Contents

> *The goal now is not whatever all the analysts first set out to do; the goal becomes the creation of the system itself. Any ethics or morals or second thoughts, any questions or muddles or exceptions, all dissolve into a junky Nike-mind: Just do it. If I just sit here and code, you think, I can make something run. When the humans come back to talk changes, I can just run the program. Show them: Here. Look at this. See? This is not just talk. This runs. Whatever you might say, whatever the consequences, all you have are words and what I have is this, this thing I've built, this operational system. Talk all you want, but this thing here: it* works.
>
> —Ellen Ullman, *Close to the Machine*

I__ "We Love Your Computer"

The month was May, the year was 2000, and the loss was one of the largest amounts of money ever caused by a worm in computer history. On Monday morning in early May, if you had a Windows system running at work, there was probably a message with the unsuspecting subject "I love you" in your Outlook mailbox. The message text read "kindly check the attached loveletter coming from me." High as a kite, you would have opened the mail (unless you were *really* sure that nobody would send you a message with that subject, in which case you probably would have opened the loveletter anyway). But what would have followed your click on the loveletter would have made you rapidly come back down to earth: the attached file love-letter-for-you.txt.vbs was not a love letter at all, but an internet *worm* (worms are these little programs that can self-replicate and spread through the internet very rapidly, usually via Microsoft Outlook programs). The "I love you"-virus, as it came to be known, sent itself to each address in your Windows system address

book and dropped an .htm-file and an mIRC (a internet chat application) script on your computer as alternative ways for self-replication. So in that week of May, the worm spread rapidly to millions of Windows users, damaging their systems by changing file types to .vbs-endings and copying itself each time they would try to execute one of these 'infected' files. By a love letter that had turned into a menace to your personal (if digital) belongings, these users suddenly got acquainted with the dark, the vulnerable, the uncanny side of the 'Web:' Computer help lines were busy and people were just plainly *scared*. Yes, you had been told by computer security experts never to give out your private address online since 'stalkers' might hunt you in real life (ironically, of course, 'spyware' finds out your private information for other *companies*). But a love letter turning into a evil worm on the spot—that had been unheard of.

Of course, this story is highly simplified. In fact, it only shows one assessment of the strike of the "I love you"-virus—that of the media and the anti-virus company 'analysts.' Ian Hopper, journalist with CNN, chose to aptly title his feature about the worm "Destructive *I Love You* computer virus strikes world wide."[1] In his article, Hopper describes how the "self-propagating and destructive" virus "wrought hundreds of millions of dollars in software damage and lost commerce." He quotes computer security expert Peter Tibbett of ICSA.net, who estimated that "the price tag (of the virus attack) would exceed $1 billion by Monday morning" of the week after the worm had first been discovered. Interestingly, *hackers*, the people whose programming skills allegedly gives birth such viruses, have largely relativized such menacing accounts of the "I love you"-attack. Frans Faase, a hacker from the Netherlands, has analyzed the virus source code in detail, and he has made his findings available on the internet.[2] Faase concludes his code analysis by saying that "the virus does not contain all kinds of dirty tricks that the Anti-virus software people claim it to have." And he goes on to say that the "virus was never intended to be anything more than a *practical joke*. It is also not the most evil virus one can think of. It does some harm, but there are some simple modifications which would make it much more harmful."[3]

---

[1] http://www.cnn.com/2000/TECH/computing/05/04/iloveyou.01/index.html.

[2] http://home.planet.nl/%7Efaase009/iloveyou.html.

[3] http://home.planet.nl/%7Efaase009/iloveyou.html, my emphasis.

The "I love you"-incident of May 2000, in my mind, highlights a great number of issues in thinking about 'digital culture.' The virus, it seems, has been constructed as an uncanny (or even 'abject') object by the media and the companies, whereas virus programming seems to be *fun* in the eyes of the hackers. With hacking as mere fun, political and cultural theory of the sort which emphasizes the role of 'counter-hegemonic groups' seems to run into difficulties when it projects its liberatory hopes onto hacker culture. On the one hand, there seems to be a pathological projection of the 'abject of the electronic age' onto hackers by the media and the general public, and on the other hand hacker culture does not seem to be political *per se*, but a multi-layered phenomenon that consists of multiple 'immagined communities' (Benedict Anderson) that lie entirely within a hegemonic/antagonistic framework. In the following pages, I will attempt to describe those different (and divergent) communities and the images that are projected onto them and that they project onto others. Without the help from influential hacker figures, this endeavour, of course, would have been impossible (and quite fruitless in its theoretical outcome).[4] But with the many comments that I have got, I hope that this paper will help do away with some of the confusion in thinking about hackers and digital culture, and maybe even lead on to a more grounded discussion about 'the political' in the datasphere. I think that, as will turn out, even if hackers are not the 'new hope' for that Marxist revolutionary subject which we've been looking for so long, there are other people that are sneaking through the contested terrain between hacking and political action—hacktivists—and that what they are doing might constitute, to my mind, an 'art of resistance.' But now, let's go underground...

---

[4] I am particularly grateful for comments on my arguments by the famous GNU/Linux programmers Richard Stallman and Eric Raymond, by Jack Napier of the Billboard Liberation Front, John Young of cryptome.org, and the legendary hacker John "Cap'n Crunch" Draper.

II__ HACKERS ON THE BIG SCREEN

Hacking will begin killing people soon (...). Hackers in Amtrack computers, or air traffic control computers, will kill somebody someday. Maybe a lot of people.

—Bruce Sterling, *The Hacker Crackdown*

Hackers appeared as a mass cultural phenomenon in the United States around 1990. The so-called 'hacker crackdown' inscribed itself into the American psyche at that time, a large-scale FBI hunt of computer criminals who were accused of having crashed the AT&T telephone system. The way in which hackers surfaced in U.S. culture, however, had little to do with the positivistic way in which the term was first employed by the model train hobbyist at MIT's Tech Model Railroad Club (TMRC) in the early 60s. In fact, looking at Hollywood movies as indicators for mass cultural perception of reality, I would argue that technology in the late 1980s was portrayed on the screen as an uncanny, finally uncontrollable, dark menace—the gooey chrome of *Terminator 2*, which leaves the individual vulnerable and disempowered. Hackers, though, were ambiguously constructed: They were the strange technology wizards who are, as 'good Americans,' fighting for their civil liberty, but they were also people with questionable motives, not hesitating to sell their technical expertise to the 'bad guys.' In addition, 'the political' was generally reduced to activism for civil liberty—the state apparatus becomes a shady force that randomly blocks you from 'restricted areas.' In the 1990 release of Renny Harlin's *Die Hard 2*, all these issues figure prominently: The movie finally took to the screen Bruce Sterling's prediction that 'hacking will kill people soon.'

In the movie, the tough, everyday guy John McClane (Bruce Willis) is waiting to pick up his wife Holly (Bonnie Bedelia) at an airport near Washington D.C. On the same evening, however, the plane of Ramon Esperanza (Franco Nero), a South American politician who is being brought to a drug-related trial to the U.S., is scheduled to arrive. A group of hackers, hired by Esperanza, take control of the airport technology to land his plane, demanding a B747 to escape to 'the tropics' together with the politician. The motive of the uncanny technology is introduced in the movie by an old lady, who, pointing to her (then brand-new) cellphone, asks McClane's wife on an airplane, "Isn't technology wonderful?" The remaining two hours of *Die Hard 2* can be read as a boldly negative answer to this question. In fact, the movie opens up a dichotomy between mere

mechanical tools and electronic technology. This dichotomy becomes apparent as, in the first scenes, McClane's car is towed and he starts an argument with a New York police officer (who neither cares about McClane's Los Angeles Police badge nor about the date being Christmas Eve). The towing scene works as a counter-statement against the rest of the movie: The human operator still has the power over her tow truck—McClane's anger is directed against her, not against the machine itself. Telephones, on the other hand, are a dangerous and unpredictable technology in the movie. The notoriously scarce pay phones are almost a running gag, and cellphones can even threaten your life: As McClane sneaks up to the hackers who have barricaded themselves in a small church, his cellphone rings, giving him away to the crossfire of his enemies. Not surprisingly, there's not a lot of 'good' technology in the movie. In a classic scene, McClane is able to press the ejection switch of a hot seat just in time to escape from a exploding plane. But generally, technology in *Die Hard 2* is constructed as the dark, uncanny in-between the men at the switches in the airport control tower and the pilots in the cockpit. Even the hackers have to experience that it can turn into a menace when, after they ingeniously hacked a whole airport control system, their B747 finally explodes—through the manual labor of John McClane.

Another notion that is deeply connected to hacking is 'trespassing,' a concept which *Die Hard 2* employs in complex ways. Individuals are trying to gain access to forbidden spaces, and an authority blocks this access for no apparent reason: The ususally crowded public space (the airport arrival halls, bars, cafés) is set against the randomly sealed-up space that is owned by someone else. Throughout the movie, the notion of 'trespassing' is connected to the uncanny when McClane actually manages to cross over into the 'forbidden.' He then finds himself within dark, uncanny surroundings, as in the gunfight between the screeching belts of the luggage transport system in the 'bowels' of the airport. The hackers, of course, are already on this other side, *close to the machine*, they use it as a camouflage for their activity. McClane is randomly blocked away from this space, and this contingency of access denial is personified in the figure of airport police chief Lorenzo (Dennis Franz). Lorenzo is the fat, annoying figure that sits in McClane's way wherever he goes, attentive only when his own personal position within the system is endangered by his own boss—bureaucracy personified. Arguably, in connecting this bureaucratic character with McClane's crossing over into the 'forbidden,'

Die Hard 2 establishes a hacker mindset in the viewer. In fact, the whole movie could be read in terms of the continuing attempts to *get access* by McClane, and, of course, by the hackers to get access to the tower, which, in a way, positions them close to McClane.

Not surprisingly, then, the movie's imagery of hackers is highly ambiguous. On the one hand, since we're dealing with a Hollywood movie, to some extent, hackers simply are the 'bad guys.' The Colonel (William Sadler), the leader of the group of hackers, is a blonde, teutonic looking man with an evil stare, and the "victory for our way of life" which he proclaims right before their B747 explodes, seems to be a victory for smoking dope in the back of a plane, and for partying in the tropics on money that you've been paid by a drug mafia figure. The political motivation of the hackers in bringing Esperanza safely to the tropics is summed-up in the statement "I've seen enough snow in my lifetime." But then again, hackers have many good traits in *Die Hard 2*. 'Social engineering,' for example, is a strategy that both McClane and the hackers use: Captain Grant (John Amos), the leader of a military platoon that apparently comes to safe the situation, turns out to be a member of the hacker group in the end. And John McClane, pretending to be a local policeman, 'socially engineers' his way to a fingerprint of a dead hacker. The movie makes clear that a hacker is not "some punk stealing luggage" (Lorenzo) but someone who can influence technology on a very deep level when the hackers not only shut down the lights of the runways, but also *reset the ground* for a plane at minus 200 feet—they turn into terrorists who can deeply influence a whole world structure that relies heavily on technology. "It's like the tower isn't there," the 'good guys' have to realize, before they send in a 'good' hacker of their own: an African-American tower technician elegantly hacks a beeper tower to sending radio signals to the pilots. So when McClane's wife Holly tells him at the very end, "They told me there were terrorists at the airport," McClane somewhat sympathetically ends the movie on the note: "They are that too."

But let's not forget about the limits of *Die Hard 2*. The movie might portray hackers ambiguously and it might bring to mind a relatively complex picture of the Hollywood projections of uncanny technology, but the whole source for the terror and the fighting, the *political* problems of the United States with South American drug cartells, entirely steps into the background as the action continues to develop. Generally, then, the movie is more about personal activism, freedom, and empowerment to *get access*. The politician Esperanza is not brought to a fair trial but simply killed—a fact that might point

to the limits that anyone who has political ambitions to inscribe into hacker culture might have to face with. So let's leave the contradictory Hollywood mindset of the late 1980s aside and see whether the concept of a 'technological uncanny' will get us anywhere when employed to the really existing internet and its digital outlaws.

III__ Theorizing the Vulnerability of Dataspace

> *The perfect bogeyman for Modern Times is the Cyberpunk! He is so smart he makes you feel even more stupid than you usually do. He knows this complex country in which you're perpetually lost. He understands the value of things you can't conceptualize long enough to cash in on. He is the one-eyed man in the Country of the Blind.*
>
> —John Perry Barlow, *Crime and Puzzlement Manifesto*

There's an important difference between saying that something is 'constructed' and saying that the image of technology in Hollywood movies is merely an uncanny fantasy. And there is also a difference between relativizing hacker culture as a complex, empty signifier and saying that hackers as a menace (crackers) simply don't exist. There *are* very real reasons for the public angst. Think of the horror that stood at the very beginning of the internet. In 1957, the Sovjet Union succeeded in lauching a satellite into the orbit, and the Sovjets won the 'space race' against the United States. America fell into the so-called 'Sputnik shock' and, once it was on its feet again, founded the Advanced Research Project Agency (ARPA) as a part of the Department of Defense. The computer history *Fire in the Valley* clearly assesses that the purpose of the network of computers that the ARPA researchers put up back then had been from the start "to build a defense-research communication channel robust enough to survive a nuclear attack."[5] And this 'horror of the beginning' has technologically continued throughout the history of the internet.

The free flow of information on a global computer network is essentially hard to control, thereby adding to the uncanny twist of the 'Web.' Corporations take great pains to secure their 'unfree' data, and some of them are selling security to private individuals in

---

[5] Michael Freiberger & Peter Swaine, *Fire in the Valley: The Making of the Personal Computer* (New York: McGraw-Hill, 2000) 209.

the form of encryption software or firewall programs. So, with 'vulnerability' being a central issue in the thinking about an uncanny logic of the datasphere, the nature of information turns into a contested, attacked, secured, and fought about concept. Two projects, I think, fit particularly well to illustrate this point. The first one is cryptome.org, which is a website that specializes in making 'restricted information' available to the public. On the project's homepage, the purpose of cryptome.org reads: "Cryptome welcomes documents for publication that are prohibited by governments worldwide, in particular material on freedom of expression, privacy, cryptology, dual-use technologies, national security, intelligence, and blast protection—open, secret and classified documents—but not limited to those."[6] Browsing through the website, one can find, for example, recent documents from the Al Qaeda trials, the access to which has actually been bought up by Cryptome. The site's aim for providing access to restricted information for individuals presupposes, of course, the two notions that there is 'secret' information and that the individuals' vulnerability is not to have access to that. Furthermore, Cryptome constructs a state apparatus that is vulnerable in that there finally *is* a way to get access to its secrets (by the cunning of crackers, mostly). These two-layered vulnerabilities surfaced again in an e-mail conversation that I had with John Young, the maintainer of cryptome.org. Young wrote that cryptome.org is "political in that we aim to offer information access different from what is dispensed by authoritarians—all of whom are censors and avid suppressors of political action."[7]

In the context of digital art, a project of the San José-based collective C5 is interesting when looking at the contested nature of information on the 'Web' and at the vulnerabilities that the free flow of information causes. For Lisa Jevbratt's "1:1," for example, C5 software robots travelled in datasphere, systematically evaluating the content of IP addresses (an IP address is the number that a 'Web' address stands for, and it consists of five numbers from 0 to 255).[8] During the first run of the bots in 1999, what appeared on the "1:1" maps of dataspace were mostly governmental or military pages that often required passwords—the map gave you an uncanny feeling about the 'real' nature of its

---

[6] http://www.cryptome.org.

[7] Personal e-mail to the author from May 1, 2002.

[8] http://www.c5corp.com/projects/1to1.

content instead of the friendly and colorful image within your everyday Yahoo! frame. In another project called Softsub, C5 'data-mines' your computer at home and feeds seemingly banal information about your directory structure and desktop layout into a program that calculates your machine's closeness to other desktop configurations.[9] Softsub, therefore, hints at the "lack of awareness (of the average computer user) about how extensively personal information that has been collected is used on the Net and to whom this information is shared."[10]

With cellphones increasingly turning into a fashion product (Nokia, for example, makes more money off the selling of plastic covers than off technology), 'vulnerability,' of course, also reaches into cellspace. In the *Hacker Crackdown*, Bruce Sterling cautions that "eavesdropping on other people's cordless and cellular phone calls is the fastestgrowing area in phreaking (phone hacking) today."[11] It seems comparatively easy to fake your identity on a cellphone, a hack that enables you to hide your location from 'authorities' (drug dealers like this) and to get free calls. In fact, any attentive reader of issue 73 of the *Datenschleuder*, a magazine of the Berlin-based Chaos Computer Club (CCC), will learn how to lead denial of service attacks (DoS) against Nokia cellphones. Interestingly, the uncanny of cell- or telephone space has a historical dimension:[12] In the 1870s, the early days of telephony, phones were regarded as spooky gadgets—mysteriously speaking machines that hardly anybody would dare talk to. Only much later, telephones came to be regarded as a *medium* with a real person on the other side. So the uncanniness stayed on with each time that the technology took another step forward: Telegraph boys, maybe being the first hackers, had fun wiring up the wrong people with each other until, in 1878, Bell fired them all and legions of professional female operators stepped in.

This suggests that hackers (or 'crackers') themselves, of course, can be 'bad guys' as well, and contribute to 'vulnerability' on the 'Web.' The National Institute of Standards and Technology, in a famous document entitled "Threat Assessment of Malicious Code and Human Threats," describes crackers in the following way: "Today, computer systems

---

[9] http://www.c5corp.com/projects/softsub.

[10] http://www.eff.org/cafe.

[11] Bruce Sterling, *The Hacker Crackdown*, Part 2. Online. http://www.mit.edu/hacker.

[12] See Sterling's *Hacker Crackdown*, Chapter 1.

are under attack from a multitude of sources. These range from malicious code, such as viruses and worms, to human threats, such as hackers and phone "phreaks." The document goes on by saying that malicious "code (...) attack a system in one of two ways, either internally or externally. (...) Human threats are perpetrated by individuals or groups of individuals that attempt to penetrate systems through computer networks, public switched telephone networks or other sources."[13] What, to the technologically illiterate, seems to be a *Die Hard 2*-construction of a menace to society, maybe becomes more understandable when you imagine someone regularly searching through your trash. Someone reads every torn bill or letter that you threw away. You'll realize that this person could find out quite a lot about you, only until now you never thought that someone might actually search something as 'abject' as your trash can. Well, some hackers would do that, and it's called 'trashing.' If you're a little frightened now about your trashing practice, you can imagine the 'uncanny' that computer network administrators feel when they notice a cracker *in their system*...

Bruce Sterling, summing-up what I've said above, writes that the "extent of this vulnerability (of dataspace) is deep, dark, broad, almost mind-boggling, and yet this is a basic, primal fact of life about any computer on a network." In my mind, this vulnerability can be best grasped with Julia Kristeva's notion of 'the abject' which she develops in her book *Powers of Horror*.[14] Using her famous example of the skin on the surface of milk which causes her sickness, Kristeva writes that there "looms, within abjection, one of those violent, dark revolts of being, directed against a threat that seems to emanate from an exorbitant outside or inside, ejected beyond the scope of the possible, the tolerable, the thinkable" (1). If we see crackers as the 'abject' of the electronic age, they constitute that "massive and sudden emergence of uncanniness"(2) and a "real threat (that) beckons to us and ends up engulfing us" (4) that Kristeva talks about. A key passage explicitly connects the *criminal* to abjection: "it is not the lack of cleanliness or health that causes abjection, but what disturbs identity, system, order. What does not respect borders, positions, rules. The inbetween, the ambiguous, the composite (...). Any crime, because it draws attention

---

[13] http://www.csrc.nist.gov/publications/nistir/threats/threats.html.

[14] Julia Kristeva, *Powers of Horror: An Essay on Abjection* (New York: Columbia UP, 1982).

to the fragility of the law" (4). The *fun* in the hacker attitude that has been described by Frans Faase, the hacker who commented the "I love you"-source code, "acknowledges the impossibility of Religion, Morality, and Law—their power play, their necessary and absurd seeming. Like perverson, it takes advantage of them, gets round them, and makes sport of them" (16). The only help against crackers as the 'abject of dataspace' is, of course, the aseptical software figure of Dr. Solomon, the white guy who periodically cleans your hard disk, thereby ritually and redemptively swiping it clean of any 'abject' data. Interestingly, accounts of cracker arrests can be grasped within the notion of the 'abject' as well. Leftist, whose parents were "traumatized" when he was arrested during the 'hacker crackdown,' and Terminus, who was arrested as well to "the stark terror of his wife and children," become the 'abject' in the family—the "threating otherness" (Kristeva) that finally turned out to be within.[15]

After this brief reading of hackers in terms of Kristeva's *Powers of Horror*, I'll continue to refer to her concepts as I will go along in my discussion about hacker culture. For now, let me point to a few other issues that surface in Edward's Said's notion of 'Orientalism' and that, I think, might illustrate some general difficulties in thinking about hackers. As Said suggests, Orientalism is not (only) the mythical, entirely unreal *idea* of the Westerner about the Orient, but also "a Western style for dominating, restructuring, and having authority over the Orient."[16] 'Orientalism' is first and foremost a "relationship of power" (5). So the concept of 'Orientalism' is a discourse that is close to discourses about the datasphere in that produces "internal consistency" (5) of an imagery while it's being based on something that *is* actually there. This notion arguably extends Benedict Anderson's concept of (hackers as) an 'immagined community,' because it points to culture as a complex, multi-layered phenomenon that lies within the Foucauldian power configurations of a hegemonic/antagonistic framework.[17] This is useful to keep in mind as I now turn to an analysis of hacker culture itself.

---

[15] Sterling, *Hacker Crackdown*, Chapter 2.

[16] Edward Said, *Orientalism: Western Conceptions of the Orient* (London: Penguin, 1978) 3.

[17] For an explanation of the notion of 'imagined communities,' see: Benedict Anderson, *Immagined Communities* (London & New York: 1983) 6.

IV__ HACKERS AT THE ELECTRONIC FRONTIER

> *The 'hacker culture' is actually a loosely networked collection of subcultures that is nevertheless conscious of some important shared experiences, shared roots, and shared values. It has its own myths, heroes, villains, folk epics, in-jokes, taboos, and dreams. Because hackers as a group are particularly creative people who define themselves partly by rejection of 'normal' values and working habits, it has unusually rich and conscious traditions for an intentional culture less than 40 years old.*
>
> —*The Hacker Jargon File, Version 4.3.1*

Hackers, in the way in which they imagine themselves and their friends (and enemies), are a complex phenomenon that entails all the difficulties of analysis that hold true for any other subculture. My way through this 'abject' maze will be that I'll describe a distinct U.S. hacker culture as being antagonistic to European hackers, and that has as its latest development the notion of 'ethical hacking.'

Hackers in the United States are much more critical about themselves than the stereotypical, if complex images of *Die Hard 2* suggest. An issue that they are very critical about is *internet access* (without which, of course, they wouldn't be able to hack at all). American hackers, it seems, share a common concern about the 'freedom of information' and about possible restrictions on the openness of the datasphere, and they also share certain premonitions about the Foucauldian workings of power within that sphere. Eric S. Raymond, a famous Linux programmer and author of the infuential book *The Cathedral and the Bazaar*, holds that the datashere is "open in that it's easy for lots of people to reach and difficult to control."[18] Raymond goes on to say that, in the datasphere, he sees "the possibility to help individuals become better able to acquire knowledge and disseminate their thoughts to others" which should give them "more leverage relative to governments and corporations." And John Young of Cryptome says that "there are sustained attempts to restrict (the internet's) becoming and remaining fully open and to instead use it for intellectual, political, social and economic control."[19] So although both hackers imagine the 'Web' as an essentially open space, the limits of that space are clear in that governments and corporations are constructed as blocking the free 'dissemination of thought,' and that the 'Web' is used for controlling purposes by an imagined state

---

[18] Personal e-mail to the author from April 29,2002.

[19] Personal e-mail to the author from April 28,2002.

apparatus.

The critical view that already surfaces in such hacker statements about control and informational freedom finds an expression in the antagonistic construction of 'the cracker,' the 'abject' of *hacker* culture who illegally breaks into computer systems. The Mentor, in his *Hacker Manifesto*, plays with this construction when he 'confesses:' "Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like."[20] Eric Raymond discussed the construction of the hacker/cracker distinction at length in an e-mail conversation with me. He holds that there "is a large, open culture of hackers (...)—technologists who invented the Internet and keep it running (...). We're no threat to anybody. There is a much smaller culture of crackers, very secretive and in parts actively criminal." Raymond traces this antagonism back to the split between the early Personal Computer hobbyists and the campus subculture of minicomputer-based hacker groups—interestingly, many expressions of hacker jargon such as 'trojan' were coined in the 1960s college environments. Nevertheless, what can be seen in this construction of 'the cracker,' in my mind, is that hackers as a subculture have their very own antagonisms. They see themselves as 'the good technologists' with certain codes and laws, while a group that they construct as 'crackers' (or 'script kiddies') disturbs their system and does not 'respect borders, positions, rules,' drawing attention to the emptiness and 'fragility' (Kristeva) of their own self-construction.

It is precisely within this terrain that the notion of 'ethical hacking,' which has become a real buzz-word again, has emerged in the 1980s. Ethical hacking, read within the context of the hacker/cracker antagonism, can be read as another attempt to dismiss the 'abject' of hacker culture. The concept goes back to Stephen Levy's book *Hackers*—true hackers, Levy writes, have a "philosophy of sharing, openness, decentralization" (...). They "were adenturers, visionaries, risk-takers, artists ... and the ones who most clerly saw why the computer was a truly revolutionary tool."[21] Free access to technology, the freedom of information, a mistrust against authority, and the view that computers can change life for the better are the basic columns of Levy's 'ethics.' Surprisingly, these values have been rediscovered by self-help business books today, the most prominent

---

[20] The Mentor, *Hacker's Manifesto*. http://www.totse.com/en/hack/legalities_of_hacking/manifsto.html

[21] Stephen Levy, *Hackers: Heroes of the Computer Revolution* (New York: Doubleday, 1984) X.

examples of which being Eric Raymond's *The Cathedral and the Bazaar* and Pekka Himanen's *The Hacker Ethic.* Raymond's overall argument in *Cathedral* is nicely summed-up by Linus Torvald's (the programmer of the kernel for the 'free' Linux operating system) law: "Given enough eyeballs, all bugs are shallow."[22] As a believer in the free market, Raymond develops a strategy for marketing Linux applications under the brand of 'open source software,' an overall aim that is shared by Pekka Himanen in *Hacker Ethic.* Himanen holds that "computer hackers can be understood as an excellent example of a more general work ethic—which we can give the name *the hacker ethic*—gaining ground in our network society."[23] This ethic, unlike the Weberian work ethic, holds that meaning 'cannot be found in work or leisure but has to arise out of the nature of activity itself" (151). Both Himanen and Raymond suggest an ethics of play which, at the same time, makes the individual *work.* Again, what we have here is the construction of laws and structure that 'hacking,' if anything, was meant to run orthogonal to.

The above discussion suggests some problems with Bruce Sterling's assessment that "there is an element in American culture that has always strongly (...) rebelled against all large (...) companies" and that a "certain anarchical tinge deep in the American soul delights in causing confusion and pain to all bureaucracies, including technological ones."[24] In fact, throughout the U.S. American hacker culture, an image of the *electronic frontier* is still prevalent that could be viewed as the positive imaginary of the unconsious of hacker culture that gets blown up as the hackers continue to face the 'threatening otherness' (Kristeva) within their own tribe. In 1990, John Perry Barlow, together with Mitchell Kapor, founded the aptly named *Electronic Frontier Foundation* (EFF), an organization to promote the right of free speech in cyberspace. Barlow, in his famous *Crime and Puzzlement Manifesto*, works a lot with imagery of the frontier and the century West: "Cyberspace (...) has a lot to do with the 19th century West. It is vast, unmapped, culturally and legally ambiguous, verbally tense (...), hard to get around in, and up for

---

[22] Eric S. Raymond, *The Cathedral and the Bazaar* (Sebastopol: O'Reilly, 1999) 41.

[23] Pekka Himanen, *The Hacker Ethic and the Spirit of the Information Age* (London: Secker & Warburg, 2001) 7.

[24] Sterling, *Hacker Crackdown*, Part 2

grabs."[25] Bruce Sterling, in *The Hacker Crackdown*, uses similar expressions when talking about the nature of the datasphere. Sterling asserts that hackers are "soaked through with heroic anti-bureaucratic sentiment" and that they "long for recognition as a praiseworthy cultural archetype, the postmodern electronic equivalent of the cowboy and mountain man."[26] Furthermore, he talkes about dataspace as the indefinite place 'out there,' and his analysis culminates in the view that "a Personal Computer can be a great equalizer for the techno-cowboy—much like that more traditional American "Great Equalizer", the Personal Sixgun" (Part 3). So I think one can generally assert, with Sean Cubitt, that the anonymity of the U.S. dataspace "has given rise to (...) the most uncompromisingly individualist of cultural icons: the outlaw, the phreak, the cowboy, the frontier." As Cubitt goes on to say, the "very Americanization of matrix vocabulary indicates less its domination by North Americans than the power of the North American mythography of westward expansion and rugged individualism in the new context."[27]

And, not surprisingly, since 'the frontier' is a contested terrain, multiple antagonisms around the hacker ethic are played out between fragmented hacker cultures underneath the blown-up imagery of the 'vast open space.' The principle of the freedom of information is contested as the programming of Linux is basically 'free,' but then again the most often visited sites about Linux applications and information about the 'open source' software scene, slashdot.org and Freshmeat, are owned and run by a company—VA Linux systems. The principle of judging people on what they know is equally contested by the tribal logic of hacker culture: This logic forsters elite thinking and boasting, since "the way to win a solid reputation in the underground is by telling other hackers things that could only have been learned by exceptional cunning and stealth."[28] Handles that contain the words 'master' or 'genius' are frequently used, and Eurpoean hackers (who usually despise of such handles) are constructed as "hash-smoking anarchist hackers who had rubbed shoulders with the fearsome big-boys of international Communist espionage" (Sterling). That computers can change life for the better is highly relativized

---

[25] http://www.totse.com/en/hack/legalities_of_hacking/wholerth.html.

[26] Sterling, *Hacker Crackdown*, Part 2.

[27] Sean Cubitt, *Digital Aesthetics* (London: Sage, 1998) 87.

[28] Sterling, *Hacker Crackdown*, Part 2.

by issues of access and the practice of 'carding' which is (at least to crackers) one of the best ways for an arguably simplistic betterment: In order to get more money for new computers, you spy on someone's credit card transactions to later use the card yourself. Finally, and not surprisingly, hackers also have constructed their very own technological and social uncanny: the figure of Microsoft boss *Bill Gates*. The hacker site enemy.org (together with many jokes) constructs Gates, as Slavoj Žižek aptly writes, as the "Master who is simultaneously our common peer, our fellow-creature, our imaginary double and—*for this very reason*—phantasmatically endowed with another dimension of the Evil Genius."[29] So, given all those antagonisms, hacker culture generally looks highly fragmented and doesn't seem to serve too easily as a 'subculture' onto which one can project hopes of a revolution (as passages of Negri & Hardt's *Empire* have done recently[30]). If anything can serve as a 'subject of resistance' at all, that might work best for a recent phenomenon that runs so orthogonal to digital culture that even the hackers don't think of as hacking—*hacktivism*.

V__ What Hackers don't call Hacking: Hacktivism

> *We are not against government, but we are for government that is representative of the needs of the people, that works to provide these needs and services for them, and that is not influenced as part of its everyday operation to meet the needs of one minority group within society—large corporations.*
>
> *—The electrohippies Manifesto*

As a practice of resistance, 'hacktivism' is a phenomenon that can be situated close to activism, but hacktivism also employs certain hacker strategies in its heavy use of technology (for example, Denial of Service attacks). Prominent hacktivist activities included the group X-Ploit's hacking of Mexico's finance ministry Website, replacing it with the face of Zapata, in sympathy with the Zapatista rebellion in the Chiapas region of Mexico; the New York Times website being replaced with a call for the release of jailed

---

[29] Slavoj Žižek, *The Ticklish Subject: The Absent Centre of Political Ontology* (London & New York: Verso, 1999) 349.

[30] See part 4.1 of Antonio Negri & Michael Hardt, *Empire* (Cambridge, Mass.: Harvard UP, 2000).

hacker Kevin Mitnick; political activists changing Indian government websites to include photos calling attention to the government-sponsored human rights violations in Kashmir; and Nike.com being 'hijacked'—the site visitors were redirected to an Australian labour rights site. As becomes apparent from this list, a practice seems to be going on that, especially as it is being contested by the 'real' hackers, deserves closer attention.

Hacktivism has its historical precursors in the beginnings of 'cultural jamming.' Critic Mark Dery describes this notion as the use of a "guerrilla semiotics—analytical techniques not unlike those employed by scholars to decipher the signs and symbols that constitute a culture's secret language."[31] Dery goes on to say that the culture jammers' question is: "Who will have access to (...) information, and on what terms? (...) In short, will the electronic frontier be wormholed with 'temporary autonomous zones' (...) or will it be subdivided and overdeveloped by what cultural critic Andrew Ross calls 'the military-industrial-media complex?'" The people first to prominently make use of this 'guerrilla semiotics' were probably Jack Napier and Irving Glikk of the Billboard Liberation Front (BLF) in San Francisco. In 1977, they started to 'improve' existing billboard messages, starting out from the insight that the internet is "a commodity which is being carved up by commercial interests more each day."[32] In their *Manifesto*, the BLF people somewhat ironically write that "the Ad holds the most esteemed position in our cosmology" and that, therefore, "to Advertise is to Exist. To Exist is to Advertise."[33] Perhaps a recent action of the BLF can illustrate this: In 1998, the group changed Apple's "Think Different" claim into "Think Disillusioned" on a famous billboard ad starring the Dalai Lama, and it altered the company's rainbow-colored apple logo into a skull. So I think it could be argued that the BLF is highly conscious of the complex Foucauldian workings of power in society: Jamming billboards, their *Manifesto* explains, is like messing with "the messenger RNA of capitalism." And it's fun, too.

The *electrohippies* are a collective that has taken such jamming practices into the datasphere. Their latest action is a 'virtual sit-in' called "Netstrike" against the Israelian government that is technically accomplished by using DoS-attacks—anyone with a modem

---

[31] http://gopher.well.sf.ca.us:70/0/cyberpunk/cultjam.txt.

[32] Jack Napier in a personal e-mail to the author from May 1, 2002.

[33] http://www.billboardliberation.com/rant/manifesto.html.

and a computer can access a site which repeatedly sends requests to the Israelian government's website until it finally crashes.[34] The *hippies*' conception of the datasphere is complex in that it includes all connected electronic media "that enable the dissemination of information and intellectual property: telephones, fax machines, information technology, radio, and the Internet." Interestingly, the collective's 'guerillia semiotics' starts out with its very name—their resignification of the term 'hippie' creates a dynamic meaning that serves well in the partly mocking and partly serious attempts to semiotically jam the datasphere. Coming from an activist background rather than a computer hobbyist scene, the *electrohippies* have an important concern that the 'real' hackers and crackers leave out: the connection between the 'real' world and the datasphere. According to the them, the "corporate forces that are damaging the world (...) are the same corporate forces that are creating this new information society because it assists their purposes. Therefore tackling the inequalities created by the new networked society before they become established is as important as tackling real world problems today."[35]

The 'hacktivismo' movement continues what might be called a notion of 'electronic civil disobedience' (ECD). The group states in their *Manifesto* that everyone shall have the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his (sic!) choice."[36] 'Electronic civil disobedience' has become a famous concept through the actions of the Zapatista movement: The Zapatista rebellion in the Chiapas region in Mexico largely depended on the use of hacker techniques and technology. With the traditional methods of public discourse being blocked or exhausted, the Zapatistas came up with the Floodnet tool, a DoS software that can be download from their website.[37] The Zapatistas and the concept of ECD also draw attention to the interplay between economical and political structures that depend heavily on the global internet: "Blocking information conduits is analogous to blocking physical locations; however, electronic blockage can cause financial stress that physical blockage cannot, and it can be

---

[34] To participate in the netstrike, direct your browser to: http://www.geocities.com/netstrike4palestine.

[35] http://www.fraw.org.uk/ehippies.

[36] http://www.hacktivismo.com/declaration_en.html.

[37] http://www.nyu.edu/projects/wray/ecd.html.

used beyond the local level."[38] So, in general, what seems to be a non-static play with technology acquires political implications in that 'hacktivism' enters and jams the terrain between the virtual and 'the real.'

* * *

What, I think, has become clear throughout this paper is that the hope that a 'post-modern' Left has projected on 'digital outlaws' (most recently in Hardt & Negri's *Empire*) such as 'ethical hackers' is somewhat problematic. Hackers as a culture are constituted by multi-layered, *imagined* communities that have divergent goals and, in part, use imagery that is questionable in that it employs again notions such as the '(digital) frontier' and the essentially open, 'vast spaces.' In addition, the American notion of the 'hacker ethic' that has recently been ascribed to the culture runs into difficulties when conceiving of the terrain that is excluded from it: crackers, 'script kiddies,' and female hackers, for example. Hacktivism, on the other hand, does enter the complex power plays within society to jam its informational channels, only that hacktivists aren't regarded as 'hackers' in the hacker scene at all. So where does that leave us at the end of this paper? In their influential book *Hegemony and Socialist Strategy*, Ernesto Laclau and Chantal Mouffe have developed a modern notion of the concept of 'hegemony.' Reading hacker culture and hacktivism in terms of this theory, it's clear that the "increasing democratization"[39] of the 'Web' means that 'web graffiti,' the Billboard Liberation Front, or projects such as the *electro-hippies*, lie entirely within the logic of hegemony in that they constitute intertwined, antagonistic movements that are spoken for and spoken about. This articulation of divergence, in Laclau's terms, brings about an experience of the "limits of all objectivity"[40] and impossibility of a fulness of hacker culture/society in the culture of hacktivism. It is within this context, then, that hacktivism as an 'art of resistance' turns out to be a performative play (Judith Butler) at a new crossroad between the political and the datasphere.

---

[38] http://www.thehacktivist.com/ecd.php.

[39] George P. Landow, *Hypertext 2.0* (Baltimore: Johns Hopkins, 1992) 277.

[40] Ernesto Laclau and Chantal Mouffe, *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics* (London: Verso, 1985) 122.

VI__ References

Anderson, Benedict. *Imagined Communities*. London & New York: Verso, 1983.

Barlow, John Perry. *The Crime and Puzzlement Manifesto.* Online. http://www.totse.com/hack/legalities_of_hacking/wholerth.html.

Cubitt, Sean. *Digital Aesthetics.* London: Sage, 1998.

Dery, Mark. *Cultural Jamming.* Online. http://gopher.well.sf.ca.us:70/0/cyberpunk/cultjam.txt.

Faase, Frans. *Analysis of the* I Love You *Virus.* Online. http://www.home.planet.nl/%7Efaase009/iloveyou.html.

Freiberger, Michael & Paul Swaine. *Fire in the Valley: The Making of the Personal Computer.* New York: McGraw-Hill, 2000.

Himanen, Pekka. *The Hacker Ethic and the Spirit of the Informaton Age.* London: Secker & Warburg, 2000.

Hopper, Ian. "Destructive *I Love You* virus strikes world wide." Online. http://www.cnn.com/2000/TECH/computing/05/04/iloveyou.01/index.html.

Kristeva, Julia. *Powers of Horror: An Essay on Abjection*. New York: Columbia UP, 1982.

Laclau, Ernesto & Chantal Mouffe. *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics.* London: Verso, 1985.

Landow, George P. *Hypertext 2.0.* Baltimore: Johns Hopkins, 1992.

Levy, Stephen. *Hackers: Heroes of the Computer Revolution*. New York: Doubleday, 1984.

The Mentor. *Hacker's Manifesto*. Online. http://www.totse.com/hack/legalities_of_hacking/manifesto.html.

Napier, Jack. *The BLF Manifesto*. Online. http://www.billboardliberation.com/rant/manifesto.html.

Negri, Antonio & Michael Hardt. *Empire*. Cambridge, Mass.: Harvard UP, 2000.

Raymond, Eric S. *The Cathedral and the Bazaar*. Sebastopol: O'Reilly, 1999.

Said, Edward. *Orientalism: Western Conceptions of the Orient*. London: Penguin, 1978.

Sterling, Bruce. *The Hacker Crackdown*. Online. http://www.mit.edu/hacker.

Žižek, Slavoj. *The Ticklish Subject*: *The Absent Centre of Political Ontology.* London & New York: Verso, 1999.