Rebels for the System?
Virus writers, general intellect, cyberpunk and criminal capitalism.

Mathieu O'Neil
ACSPRI Centre for Social Research
Research School of Social Sciences
The Australian National University

Continuum: Journal of Media & Cultural Studies 20(2): 225-241.

In recent years there have been numerous reports of attacks against computer systems around the world by viruses created by ‘computer hackers’. It is asserted in the media that the time and energy required to assess and repair the damage caused by this malicious software, sometimes known as ‘malware’, is proving increasingly costly to corporations. The seriousness of the threat posed by rogue computer programmers to the economic system seems to be borne out by actions such as that undertaken by Microsoft in November 2003, when it offered a bounty of $250,000 for information leading to the capture of the authors of the Sobig virus and MSBlast.A worm. In our networked world, nothing, it seems, could be more disruptive than the break-up of the global flows of data resulting from this electronic sabotage. ‘Hackers’ are commonly divided into law-abiding and lawbreaking programmers. This article aims to question whether the distinction is justified, in the context of globalised capitalism. However, for clarity’s sake, the terms ‘virus writers’ or ‘computer intruders’ will be used when referring to lawbreaking individuals and groups, and ‘legitimate hackers’ when referring to law-abiding individuals and groups. Yet since all of these individuals and groups share a commitment to autonomy, for example the freedom to access information without restrictions, the term ‘hacker’ will be used when referring indiscriminately to those people who engage in ‘hacking’, the unauthorized or uncontrolled use of computers.

Contemporary capitalism’s cycles of production and consumption are fuelled by the development of information and communication technology (ICT). Technoscientific progress depends on cooperatively produced knowledge, which Marx called ‘general intellect’. It would be tempting to portray hackers – highly specialized knowledge workers who rebel against state and corporate authority – as a progressive general intellect, opposed to the economic and social order. This reading would mesh nicely with an understanding, popular amongst contemporary intellectuals, of legitimate hackers as a positive social force, who have been unfairly lumped together with computer vandals in order to disqualify threats to the dominant system, such as free software. My own understanding of hackers, however, is quite different. I do not mean to imply that individual hackers do not feel that they are genuinely resisting dominant norms and values; but I am interested in defining how the economic and social order can accommodate, and, perhaps, coopt this resistance. I start with the premise that hacking is indeed a gesture of defiance. Popular perceptions of hackers as ‘rebels’ have been shaped by many sources, but few have proven as influential as William Gibson’s 1980s cyberpunk fiction. Reviewing cyberpunk’s economic positioning of hackers – how Gibson’s ‘computer cowboys’ fit into the labour market – will inform a reassessment of the socio-economic impact of real-world virus writers and hackers in globalised capitalism.

Freeware and Malware

Though hacker culture originated in the United States, the development of the Internet has allowed it to spread worldwide. Originally, a ‘hack’ meant a creative solution to an interesting problem and ‘to hack’ was simply to write code. The shared culture of expert programmers and networking wizards traces its history through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments: ‘Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work’ (Raymond, 1986). The search for knowledge that lies at the root of hacking, both legitimate and criminal, can be traced to a common source. All hackers show, from an early age, a great interest for material objects, an interest which expresses itself through the desire to dismantle these objects, to see through them in order to understand how they function (Breton, 2000, p. 62). Levy (1984, pp. 27-31) defined the ‘hacker ethic’ as the commitment to the free access of computers and information, the mistrust of centralized authority and the insistence that hackers be evaluated solely in terms of technical virtuosity and not ‘bogus’ criteria such as degrees, age, race or position. Turkle (1984, p. 232) writes that a good hack must be simple, technically masterful and illicit, in the sense of being against a legal, institutional or customary rule. The principal rule of capital is private property. Richard Stallman, embodying the hacker ethic, famously stated: ‘I consider that the golden rule requires that if I like a program I must share it with other people who like it. (…) I have decided to put together a sufficient body of free software so that I will be able to get along without any software that is not free’ (Stallman, 1985). Stallman went on to launch the General Public License (GPL, sometimes known as ‘copyleft’) a legally binding license which prevents free software from becoming proprietary, as well as the Free Software Foundation, to aid in the diffusion of his ideas, practices, and code. His GNU software system eventually led to the creation of Linux, the well-known non-proprietary computer operating system. Another significant achievement of legitimate hackers is the dissemination of peer-to-peer (P2P) computing, a decentralized system where computers communicate directly with each other. Popular sectors of P2P are distributed processing, and especially file sharing: for example, software applications such as the banned Napster or Kazaa allow users to communicate synchronously, searching each other's computers for files. It is sometimes asserted that P2P represents a democratizing force, where ‘end users are no longer second-class citizens’ (Kan, 2001) and can venture into what was once the exclusive domain of highly trained systems administrators. Free software and P2P could both be described as technical-legal viruses which attack the dominant proprietary system.

In this legitimate hacker universe, symbolic capital is earned by producing free code, by testing the code of others to improve it, and by contributing to the maintenance of the community's institutions, such as Internet bulletin boards and newsgroups. Status and prestige are produced wholly within the community, and conversely any form of discipline or regulation from without is viewed with suspicion. Not surprisingly, anarchistic or Libertarian ideas are widespread amongst hackers. Eric Raymond writes that aspiring hackers should develop an instinctive hostility to censorship, secrecy, and the use of force or deception to compel responsible adults. They should also be willing to ‘act on that belief’ (Raymond, 1986). This attachment to individual autonomy explains why, even though legitimate hackers are often at pains to distinguish themselves from computer intruders and virus writers, the boundary separating both groups is not hermetically sealed.

Moreover, in terms of the hacker ideal of freedom of movement and access, computer viruses and worms are the best possible kind of programs: they are created to travel freely, despite the barriers which may have been set up to restrict their dissemination. A computer virus is a program which replicates and disseminates itself over networks in order to alter other programs and operating systems. Worms (sometimes called ‘autonomous attack agents’) are a type of program, which, unlike viruses, do not require human agency to infect computers and propagate themselves. John von Neumann developed the theory of self-reproducing automata in 1949, and several self-replicating programs were produced in the 1970s and 1980s, but it was not until 1984 that the viral analogy was introduced by Fred Cohen, whose paper ‘Computer Viruses - Theory and Experiments’ attracted international attention (Cohen, 1987). An example of the serious academic tone in which programmers describe worm development was posted on the Internet in 2001:

> There are almost no published works dealing with virus techniques on the Unix platform. (…) Subversive dynamic linking provides a mechanism for greatly expanding the capabilities of the Unix parasite, freeing developers from many of their previous constraints. [In conclusion] we have demonstrated (…) how a reliable mechanism of utilizing libraries greatly enhances parasite functionality. (…) This method is legitimate and portable. Thus, the threat of under-featured parasites has been ended forever. (The grugq, 2001a)

By publishing descriptions of their work on the Internet in this manner, rather than releasing it directly, ‘malware’ authors can absolve themselves of the responsibility for the damage it may cause when some less experienced programmer appropriates it, claiming it as his. As a result of a pseudo-Darwinian ‘survival of the fittest’ where only the stealthiest variants survive, reproduce, and further mutate, viruses and worms have become increasingly effective. In February 2003, the Slammer worm infected 75,000 servers (90% of connected vulnerable machines) in ten minutes. Most of Bank of America’s 13.000 ATM machines could not function for part of the day, flight delays and cancellations occurred at Houston’s Continental Airlines after its online ticketing system was overwhelmed, and various media outlets (such as the *Atlanta Journal-Constitution*, the *Associated Press* and the *Philadelphia Inquirer*) experienced publishing problems as a result of the worm (Krebs, 2003). The Sobig.F virus, which struck in August 2003, infected millions of computers and caused over 300 million infected emails to be sent during its first week of activity. In January 2004, the Mydoom virus overtook Sobig.F as the largest virus outbreak ever, flooding the internet with 100 million infected emails in its first 36 hours (AFP, 2004). The authors, groups of programmers known as the VX scene, are structured around a strong elitist sensibility, well-known figures (‘sceners’), and language (the ‘code’), which are closed to outsiders and beginners: to be included, a degree of skill and expertise must be demonstrated. In a text written to acompany the *iloveyou* ‘virus art’ exhibition, Massimo Ferronato writes that the products of the scene are seen as a manifestation of creative brainwork, a ‘replicant mural (...) that sends out a message about the accomplishments of its inventor’ (Ferronato, 2004). Members of the scene are prone to describing their activities as creative or artistic. A *New York Times* report on the ‘Virus Underground’ asserts that for programmers replicating an existing virus is ‘lame’, the worst of all possible insults. ‘To allow his malware to travel swiftly online, the virus writer must keep its code short and efficient, like a poet elegantly packing as much creativity as possible into the tight format of a sonnet’ (Thompson, 2004, p. 28). Other commentators, however, declare that there are two primary motives for virus writers: malice and ‘masturbatory gratification’ (Lowe, 2004, p. 16).

Do viruses solely express the antisocial and destructive tendencies of their authors? MyDoom was programmed to attack the website of SCO, a Utah-based company, which appears to have antagonized the hacker community because it holds the copyright to the UNIX program and considers that elements of Linux constitute an infringement of this license. Blaster/Lovsan, which appeared on August 12, 2003, exploited a security fault in the Windows operating system and secretly attempted to transmit itself to other machines. It would then restart the machine every sixty seconds, preventing users from downloading an antivirus program or a ‘patch’ to fix the system. Blaster’s ultimate purpose was to launch a ‘denial of service’ attack on a Microsoft website. All the infected computers were to attempt to connect to it at the same time, thereby provoking an electronic traffic jam and forcing Microsoft’s server to crash. The attack was programmed for Friday 16 August but was unsuccessful, as Microsoft’s engineers managed to crack Blaster’s code and close down the targeted site before the start of the attack (Foucart, 2003, p. 23). In this instance, the programmers responsible for the scheme would probably say that, as in the biological context, where the genetic diversity of a population protects it against extinction through viral infections, computer networks are mainly rendered susceptible to viruses by the monocultural character of the software environment. Presumably, they would also argue that they were seeking retribution from a company which had achieved its near-monopoly status by systematically breaking the hackers’ own code of conduct and withholding information (the source code of its Windows operating system is Microsoft’s most treasured secret).

The concept of general intellect is useful in helping us to understand the role hackers play in society. Karl Marx used the term to refer to the abstract knowledge or collective intelligence of a society at a given historical period which becomes embodied in ‘fixed capital’ such as technology: ‘The development of fixed capital indicates to what degree general social knowledge has become a direct force of production’ (Marx, 1973, p. 706). Marx believed that general intellect, which increasingly propels production forward, would ultimately help to destroy capitalism. He advanced two main reasons: first, mechanization would lessen the need for people to sell their labor power and hence undermine the basis of the social order. Second, because of the increasingly cooperative nature of work required for technoscientific advancement, ‘both private ownership and payment for isolated quanta of work-time (would) appear increasingly as irrelevant impediments to the full use of social resources' (Dyer-Witheford, 1999, p. 220). As we know, far from leading to socialism, the advent of a network society has allowed capitalism to consolidate its global reach. However general intellect has been reinterpreted by theoreticians associated with the *Futur Antérieur* journal as a 'labour of networks and communicative discourse' (Vincent, 1993, p. 127). They describe its subjective component, 'mass intellectuality', as the system of social competencies which support the operation of a high-tech economy. Since this economy is based on information and communication, it manifests itself not only in the productive process but also through a whole range of educational and cultural relations (Virno, 1996, p. 268). An important question then arises, namely to what extent capital can contain what Vincent calls this 'plural, multiform, constantly mutating intelligence'? He notes that capital 'appears to domesticate mass intellect without too much difficulty' (Vincent 1993, p. 121), but only through the strict application of intellectual property rights. Dyer-Witheford (1999, p. 228) perceives in the global exchanges of the network, despite all the 'banalities and exclusivities of Internet practice', glimpses of 'what seems like the formation of a polycentric, communicatively connected, collective intelligence'. In this scenario, legitimate and criminal hackers would feature as the complementary lobes of a counter-hegemonic brain, some lashing out directly against transnational corporations, others constructively building an alternative to proprietary practices. Could this be the germ of the dissident mass intellectuality that will, according to Negri (1994, p. 89), reappropriate the organizational and technological knowledge necessary to run society? Before addressing this question, I propose to analyse the genesis of the hacker's rebellious image, and how this image compares with reality.

Romancing the Virus

In early 2003, an Australian computer magazine published an article about 'polymorph' viruses. The anonymous author stated that simply disinfecting such 'hybrid' or 'blended threats' does not always prove effective, as they lie dormant but provide an entryway for future malware. And she added: 'Like something from the cyberpunk world of William Gibson's *Neuromancer*, in an attempt to evade detection by antivirus software, these shapeshifters mutate each time they infect a PC' (Anonymous, 2003, p. 86). This is but one example among many, as the term 'cyberpunk' has come to signify in shorthand any kind of relationship to technology which is idiosyncratic and non-corporate. Gibson's impact is perceptible in references to cyberpunk in technology-oriented journals and websites as well as in such texts as Salam Pax's *Bagdhad Blog*, an online account of the US-led invasion of Irak in 2003, since published as a book. Pax writes that a Bagdhad street market where cheap RAM, broken monitors, Falafel stands and weapons are being sold 'looks like something out of a William Gibson novel' (2003, p. 166). Twenty years after their publication, *Neuromancer* (1984) and its sequels *Count Zero* (1986) and *Mona Lisa Overdrive* (1988) thus still serve as the reference point for discussions of hacking and viruses. In these novels, an elite cadre of 'console jockeys' use 'icebreakers' (virus/penetration programs) to conduct 'runs' against data fortresses protected by deadly 'black ice' (antivirus programs).

In what Gibson initially called the ‘Matrix’ hackers make deals with, and attempt to understand, sentient programs, which are portrayed in the guise of Haitian Voodoo deities. The corollary to this linking of spirits and machines is the disparagement of the body. The trilogy begins with the hacker antihero Case’s attempt to steal data from his employers. In revenge, they damage his nervous system, destroying his ability to hack and expelling him from the bodiless exultation of cyberspace: ‘the elite stance involved a certain relaxed contempt for the flesh. The body was meat. Case fell into the prison of his own flesh’ (Gibson, 1984, p. 6). Cyberpunk’s integration of technology and punk rock, high-tech and lowlife, and hallucination and reality, transformed the programmer as antisocial ‘nerd’ into the programmer as antisocial ‘cowboy’, who was as adept at hacking code as at making dangerous street deals. This new identity was symbolized by frequent references to cranial jacks, black leather jeans, mirrorshades and amphetamine addiction; today the image persists in such mass cultural products as Hollywood’s *Matrix* trilogy, where protagonists in search of the meaning of cyberspace jack in and out of a virtual universe featuring anthropomorphized virus programs.[1]

However, unlike their Hollywood imitators, Gibson’s hackers’ neo-Arthurian quest for the ‘shape’ or meaning of the ‘Matrix’ and of the artificial beings which inhabit it is entwined with a clear understanding of capitalist business practices. The activities of real-life hackers, with their championing of a non-financially motivated code of conduct, may appear somewhat disconnected from economic necessity. Gibson’s fiction restores the logic of the marketplace; his characters never lose sight of the primary objective of earning a living. An illustration of the manner in which his ‘computer cowboys’ pursue this goal can be found in *Count Zero*. A minor character, ‘The Wig’, realizes that the life-span of silicon chips far exceeds that of computer production cycles. Still functioning but obsolete machines are going into any number of ‘very poor places struggling along with nascent industrial bases. Nations so benighted that the concept of nation was still taken seriously’. Using his skills and knowledge, The Wig pillages several million tiny bank accounts for a week, ‘incidentally bringing about the collapse of at least three governments and causing untold human suffering’, then retires (Gibson, 1986, p. 121). In contrast, the principal narratives of the trilogy follow a caper movie formula where a team of hackers and mercenaries is recruited to perform a heist. In *Neuromancer*, the employer of the cowboy Case is an autonomous AI, itself the creation of the Tessier-Ashpool Corporation. The main programmer protagonist in the second instalment of the trilogy is *Count Zero*, a teenage hacker wannabe, while the professional computer and violence specialists are the disposable employees of Hosaka, Maas Biolabs, and Virek, giant conglomerates who hire them to ‘exfiltrate’ engineering specialists (to kidnap them from their fortified research centres). The techniques employed by these organisations, whose power seems unlimited, can only be described as criminal or terrorist. The trilogy is concluded by *Mona Lisa Overdrive* with some of the characters disappearing into cyberspace, while the physical world is left in the care

[1] *Matrix Reloaded* is said to be the first major motion picture to accurately portray a malicious hack. When Carrie-Anne Moss’s superhacker Trinity sets her sights on a power grid computer, she is shown correctly running Nmap, a popular freeware port scanner that sends packets to a machine or network to discover what services are running (Poulsen, 2003).

of the corporations/crime syndicates, symbolised by the consecration of a new leader of the British Yakuza. Gibson's fiction thus illustrates precisely the twin dynamic of the Internet's development: on the one hand, a discourse which presents bodiless cyberspace as the last hope of humanity, the only possible utopia, since no chance remains of changing the offline world. On the other, a policy of worldwide deregulation of state assets and laisser-faire economics which puts the unfettered corporate control of networks beyond discussion (see Schiller, 1999). But Gibson takes this process one step further by depicting a world in which, in accordance with Libertarian principles, the centralized control of the state is completely absent; a world where cheerfully asocial programmers serve criminal empires.

Demons and Angels

Are real-life hackers involved in mafia capitalism? At first glance, lawbreaking hackers and organized crime are not so dissimilar. The hacker underground, though its cultural base is less defined, and its internal structure more fluid than that of criminal organisations, nonetheless makes its own rules, distrusts outsiders and is reluctant to expose its innermost workings to the world. The same can be said of the various mafias. Where then could collusion between the two groups occur? For the criminal corporation to prosper, it must be based in a location where state authority has been considerably weakened. When the state cannot guarantee law and order, other modes of regulating market forces step in. In Russia, for example, the collapse of the Soviet Union was followed by the emergence of a kleptocratic system. The absence of effective state regulation and control led to the establishment of a symbiotic relationship between a newly emerging private business sector and its protection/extortion by criminal networks. This crime-penetrated business linked up with politicians at the local, provincial and national level, so that ultimately politics, business, and crime became intertwined (Castells, 1997, p. 190).

At the same time the traditional Russian strength in mathematics at higher education level and the depressed state of the economy were conspiring to produce a large number of potential hackers, or 'khakeri' – sometimes known as 'housebreakers', or 'vzlomshchiki' (Heintz, 2000, p. 1). The primary consequence of this situation can be observed in the field of software piracy. According to the Business Software Alliance, a computer industry watchdog group, Russia and the Ukraine had the highest rate of software piracy in Europe in 2000 (BSA, 2001, p. 3). Russians have also been implicated in several high-profile criminal hacking cases: mathematician Vladimir Levin was caught and sentenced in 1998 to three years' imprisonment in Florida for withdrawing $12 million from a bank's accounts and transferring it to his own. In 2000, unsuccessful Russian Net-entrepreneur Vasily Gorshkov, aged 24, with the help of 19-year-old programmer Alexey Ivanov, started scouring the net for weak links in databases. Once these had been identified, they would steal items of information and contact the system's administrator to demand money in order to 'fix the problem'. Gorshkov and Ivanov also used online payment service PayPal Inc. to turn pilfered credit card numbers into cash by setting up fake accounts (Eunjung Cha, 2003, p. A01).

These few examples aside, the fact that talented hackers and organized crime exist in the same environment does not constitute, in itself, proof of collusion. In the United States, a colorful article in a computer security journal asserted that ‘the mob’ was moving into cyberspace, but failed to provide any evidence, aside from two unreferenced assertions concerning a so-called ‘Israeli Mafia’ (responsible for ‘several homicides’ in Silicon Valley) and the ‘One Eye Jack Gang’ (also based in California) ‘suspected of being behind a multi-million dollar chip scam’ (Bequai, 1997, p. 28). A leading expert in the field of international security studies, writing in an official online journal of the United States State Department, could do little more than offer conjecture: competent programmers can be bribed or coerced to collaborate with criminals; the transnational nature of the Internet makes law enforcement difficult; it also offers great opportunities for fraud and extortion; and it favours anonymity and secrecy. In conclusion: ‘the synergy between organized crime and the Internet is not only very natural, but one that is likely to flourish and develop even further in the future’ (Williams, 2001). Any proof that this is actually happening is less forthcoming in this report, apart from the example of an electronic scam directed by a group of twenty people, ‘some of whom were connected to mafia families’, against the Bank of Sicily in October 2000 (Ibid.).

There are striking similarities between these assertions of a hacker connection to so-called ‘criminal capitalists’ and the oft-repeated statements by government officials that hackers represent a grave threat to National Security. A typical example was the testimony of Jack L. Brock (Director, Defense Information and Financial Management Systems, General Accounting Office) before the U.S. Senate: Brock claimed that ‘the Defense Information Systems Agency estimates that as many as 250,000 attacks against the Department of Defense *may have occurred* last year’ (Brock, 1996; emphasis added). This rhetoric became the official doctrine of the United States when President William J. Clinton declared that ‘terrorist and outlaw states are extending the world’s field of battle, from physical space to cyberspace, from our earth’s vast bodies of water to the complex workings of our own human bodies’ (Clinton, 1999, p. 3486). In contrast, Dorothy Denning notes that ‘there is little concrete evidence of terrorists preparing to use the Internet as a venue for inflicting grave harm’. Most instances of politically-motivated conflicts in cyberspace incidents take the form of defacing, or disrupting, an enemy’s website. The only known incident of hackers attaining a military target occurred during the Kosovo conflict, when the Bosnian Serb news agency SRNA reported that the Serb Black Hand hacker group had deleted all the data on a U.S. Navy computer (Denning, 1999).

A decade earlier, Denning had already pointed out that the world is crisscrossed by many different information and computer networks that are used to deliver essential services and basic necessities - electric power, water, fuel, food, goods. These networks are all accessible publicly and hence vulnerable to attacks, and yet virtually no attacks or disruptions actually occur (Denning, 1990). If that is the case, what are we to make of these repeated warnings that some terrible disaster may be about to happen, with little in the way of corroboration? The inescapable conclusion is that the threat of cyberterrorist or hacker attacks is grossly exaggerated. The mass media’s portrayal of hackers as monsters with incomprehensible motives has been extensively documented by Halbert

(1997) and Nissenbaum (2004). Hackers are constructed as deviants, likened to rapists who penetrate defenceless systems, and this process is validated through public trials (such as the prosecution of super-hacker Kevin Mitnick).

The demonisation of hackers serves several purposes. It represents a means of enforcing social discipline, of defining what is normal behaviour and of legitimizing the government's action (Halbert, 1997, p. 369). This ritual reassertion of the state's essential goodness, as opposed to the evilness of its enemies, is specially useful to justify increases in the resources of security agencies. Bruce Sterling has made an important contribution towards understanding the concerns of private sector security experts, who, when they perform their job well – and nothing untoward happens to their company – run the risk of appearing completely superfluous. Hence the importance of giving the maximum publicity to real or perceived threats. The same reasoning can be applied to associated law enforcement agencies (Sterling, 1992, p. 19). The terrorist attacks of September 11 have amplified this process to a degree that rivals the imagination of William Gibson. The Cyber Security Enhancement Act, part of the Homeland Security Bill of 2002, called for the creation by the government and the private sector of a huge database to identify terrorist threats, and prescribed life sentences for hackers who 'recklessly' endanger lives. The Act strengthens the restrictions on privacy contained in previous legislation such as the Patriot Act, by requiring Internet Service Providers to hand over user records to law enforcement agencies (Hales, 2002). Critics point to this as a further erosion by the US Government of citizens' privacy rights, an earlier example being the FBI's reluctance to allow use of encryption technology which render communications perfectly secure.

Ross (1991) and Helmreich (2000) have noted how the discourse on computer viruses mirrors that dealing with AIDS. Speaking in a biological register allows computer security rhetoric to obscure the historical and cultural specificity of conceptions of bodies, nations and economies (Helmreich, 2000, p. 474). The analogy extends beyond the tropes of sickness and infection to the stigmatization of 'unsafe practices'. The mainstream discourse on computer viruses echoes the moralizing discourse which disapproves of sex with strangers. It upholds the virtues of hygienic safe computing by a 'responsible user' (Parikka, 2005) who, in particular, will only acquire software through reputable dealers, in order to discredit the exchange of copied files. According to Nissenbaum (2004), this is the fundamental cause for the deliberate confusion by the authorities of legitimate hackers with their evil twins, computer intruders and virus writers; and for the characterization of hackers as vicious victimizers of helpless corporations. A new prototype of hackers as untamed and dangerous has been established to discredit the social good which legitimate hackers actually embody: 'If hackers are thieves, vandals and terrorists, it makes no sense to ask whether hacking is good or bad, whether we are for or against it' (Nissenbaum, 2004, p.204). In this view, the hacker ethic, based on the free flow of information and unrestricted access to computer resources, is fundamentally inimical to the commercial use of the Internet. Since memory replication is the basis of computing, hackers have no choice but to battle against the sanctity of property rights, and the self-organized, cooperative and horizontal network of hackers does embody an alternative general intellect, which is not oriented towards the accumulation of financial capital. Indeed, other commentators describe hacking in quasi-revolutionary terms. Pekka Himanen writes that for hackers the purpose of life is found between ‘Friday’, the Protestant ethic which upholds that work is the supreme material and spiritual value, and ‘Sunday’, the pre-Protestant worldview which understood ‘toil’ as a form of punishment. According to Himanen, the hacker ethic blends work and leisure, as it founded on the passionate desire to create (Himanen, 2001). McKenzie Wark asserts that the activities of what he calls the ‘hacker class’, being based on the free manipulation and exchange of inexhaustible digital information, challenge the very basis of the process of accumulation: ‘New hacks supersede old hacks, and devalues them as property’ (Wark, 2004).

Rebels for the System

This vision would form a compelling narrative, if only it were true. It may prove advantageous for states and corporations to disseminate the image of dangerous hackers; dealing with the aftermath of virus attacks may be costly for corporations; but overall, the benefits of rogue programming for capital far outweigh the disadvantages. I will briefly outline some of these benefits, starting with lawbreaking hackers. First, virus writers who exploit faults in systems play the same role that users/testers do in free software projects (Ghosh, 1998; Raymond, 1998) – they compel the system programmers to make their code more efficient. That the testing process is encouraged in one instance and dreaded in another does not change its outcome: an improvement in the system. This is true of sofware such as that produced by Microsoft as of the Internet itself, whose ‘payload’ (carrying capacity) will best be assessed when stretched by intense traffic. After all, the earliest worm was introduced in order to test the performance of large-scale networks; and computer scientists are still working on the building of ‘benign worms’ which will perform similar functions, or be used to fight uncontrolled programs (Qing & Wen, 2005, p. 343).

Second, from a marketing perspective, if there were no viruses, there would be no need to upgrade security systems so often, or to purchase antivirus software, personal firewalls, and the like. Threats to capitalism have been turned into general fears and risks, which in turn are translated into consumer products that aim to control that fear and deliver safety (Parikka, 2005). Making users personally responsible for their security signifies that they must be trained to practice write-protection, to limit access, to create back-ups, and to purchase and update malware protection software. Third, it appears that one consequence of virus propagation which is consistently described as negative is the direction of unwanted advertising to consumers. This was the purpose of the various versions of Sobig, which took control of the computers of unwitting private users to send thousands of advertising emails (‘spam’) in their name (Thompson, 2004, p. 32). That some hackers may have teamed up with ‘spammers’ usually draws condemnation from ICT industry spokespeople. However, it could be argued that the practice of spamming corresponds precisely to the advantages of ‘e-business’ which the ICT industry has been touting for years, such as the ability to reach consumers directly with cheap and personalized advertising messages.[2] Anti-spamming technology also

[2] The same could be said of the reportedly increasing quantities of ‘spyware’ and ‘adware’ being secretly

represents a lucrative market, as demonstrated in May 2004 when anti-virus manufacturer Symantec announced it would pay about $300 million to acquire Brightmail, a maker of anti-spam technology.

Finally, it is likely that the contemporary War on Terror, like all other modern wars, will fuel technoscientific innovation. Cyberwarfare will require talented programmers – and who better to fight this battle than hackers? Indeed, some lawbreaking hackers demonstrate an eager readiness to 'switch sides' at the drop of a hat and join the ranks of computer security personnel. The worm-creating 'Grugq' used his Unix parasite as a self-promotion tool, posting the article which detailed his findings on the bulletin board of *neohapsis* (a computer security company), and concluding his introductory message with 'PS. If you can offer me a job in the computer security field in either the UK or Europe, please let me know' (The grugq, 2001b). He was perhaps attempting to emulate Eric Bloodaxe (a.k.a. Chris Coggans) a member of hacker super-group the Legion of Doom who went on to help establish computer security firm Comsec, and later became senior network security engineer for the WheelGroup network security company (Jordan and Taylor, 1998, p. 771). More recently, the author of the Sasser worm, Sven Jaschan, was hired by German security software Securepoint to create firewalls (AFP, 2005). In fact, businesses have long hired computer intruders to conduct pseudo-attacks against their systems in order to detect security weaknesses (Shipley, 1999), and state agencies are now adopting the same methods: the US Department of Energy has sponsored the Idaho National Engineering and Environmental Laboratory to create a cyber security centre which employs hackers to conduct mock intrusions into both government and private facilities (Tanner, 2004).

Hackers are deeply embedded within contemporary criminal capitalism. Not because hackers are paid by states and corporations to commit fake crimes, or even because they participate in mafia capitalism – no evidence of such participation exists – but because hackers epitomize the contradictions inherent in the development of information and communication technology. Commerce depends on the creativity of 'mass of informal, innovative, intellectual activity – "hacking" – [...] even as it criminalizes it' (Dyer-Witheford, 1999, p. 228). Moreover, the transmission of digital data over networks means that information must be copied from one node to another. Hackers, the masters of technological creativity and piracy, are not exactly at odds with a digital economy which pits content providers against hardware manufacturers, as symbolised by the

installed on individual consumers' machines. IMesh, a popular file-sharing application, 'bundles' an application known as Marketscore. All the user's web traffic is then routed through Marketscore's servers, where it is analysed to create research reports on 'Internet trends and e-commerce activities'. Even data entered on secure websites such as passwords, credit card numbers and bank account numbers is accessible (Delio, 2004). Marketscore is 'adware'; it performs many or all of the same functions as its illegal cousin 'spyware', but alerts users to its presence and intentions – a reference to the program may be included in the legal jargon of one of the on-screen installation agreements that computer users routinely accept, for example (Eunjung Cha, 2004, p. A01). In December 2004 Microsoft purchased computer security firm Giant Company Software Inc, and announced in January 2005 its intention of entering the computer security market by releasing Giant's product, by then known as 'Microsoft Windows AntiSpyware' (Musgrove, 2005, p. E05); it has since been redubbed 'Microsoft Defender'.

infamous Apple Computer slogan: ‘Rip. Mix. Burn. It’s your music’. The digitization of commodities compels actors on the market to continuously break laws; it is in this sense that capitalism can be said to have become criminal. And when consumers all engage in the mass piracy of cultural commodities, the only solution for corporations is to engage in mass spying – file-sharing versus spyware, buyers and sellers locked in a neverending spiral of crimes and countercrimes. Hacking-as-dangerous-pleasure occupies the central place in this ‘knowledge economy’, representing both contemporary capital’s greatest marketing success and its greatest mystification about contemporary conditions of production. In terms of marketing, the ethereal ethic of the public domain, the digital commons, and free software help to overcome the potential ‘sales resistance’ of consumers (Mandosio, 2000, p. 140). Hackers’ creation of non-copyrightable, evolutionary and democratic free software is a boon for the manufacturers of computer equipment. The anarchistic discourse of the free software community conveys the impression that the Internet is a cornucopia brimming over with free offerings. Naturally, this enticing prospect will help to *create* in consumers the *need* for the hardware and Internet connection required to access this free bounty. Moreover, in the future, P2P file sharing networks are likely to be adapted to allow electronic ‘fingerprinting’ of files, and hence their commercial exploitation, using for example the SnoCap software, created by Shawn Fanning, the student hacker who invented Napster (Mcguire, 2004).

In terms of production, focusing on the knowledge worker forbids an accurate understanding of the reality of the productive process within globalized capitalism. General intellectuals, cyberpunk fiction writers and the mass media discourse on technology all focus on the bodiless world of software code, and on its interpreters, a highly talented caste of technicians, whose idiosyncracies are fondly overlooked by their managers and company stockholders, and whose work ethic ‘emphasizes passionate and free-rhythmed activity’ (Himanen, 2001, p. 56). This reflects the gendered vision of human activity in which the male life of the mind is valued over womens’ confinement to the visceral body (Wajcman, 2004, p. 77), and which excludes females from a technological sphere peopled by male ‘nerds’. Focusing on software also deflects attention away from the manner in which hardware is produced – by another, quite different type of worker in the global economy (see Klein, 2000). Immaterial coding conceals the reality of the global workforce, which, throughout the third world, is mostly made up of women. It also hides the contemporary restructuring of work that broadly has the characteristics formerly ascribed to female jobs, jobs literally performed only by women. The process of feminization of work can be understood as when individuals are made extremely vulnerable and subjected to time arrangements that make a mockery of a limited work day (Haraway, 1991, p. 166). Focusing on male hackers encourages us to forget the Chinese factories where the hardware is produced to a rhythm that is anything but free, and where the noxious digital waste is disassembled and recycled (Basel Action Network, 2002).

That an alternative general intellect (in the form of law-abiding and lawbreaking hacker activity) is riven with contradictions necessarily leads to a questioning of the progressive or revolutionary potential of the concept of general intellect itself. The notion’s focus on ‘knowledge workers’ also results in a blindness to the nature of the technological system, and its effects. If we accept the productivist tenet that technological development is a positive and progressive force, then general intellect such as that embodied by the hacker community may indeed constitute what Deleuze and Guattari (1987, pp. 3-25) call ‘machines of struggle’ fighting the domination of capital: a horizontal, decentered, networked resistance reappropriating technology for democratic purposes. Other commentators, however, hold the view that since technology destroys the environment and atomizes individuals, it embodies, rather than liberation, the very principle of domination. Donna Haraway’s early work (1991, p. 164) reminded us that technology's extension of capitalism’s control over the globe signifies the translation of the world into a problem of coding, in which all resistance to instrumental control disappears, and all heterogeneity can be submitted to disassembly, reassembly, investment and exchange. All external references, the idea of nature for example, are irrelevant to the imperative of technological development. This process has acquired its own logic, and has become a substitute for the world, or the only possible world, irrespective of whether one envisages this world as articulated by capitalist accumulation or not. Gunther Anders (1956/2002, p. 37) writes about the Promethean shame of people who are reduced to being interchangeable cogs within gigantic units of production and consumption. In this role, they are less skilled than machines; they experience inferiority complexes; they feel ashamed of not being strong enough, of their psychological frailty, of growing old. After all, when confronted with electronic failure, a problem so beyond our power to resolve that it appears almost fantastic, we become as helpless as a child with a broken toy. The increased autonomy promised to us by an alternative general intellect, which would not obey the rules of a repressive market economy, must necessarily be qualified by this limit, which extends from a simple practical frustration (the impossibility of repairing an appliance) to the myriad complexities of the contemporary technological system, which can only be run by hyper-specialized technicians and technocrats. Indeed, despite the immense quantity of technical knowledge available in our society, to a far greater degree than our ancestors, we lack technical know-how. The ‘rebellion’ of rogue computer programmers, in addition to its structural role as both foil and aide to capital and the state, also performs the social function of distracting us from technological alienation and technocratic control. Hackers, who dispose at will of their own miniature software-building factories, may offer a symbolic compensation to our feeling of inferiority towards technology: the notion that some of us are able to modify and disrupt our corporate-produced technological environment, rather than be passively submerged in it.

References

AFP (2004) ‘Mydoom overtakes Sobig.F as biggest computer virus ever’, 29 Jan.

AFP (2005) ‘Experts warn against hiring hackers’, 23 May.

Anders, G. (1956/2002) *L'Obsolescence de l'Homme*, trans. Christophe David, Editions de l'Encyclopédie des nuisances, Paris.

Anon., (2003) ‘Meet the superbugs’, *Australian Personal Computer,* Feb., pp. 82-86.

Basel Action Network (2002) *Exporting Harm: The High-Tech Trashing of Asia*. Available at: http://www.ban.org [Accessed 15/06/2004]

Barlow, J.P. (1996) *A Declaration of the Independence of Cyberspace*. Available at: http://www.eff.org/~barlow/Declaration-Final.html [Accessed 21/03/2004]

Bequai, A. (1997) 'Organized crime: manipulating cyberspace', *Computer Audit Update*, vol. 1997 no. 12, pp. 25-29.

Breton, P. (2000) *Le culte de l'Internet. Une menace pour le lien social?*, Editions La Découverte, Paris.

Brock, J.L. (1996) 'Information Security: Computer Attacks at Department of Defense Pose Increasing Risks', Testimony before the Permanent Subcommittee on Investigations, Committee on Government Affairs, U.S. Senate. Available at: http://www.fas.org/irp/gao/aim96084.htm. [Accessed 30/03/2004]

Business Software Alliance (2001) *Sixth Annual BSA Global Software Piracy Study*.

Castells, M. (1997) *End of Millennium. The Information Age: Economy, Society and Culture*. vol. III, Blackwell, London.

Clinton, W.J. (1999) 'Keeping America secure for the 21st Century', *Proceedings of the National Academy of Sciences*, vol. 96, no. 7, pp. 3486-3488.

Cohen, F. (1987) 'Computer viruses: theory and experiments', *Computers and Security* vol. 6, no. 1, Feb., pp. 22 - 35

Deleuze, G. & Guattari, F. (1987) *A Thousand Plateaux: Capitalism and Schizophrenia*, trans. Brian Massumi, Athlone, London.

Delio, M. (2004) 'Spyware on my machine? So what?', *Wired News*, 6 Dec. Available at: http://www.wired.com/news/technology/0,1282,65906,00.html [Accessed 10/12/2004]

Denning, D.E. (1990) 'Concerning hackers who break into computer systems', *Phrack* no. 32. Available at: http://www.phrack.org [Accessed 30/03/2004]

----------------- (1999) 'Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy', Nautilus Conference.

Available at: http://www.nautilus.org/infopolicy/workshop/papers/denning.html [Accessed 30/03/2004]

Dyer-Witheford, N. (1999) *Cyber-Marx. Cycles and Circuits of Struggle in High-Technology Capitalism*, University of Illinois Press, Urbana and Chicago.

Eunjung Cha, A. (2003) 'Internet dreams turn to crime. Russian start-up firm targeted U.S. companies', *The Washington Post*, 18 May, p. A01.

--------------------- (2004) 'Computer users face new scourge. Hidden adware programs hijack hard drives', The Washington Post, 10 Oct., p. A01.

Ferronato, M. (2004) 'The VX scene', *I love you*. Available at: http://www.digitalcraft.org/iloveyou/catalogue_VXscene_Massimo_Ferronato.htm [Accessed 15/12/2004]

Foucart, S. (2003) 'Internet est victime d'une recrudescence des attaques de virus', *Le*

Monde, 3 Sept., p. 23.

Ghosh, R.A. (1998) 'FM Interview of Linus Torvalds. What motivates free software developers?' *First Monday*, vol. 3, no. 3. Available at: http://www.firstmonday.org/issues/issue3_3/torvalds/index.html [Accessed 12/01/2004]

Gibson, W. (1984) *Neuromancer*, Ace Books, New York.

-------------- (1986) *Count Zero*, Ace Books, New York.

-------------- (1988) *Mona Lisa Overdrive*, Bantam Books, New York.

Grugq, The (2001a) *Cheating the ELF: Subversive dynamic linking to libraries*. Available at: http://hcunix.7350.org/grugq/doc/subversiveld.pdf [Accessed 21/03/2004]

-------------- (2001b) 'Subversive dynamic linking on UNIX platforms', *Neohapsis Archives*. Available at: http://archives.neohapsis.com/archives/vuln-dev/2001-q4/0333.html [Accessed 30/03/2004]

Hales, P. (2002) 'Cyber security act slips into homeland security legislation. Hackers face life imprisonment, snoops gain sweeping powers', *The Inquirer*, 14 Nov. Available at: http://www.theinquirer.net/?article=6250 [Accessed 30/03/2004]

Halbert, D. (1997) 'Discourses of danger and the computer hacker', *The Information Society* no. 13, pp.361-374.

Haraway, D. (1991) *Simians, Cyborgs and Women: The Reinvention of Nature*, Routledge, New York.

Heintz, J. (2000) 'Russia home to hard-working hackers. Notorious or desperate? Economic woes encourage fabled "khakeri"', *The Associated Press*, 20 Nov.

Helmreich, S. (2000) 'Flexible infections: Computer viruses, human bodies, nation-states, evolutionary capitalism', *Science, Technology & Human Values* vol. 25 no. 4, pp. 472-491.

Himanen, P. (2001) *The Hacker Ethic. A Radical Approach to the Philosophy of Business*, Random House, New York.

Jordan, T. & Taylor, P. (1998) 'A sociology of hackers', *The Sociological Review* vol. 46 no. 4, pp. 757-780.

Kan, G. (2001) 'Next step for P2P? Open services', *openp2p.com,* 8 Feb. Available at: http://www.openp2p.com/pub/a/p2p/2001/08/02/openservices.html [Accessed 27/01/2005]

Klein, N. (2000) *No Logo: Taking Aim at the Brand Bullies*, Flamingo, London.

Krebs, B. (2003) 'Internet worm hits airlines, banks', *washingtonpost.com*, 26 Jan. Available at: http://www.washingtonpost.com/wp-dyn/articles/A46928-2003Jan26.html [Accessed 15/01/2004]

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*, Doubleday, New York.

Lowe, S. (2004) 'The worm has turned', *Sydney Morning Herald*, 13 May, p. 16.

Mandosio, J-M. (2000) *Après l'effondrement. Notes sur l'utopie néotechnologique*, Editions de l'Encyclopédie des nuisances, Paris.

Marx, K. (1973) *Grundrisse*, Penguin, Harmondsworth.

McGuire, D. (2004) ‘Mashboxx aims to make file sharing legit. Grokster founder prepares licensed P2P service’, washingtonpost.com, 22 Dec. Available at : http://www.washingtonpost.com/wp-dyn/articles/A18568-2004Dec22.html?referrer=email Accessed 24.01.2005 [Accessed 20/01/2005]

Mentor, The (1996) 'The conscience of a hacker aka The Hacker's Manifesto', *Phrack*, vol. 1, January 8, 1996.

Musgrove, M. (2005) ‘Microsoft offers anti-spyware software. Analysts say move signals interest in security market’, *The Washington Post*, 7 Jan., p. E05.

Negri, T. (1994) ‘Constituent republic’, *Common Sense* no. 16, pp. 88-96.

Nissenbaum, H. (2004) ‘Hackers and the contested ontology of cyberspace’, *New Media and Society* vol. 6 no. 2, pp. 195-217.

Parikka, J. (2005) ‘Digital monsters, binary aliens – Computer viruses, capitalism and the flow of information’, *Fibreculture* 4. Available at: http://journal.fibreculture.org/issue4/issue4_parikka.html [Accessed 15/10/2005]

Pax, S. (2003) *The Baghdad Blog*, Atlantic Books, London.

Poulsen, K. (2003) ‘Matrix sequel has hacker cred’, *SecurityFocus*, 16 May 2003. Available at: http://www.theregister.co.uk/2003/05/16/matrix_sequel_has_hacker_cred/ [Accessed 8/12/2004]

Qing, S. & Wen, W. (2005) ‘A survey and trends on internet worms’, *Computers & Security* 24, pp. 334-346.

Raymond, E. (1986) ‘How to become a hacker’, *Thyrsus Enterprises*. Available at: http://www.catb.org/~esr/faqs/hacker-howto.html [Accessed 30/03/2004]

---------------- (1998) ‘The cathedral and the bazaar’, *First Monday*, vol. 3, no. 3. Available at: http://www.firstmonday.org/issues/issue3_3/raymond/index.html [Accessed 5/06/2003]

Ross, A. (1991) ‘Hacking away at the counterculture’, in *Technoculture*, eds C. Penley, & A. Ross, University of Minnesota Press, Minneapolis.

Schiller, D. (1999) *Digital Capitalism. Networking the Global Market System*, The MIT Press, Cambridge (Mass).

Shipley, G. (1999) ‘Anatomy of a network intrusion’, *Network Computing*, 18 Oct. Available at: http://www.networkcomputing.com/1021/1021ws1.html [Accessed 12/01/2004]

Stallman, R. (1985) ‘Why I must write GNU’, *The GNU Manifesto webpage*. Available at: http://www.gnu.org/gnu/manifesto.html [Accessed 5/06/2003]

Sterling, B. (1992) *The Hacker Crackdown. Law and Disorder on the Electronic Frontier*, Bantam Books, New York.

Tanner, A. (2004) ‘Hackers seek to save America’, Reuters, 17 Sept.

Thompson, C. (2004) 'The virus underground', *The New York Times Magazine*, 8 Feb., pp. 28-36.

Turkle, S. (1984) *The Second Self: Computers and the Human Spirit*, Granada, London.

Vincent, J-M. (1993) 'Les automatismes sociaux et le general intellect', *Futur Antérieur* 16, pp. 121-130.

Virno, P. (1996) 'Notes on the general intellect', in *Marxism beyond Marxism*, eds S. Makdisi, C. Casarino, & R. Carl, Routledge, London.

Wajcman, J. (2004) *Techno Feminism*. Polity Press, Cambridge.

Wark, M. (2004) 'A Hacker Manifesto (version 4.0)', *Subsol*. Available at: http://subsol.c3.hu/subsol_2/contributors0/warktext.html [Accessed 18/04/2004]

Williams, P. (2001) 'Organized crime and cybercrime: Synergies, trends, and responses', *Global Issues. An Electronic Journal of the U.S. Department of State*, vol. 6, no. 2. Available at: http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm [Accessed 21/03/2004]