones become obsolete before they can ossify. All that is solid melts into air, all that is holy is profaned. (Marx/Engels 1971: 39)

FBI detectives have launched an investigation in the US after a British couple who paid almost £5,000 for a Rolex watch in an Internet auction received just a photograph of the item in the post. (The Guardian 15.02.2001)

In *The Republic*, Plato compared mankind’s search for philosophical truth to the condition of prisoners chained together in a cave with their backs to the entrance and only able to see shadows of the world outside being reflected onto the back of the cave wall. Plato’s metaphorical description also encapsulates the increasingly ethereal nature of contemporary capitalism where our direct experience of the physical world is increasingly mediated and distorted by media images and abstract commodity forms. In the anti-capitalist bestseller *No Logo*, Naomi Klein describes this process as a corporate “race towards weightlessness” where the aim of companies has become “divestment of the world of things.” (Klein 2001:4) The perennial pertinence of Marx’s above poetically charged analysis of capitalism’s ever-increasing levels of abstract, yet socially transformative power, is illustrated by the way in which it has been enthusiastically re-appropriated by business gurus. The hyperbolic tone of their work makes Marx’s language seem relatively understated to the extent that it has been described as the “deranged optimism” and “corporate salivating” of “business pornography,” and which is illustrated in the spate of such recently evocative business titles as: *Living on Thin Air; The Empty Raincoat; Being Digital; and The Weightless World*.

Despite this rhetoric of immateriality there are various points at which refractory reality reasserts its influence and serves as a brake upon capitalism’s limitless expansion. The Reclaim the Streets movement, for example, brings (as its name implies) its particular brand of anti-capitalist opposition into the streets most to emphasize directly the enervating effects of urban traffic upon community life. The account below also neatly illustrates how even the vanguard of the E-economy can not totally insulate themselves from the practical consequences of their virtual activities:

*Dotcom entrepreneurs in San Francisco are being forced to hire 24-hour security guards after a spate of arson and graffiti attacks on their plush high-tech offices and the systematic vandalism of employee's expensive cars ... The uprising against “dot-commies” ... is led by two protest groups, the Yuppie Eradication Project and AARGG! (All Against Ruthless Greedy Gentrification) Many are the same dissidents who disrupted the World Trade Organisation meeting in Seattle last year ... Protesters are angry that premises used by non-profit arts groups are being taken over ... San Francisco's large artists' community has formed Art Strikes Back to fight a rearguard action. Every day, groups of artists block pavements outside dotcom companies to sneer at employees. The current wheeze is to flit around like ants while talking into plastic mobile phones about selling stock options, 20-hour work days and caffe lattes. Even the city's down-and-outs are adding to the conflict with their signs reading: www.sparechange? (The Daily Telegraph Oct 7th 2000 [Davis 2000:22])

Hacktivism’s potential fruitfulness as an oppositional strategy to global capitalism resides in not just its explicit recognition of capitalism’s innately decontextualising and abstracting tendencies, but its
willingness to create an oppositional strategy that utilises activities based not only within global computer networks but also on the streets.

**Hacktivism hits the streets**

Technical culture has gotten out of hand. The advances of science are so deeply radical, so disturbing, upsetting and revolutionary, that they can no longer be contained. They are surging into culture at large; they are invasive; they are everywhere. The traditional power structure, the traditional institutions have lost control of the pace of change … And now that technology has reached fever pitch, *its influence has slipped control and reached street level* … times have changed since … Science was safely enshrined - and confined - in an ivory tower. The careless technophilia of those days belongs to a vanished sluggish era, when authority still had a comfortable margin of control. (Sterling 1986:x & xi [emphasis mine])

Cyberpunk fiction, which gave us the now working concept of cyberspace, uses “the street” as a compensatory trope with which to represent the vibrant and at times uncontrollable energy of the physical world’s commercial activity. Such depictions of the street provide a febrile and gritty flip-side to the abstract informational activity of the global information networks that underpin capitalism:

> Get just wasted enough, find yourself in some desperate but strangely arbitrary kind of trouble, and it was possible to see Ninsei as a field of data … Then you could throw yourself into a highspeed drift and skid, totally engaged but set apart from it all, and all around you the dance of biz, information interacting, data made flesh in the mazes of the black market … . (Gibson 1984:26)

In *Nymphomation*, Celia is a street-urchin whose genetically-based lucky winning streak threatens the corporate power of the ominously named “Company” that runs the lottery competition that has become a society-wide obsession for a dystopian future England, whilst another character, Jaz, opines: “I think learning sucks … I just want to be in business, that’s all. Away from my father’s clutches. I just want to sell some bad-arse gadgets on the filthy streets.” (Noon 1997: 15) The “street” not only provides a source of practical opposition to capitalist values, it also represents a fictional trope for the unpredictable and potentially uncontrollable nature of new technological developments. Within cyberpunk fiction it is seen as the source of an unpredictable and ambivalent energy that both promises a source of opposition to the global capitalist order, but also an important reservoir of entrepreneurial energy.

Cyberpunk’s identification of exhilarating energy in both the matrix and the street is mirrored in the dual strategy adopted within hacktivism whereby its oppositional activity works at both material and immaterial levels. A good example of this dual strategy is provided by the practice of culture jamming which combines the manipulation of semiotic codes with physical changes to capitalist products. Thus, the Barbie Liberation Organisation switched the voice boxes of GI Joe and Barbie dolls and groups such as Adbusters use techniques such as “billboard banditry” to make small but crucial changes to corporate adverts that creates a process of “subvertising.” After the Exxon Valdez disaster, for example, the San Francisco-based Billboard Liberation Front subverted a radio promotion poster so that instead of “Hits Happen. New X-100” it read “Shit Happens — New Exxon”. The broadly-defined concept of culture jamming parallels the broad interpretation of hacking as being a mindset applicable to a heterogeneous range of artefacts, it adopts hacktivism’s technique (in turn copied from the original hacker ethic) of reverse-engineering the intended outcomes of a particular system. Culture jamming turns the original purpose of a cultural artefact back on itself to create the opposite outcome to the one originally intended.

**Conclusion**

The huge recent growth in the number of communication networks has simultaneously increased the global commodification process and its vulnerability to dissenting forces. The erosion of the original hacker ethic arguably occurred because the early generations of hackers were more interested in the intellectual thrills that access to computer systems could afford, rather than the potential such access contained for oppositional political purposes. The apparently complete dependence of contemporary national governments and global capitalism upon such complex communication networks, however, has
created room for a more deliberately focused political agenda to be added to the anti-authoritarian, but pro-system attitudes that have always existed within hacking.

Whatever the philosophical and practical differences may be between hacking and hacktivism, the key significance of hacktivism is the way in which it has produced a political strategy that is faithful to the combination of hacking’s previously identified love of abstract systems as well as its commitment to the reappropriation and subversion of the original purposes of specific technological artefacts. It remains to be seen whether hacktivism can successfully confront capitalism’s pervasive yet increasingly immaterially networked nature, but its willingness to use both abstract and grounded political techniques offers a potentially innovative political strategy that remains true to hacking’s original penchant for understanding and manipulating systems, it merely concentrates upon the uber-system: global capitalism.

Paul A. Taylor is the author of *Hackers: Crime in the Digital Sublime*. He is Lecturer in the Sociology of Technology at University of Salford, UK. His area of research is in politics and culture of the information age.

**Notes**

1. Pekka Himanen’s (2001) update of the hacker ethic identifies three main components: a) The Work Ethic: a revitalisation of the Protestant work ethic where hackers demonstrate a marked level of passion for their work; b) The Money Ethic: a commitment to work that is valuable because it is recognised as such by one’s peers rather than any remuneration one may receive for it; c) The Nethic: the importance of promoting access to information and computing resources.

**References**


Petersen, J. aka Agent Steal (1997) “Everything a hacker needs to know about getting busted by the feds.” Available at: http://www.grayarea.com/agsteal.html

