Jon McKenzie
The University of the Arts

!nt3rh4ckt!v!ty

Hacker Trading

On the morning of April 7, 1999, the stock price of PairGain Technologies Inc. suddenly rose more than 30% amid rumors that the company was being acquired by an Israeli rival, ECI Telecom Ltd. The rumor of a buy-out of PairGain had been in the air for months, but that morning it caught fire on a Yahoo! finance bulletin board (fig. 1).

Fig. 1

Stacey Lawson, a 32-year-old female IT manager from Knoxville, posted a message about the buy-out along with a link to a Bloomberg News page that announced the story as well as quotations from the CEOs of PairGain and ECI. As rumors are wont to do, the story of the buy-out traveled quickly, accelerated by cutting-edge information technology—there were mass e-mailings via a Web service called Hotmail—and by good old fashioned speculative greed. In a short time, the price of PairGain skyrocketed and over 13 million shares of PairGain were traded that day on NASDAQ, about 700% higher than its daily average.

But something was amiss. Investigators from NASDAQ and the Securities and Exchange Commission (SEC) suspected insider trading—in this case, insider information being leaked in order to dramatically increase the stock's value. The management of PairGain and ECI were contacted, but both denied being involved in any negotiations. For its part, Bloomberg News also denied knowledge of the buy-out, and it was discovered that the report had actually been published on Angelfire.com, a site operated by Lycos. Smelling a hoax, investigators turned to Angelfire and to the Yahoo! bulletin board and started sniffing out the remnants of electronic shenanigans and digital chit-chat. Someone had apparently downloaded graphics from Bloomberg.com and used them to create a bogus Web page reporting the buy-out; next a message was posted on Yahoo! with the link to the bogus news report and mass e-mails were launched through Hotmail.

The FBI was called in, though by then the ploy's plot had become clear: invest in PairGain at one price, start a buy-out rumor using Hotmail and Yahoo!, "sub-

Fig. 2

stantiate" it with a "news report," all in order to drive up the stock's price, and then make a tidy profit by selling it off. By noon of the same day, news of the hoax had brought PairGain's price back down (though it ended the day up nearly 10%). A few days later, the gig was really up. Following the trail of IP addresses left at the sites of the hacks, FBI agents closed in on Gary Dale Hoke, a 25-year-old, mid-level engineer employed at PairGain's Raleigh, NC, operation. He was arrested and charged with securities fraud. In June, Hoke pleaded guilty. He apparently acted alone.

Hoke's hoax made headlines in both traditional and online media, and morals were quickly drawn up: old tricks can find new outlets—and new suckers—on the Web, and covering your tracks in cyberspace is harder than you might think. But there are other lessons as well. Hoke's stated motive, for instance, was hardly illegal: personal gain, the maximization of profit, is considered a prime mover of stock market speculation. What was illegal were his means: the fraudulent dissemination of securities information. For those of us interested in interactivity—which may be situated at the limen of social and technological performance—the most pertinent lessons of the PairGain hoax lie in his techniques, namely, the creation of a digital avatar (an alias of Hoke, Stacey Lawson enjoys tennis, dancing and water sports), the mimicry of a report by a leading financial news source ("ECI Telecom and PairGain Technologies, Inc. today jointly announced that they have entered into a definitive agreement"), the rumorological use of bulletin board and e-mail services ("GO PAIR!!!!")—and, perhaps most importantly, in the speed and ease with which all these techniques broke down.

Hoke had applied his knowledge of online communities, telecom companies, and interactive multimedia in a project designed to hack his way to riches. In terms of this objective, he failed miserably, for not only will he do time in prison, his plea bargain commits him to repay millions of dollars to investors who lost money trading PairGain that day. But it appears he did gain something: a place in interactive history. Though the SEC had previously brought charges against online investment sites for the practice of "pumping and dumping" (driving up prices and then unloading stocks), Hoke will likely go down as the first person to commit this brand of security fraud. He may be the world's first hacker trader.

Interhacktivity

In these pages, I will explore a certain combination of interactivity and hacking. Restricting myself to the domain of the World Wide Web, I will examine this combination under the term *interhacktivity*. What is interhacktivity? To flesh out a

response to this question, let's begin by examining its components.

Web interactivity is often approached as a rather intimate exchange between an individual and a Web site, the reciprocal feedback of human and computer behaviors. Even critiques of interactive alienation presuppose its intimacy. And, indeed, today's computer and Web developers seek to make interactivity as individualized as possible. Drawing upon decades of research in human-computer interaction, they strive to create highly personalized interactions and unique online experiences. The entire new media industry—which includes Web developers, software companies, game developers, computer and telecommunication companies—has put into gear a shift called for years ago by Brenda Laurel: to move from engineering interfaces to designing experiences. The result: at decade's end, Web interactivity is more humanistic, more artistic, and much, much more profitable.

But clicked into from another window, custom interfaces and personal experiences can be reloaded in different way: as highly orchestrated, highly replicable productions, something else new media companies know quite intimately since their business consists precisely of teams of corporate execs, programmers, engineers, researchers, designers, writers, and production managers, all working together to create these intimate interactions.

Produced along the borders of cultural and technological systems, Web interactivity is a sociotechnical performance before it is a human-computer interaction. Executives sign deals, engineers build systems, programmers hack code, producers pull it all off. Interactive scenarios arise from decisions about a Web site's audience and functionality, about the "branding" of product and personal identities and the "look and feel" of their interactivity. To pregauge user interests and activity, researchers study related sites and may conduct surveys, interviews, and usability tests with in-house or specially-selected groups. Results are fed back into the user experience scenarios, which are refined as information architects design site structure and navigation paths, and these scenarios take shape as content strategists and information designers determine what information appears on each page and how it is presented. "Creatives"—multimedia artists, graphic designers, and writers—generate the sights and sounds and texts that animate the experience (or not). And last but not least, indeed, first and foremost, programmers and engineers craft the codes and systems through which people and machines digitally interact on the Web. In short, while one can theorize interactivity as the exchange of inputs and outputs or stimuli and response, or, more poetically, as the co-creation of a unique experience between a person and a computer, there is no human-computer interaction that does not presuppose complex social and technological networks, and, with them, the values and power setups they enable and are enabled by.

It is precisely at this level that interactivity is hacked. The terms "hacker," "hacking," and "hack" all vary widely in their deployment. "Hacker" can be fairly inclusive, referring to any computer programmer, and "hacking" may be used to mean simply writing code. Yet the terms "hacker," "hacking," and "hack" can also

be very exclusive in their semantic range. Within the programming community, for instance, the term "hack" can refer to an inelegant, very effective, solution to a difficult programming problem. Hacks are mediocre, *ad hoc* responses or, if you prefer, *ad hack* solutions to situations that really require more creative rewriting of a program. But a hack can also be just the opposite: a brilliant bit of code.

And there's another, far more widely-used, sense of hacking, one that, while still more exclusive than the original meaning, has entered into popular culture. Here hacking has become the digital version of breaking and entering—for starters—for it often refers to illegally gaining entrance to a computer system, such as a public Web server or a private communications network, and then violating its databases or applications. A hacker in this sense is no longer someone who "simply" writes computer code. It's someone who infiltrates or "cracks" the programs and files of others. Within the hacker community, some distinguish hackers from crackers, defining hacker as one who writes code, and cracker as one who breaks or cracks them. These cracker hackers can and do write code, but their hacks are produced to get around firewalls, download documents, replace files, overwrite data, and/or overload entire computer and communication systems.

Combining this last sense of hacking with the notion that interactivity is a sociotechnical performance, we can define interhacktivity as interactivity that has been hacked, or has as its goal some sort of hacking. Coming at it from the other end, interhacktivity is hacking that focuses specifically on the interactivity between humans and computers. It is hacking that not only takes aim at technical systems, *but also targets social systems*. As such, interhacktivity shares certain affinities with propaganda, political discourse, consumer marketing, psychological warfare, education, activism, and confidence games. (A hack can also be a prank.)

As an emblem of interhacktivity, the PairGain hoax involved using specific technical practices (e.g., the creation of a bogus news site and mass e-mailings) in order to hack a specific community, the users of the Yahoo! bulletin board and, more broadly, investors who utilize the Web as part of their speculative strategy. Hoke had planned his scam for two months before putting it into action, and he chose his targets carefully. Yahoo! is one of the web's most popular portal or entry sites, and as such, its bulletin boards have a huge user base. His e-mails were also strategically targeted, being sent out to money managers and trading desks. Most importantly, Hoke sought to exploit the inherent rumorological tendencies of the investment community. He did not actually start the rumor of a PairGain buy-out; he merely simulated its confirmation and then sat back to capitalize on the speculative effects of this simulation.

In a sense, Hoke's interhacktivity drew upon an existing sociotechnical system in order to create a quasi-autonomous economy, one that, for a short time a least, performed better than he himself had foreseen. But in the end, he didn't capitalize on his scam. Though Hoke owned PairGain stock, its performance alarmed him and he didn't push the sell button. According to Christopher Painter, an assistant

U.S. attorney, "Things got set in motion and he got cold feet" (cited by Gaw). His interhacktive system had frozen up.

Interhacktivities, Major and Minor

Perhaps the question is not really "what is interactivity?" or "what is hacking?" or even "what is interhacktivity?" Rather, the most pressing query may be "which one?" For there are interactivities and interactivities, hacks and hacks, interhacktivities and interhacktivities. All are multiple and divided, for all are marked by internal differences, external situations, diverse evaluations and multiple power plays. Which interactivity? Which hack? Which interhacktivity? The challenge lies in sorting them all out while also engaging them critically and creatively.

Here Deleuze and Guattari's distinction between major and minor becomes pertinent. "Major" and "minor" are terms they introduce to distinguish normative and mutational processes in art, science, and society at large. A major art, a major science, a major language is one that dominates a given sociotechnical system or tradition. The major is filled with Great Works, Great Men, Great Events. The minor, however, works against but also within the major. In theorizing the minor literature of Kafka, for instance, Deleuze and Guattari investigate (1) how Kafka experiments upon the major languages used in his native Czechoslovakia, transforming its senses into new and strange intensities; (2) how such experimentation is necessary but insufficient if it does not connect to a political immediacy; and (3) how Kafka's writing functions not so much as a social critique but as a "relay for a revolutionary machine-to-come," as a collective assemblage of enunciation already in contact with the future (16-18). Risks arise at each of these levels, not the least of which is falling back into the reading machines of major literature—its canons and periods, its genres and authorities. Not only can a major language become minor, a minor literature can also be made major.

This distinction between major and minor opens up several possibilities for theorizing interhacktivity. We can define the Internet's rapid (and some would say complete) commercialization since the Web's arrival as the emergence and consolidation of a major interactivity, the establishment of dominant communication channels and standards of behavior—both human and computer. What began as a national security project, matured as a research network, and then blossomed strangely, briefly, in Mosaic bits of HTML, today finds itself overgrown by its progeny: e-commerce, webcasts, personalized experiences, transactivity.[1] The scripting of user scenarios, the customizing of pages, the targeting of banner ads, the "driving" of content to users—such practices are coming to define Web interactivity. But this major interactivity is also shaped by other sociotechnical systems clustered around the Web, such as "traditional" media (especially television and telephonics), the stock market (especially the technology-ladened NASDAQ), and state governments (particularly that of the United States).

From this perspective, interhacktivity is a form of minor interactivity. By

hacking into the major interactive practices promoted by internet service providers, corporate sites, and portal search engines, interhacktivity seeks to disrupt technical systems and detour the social experiences of users. Their codes are decoded and scrambled, their standard performances altered, sociotechnical systems may become disoriented, function wildly, even crash. The PairGain hoax, with its breach of security measures, its miming of discourses and practices, and its intervention in not one but several communities—offers an example of minor interactivity.

Yet from another perspective, we can ask to what extent Dale Hoke's scheme constitutes a minor interactivity. He no doubt experimented with the discourse and practices of a recently established yet powerful sociotechnical system. But that's as far as this interhacktive intervention went. There is no evidence that Hoke sought to connect his experimentation to any political situation, much less use it to construct an assemblage that tunes in futural arrangements of power and resistance. This comes as no surprise, given Hoke's apparent motive of personal financial gain. So rather than simply define interhacktivity as minor interactivity, it may be more productive to also distinguish between major and minor interhacktivities.

Major interhacktivity involves hacking the interactive network of a sociotechnical system, but that involvement either fails to challenge dominant societal norms or conforms to them, whether implicitly or explicitly. The PairGain hoax now offers itself as an example of major interhacktivity. Hoke recombined a number of existing discourses and practices to intervene in the sociotechnics of computer-enhanced investing. But although his hacking of an interactive network did violate a number of its protocols (and a Federal law), it did not transgress its underlying norm, a norm that increasingly characterizes more and more of American society: to make a profit in the stock market.

By contrast, minor interhacktivity entails hacking the interactive workings of sociotechnical systems in order to challenge repressive situations and the norms that help produce them. One recent site of minor interhacktivity was the Bhabha Atomic Research Centre (BARC), India's premiere nuclear research facility. BARC had been crucial in the recent development of that country's atomic bomb capability, and shortly after the Indian government's series of five underground nuclear tests in May 1998, the site was infiltrated by first one, then two, then legions of hackers.

Apparently, the first to enter was a certain t3k-9 (read "tech-nine"), a fifteen-year-old American who after learning of the nuclear tests on TV searched the Web and discovered the BARC Web site. Using a password cracker program, t3k-9 "cracked" into BARC's supposedly secure server in less than a minute. Once inside, t3k-9 then downloaded all the passwords and log-in names, some e-mail messages, and one souvenir scientific document, and, before leaving, erased all tell-tale electronic footprints. T3k-9 also created a "backdoor" that would allow easy reentry. A short time later, t3k-9 confided the hack to an online friend and fellow hacker named IronLogik.

IronLogik, an eighteen-year-old Serbian immigrant living in the United States,

carefully prepared his entrance into BARC by threading his way through numerous corporate, government, and military sites. He even picked up a new IP address from Los Alamos before using t3k-9's backdoor to enter the BARC servers. Once inside, IronLogik established himself as a virtual system administrator, gaining almost total control of the network. He downloaded some e-mail and listened in on a few online conversations. Though he was tempted to enter BARC's internal intranet—where the highly sensitive material would be stored—IronLogik decided the risks were too great.[2]

Meanwhile, t3k-9 had posted the entire BARC password file, some 800 passwords, to other hackers. They wasted little time in entering the research facility's computer system. One group, named milw0rm, methodically wreaked havoc on the system, and in doing so went public with the BARC hack. Milw0rm is composed of teenage hackers who live in England, the Neatherlands, New Zealand, and the United States. Soon after t3k-9 posted the password list, milw0rm entered BARC and over the course of a few days gained control of six of its eight servers. Not content to lurk around the system, they also downloaded e-mail, but went a few steps further. The group erased the data on two servers and replaced BARC's homepage with one of their own design (fig. 3). It contained a message to the nation of India.

The full text reads:

> oh gn0, like this is what happens if j00 play with atomic energy!#@!
>
> It g0es b00m@#@#@# so PLEEEZE, do not fuck around, didn't you parents ever teach you manners?
>
> I like the world in its current state (i guess), well its better than the world would be if the b0mb went b00m.
>
> think about it k1dz, its not clever, its not big, so don't think destruction is cool, coz its not.

Fig. 3

If a nuclear war does start, you will be the first to scream.

You all saw the movie WARGAMES right? well. . . . That could have been us$#@

So India, LISTEN TO WISE OLD MILW0RM. . . . You do not need nuclear weapons in the 1990s!#@!

STOP THE SH1T

0wned

Savec0re - JF - VeNoMouS

JF - Hamst0r - Keystoke - savec0re - ExtreemUK

The Nuclear p0wer 0wn1ng spree continues.[3]

Milw0rm's hack reverberated across diverse sociotechnical systems, not only those of BARC and other nuclear research facilities, but also intelligence agencies and diplomatic corps, arms control and activist communities, states and peoples, all of them communicating and interacting over the same network. In a June 3, 1998, interview, milw0rm members savec0re, VeNeMouS, and JF stated that they had entered the site through its Sendmail program and reiterated their protest against the Indian government's nuclear tests. "I'm just sick of nuclear shit," said VeNeMouS. The three also threatened to infiltrate the Pakistani government sites as well.

After first denying the hacks, BARC officials the next day confirmed that their computer systems had been infiltrated over five megabytes of e-mail and downloaded. BARC also announced that a second group of hackers had attacked the Web site, this time leaving this message: "This page has been hacked in protest of a nuclear race between India, Pakistan and China. It is the world's concern that such actions must be put to end since, nobody wants yet another world war. I hope you understand that our intentions were good, thus no damage has been done to this system. No files have been copied or deleted, and main file has been just renamed." BARC closed down its site temporarily and upgraded its security.

The cracking of Bhabha Atomic Research Centre generated countermeasures elsewhere and unleashed heated debate about nuclear proliferation, cyberterrorism, information security, and hacker ethics. The U.S. Army issued a warning to its own information systems managers to monitor and block suspected IP addresses identified in the BARC hack. An editorial by ZDNet, a popular site that also houses Inter@ctive Week, denounced the hackers' actions on the grounds that they had denied information to U.S. intelligence agencies while benefiting the "real terrorists."[4] For their part, milw0rm members stated that their purpose was to draw attention to the lax security around some nuclear research sites. "If you're gonna amass data which can take [so] many lives," said savec0re, "at least secure it." The hacker and activist communities were each divided, programmers over whether the hacker ethics (in two tablets: "information wants to be free" and "thou shall not destroy data") had or had not been violated, the activists over the hack's overall efficacy as well as the electronics of "by-any-means-necessary." Even the hacktivists who cracked BARC were split. IronLogik disparaged milw0rm for destroying documents, defacing the

homepage, and taking credit due to himself and t3k-9,

The BARC and PairGain incidents are both highly interhacktive. In each case, codes and behaviors of specific infrastructures were cracked in order to hack the words and behaviors of their social interactors. In each case, a hacking of interactivity occurred that altered, however briefly, one or more sociotechnical systems. Beyond this, however, the two hacks diverge, allowing us to flesh out major and minor interhacktivities in more detail. With PairGain, the hack created a small, detoured market for the purpose of making some tidy profits, while at BARC the hack took over the controls of a government computer facility in order to protest the facility's role in nuclear weapons tests. Unlike the PairGain hoax, the BARC incident connected to an immediate political situation—the arms race in Asia and the world. Milw0rm attempted to maintain the protest's momentum by a "mass hack," replacing some 300 homepages (ranging from business and sports sites, to porn and fan sites) with a protest page. It is this linking, this seizing of a political moment, that marks minor interhacktivity.

Performative Power and Interhacktivism

The question "what is interhacktivity" opens up into another: "which interhacktivity?" But we might also ask: *why interhacktivity*? What's the attraction, what's the point, or, rather, the angle of interhacktivity, of interactivities that hack other interactivities? And why interhacktivity *now*?

The emergence of interhacktivity must be situated in terms of a fundamental shift in knowledge and power. The disciplinary formation analyzed by Foucault emerged in the eighteenth century and has lingered far into the twentieth. But since the Second World War, it has steadily been displaced by another. While discipline was based on training physical bodies in discrete institutions—schools, factories, prisons, etc.—that were all governed by discourses of the enlightenment, this new power/knowledge upgrades all bodies with a digital *doppelgänger*, a body of information electronically shared by networks of overlapping institutions. At the level of discourse, the enlightenment's grand narratives of Progress and Liberation have been overtaken by the discourse of sociotechnical systems. In 1984, Lyotard named this formation "performativity." "In matters of social justice and of scientific truth alike, the legitimation of that power is based on its optimizing the system's performance—efficiency" (xxiv). As far back as 1955, Marcuse argued that postindustrial societies were governed by the techno-rationality of "the performance principle." Since then, there have emerged paradigms of research into cultural, organizational, technological, and financial performance: artists, executives, computers, and stock markets all perform, though in very different ways. Beneath them all, however, lies what I call the performance stratum. Performance is to the twentieth and twenty-first centuries what discipline was to the eighteenth and nineteenth: a historical stratum of power and knowledge.[5]

Interhacktivity, hacking, interactivity: all must be understood as effects of per-

formative power—and as its potential instruments. There is a challenge or demand for individuals, groups, and entire nations to get their act together, to get interactive, to get wired, to get on the World Wide Web—or get left behind. It's nothing personal, really, just the personalized interface of dominant sociotechnical systems. Web interactivity emerges not only from the computer's hypertextual multimedia, but also from the ability to switch quickly between social systems, an ability made possible by communication networks. As such, major interactivity feeds into and out of the multitasking performed in turn-of-the-millennium workplaces, as well as the channel-surfing and role-playing performed in contemporary living rooms and boudoirs. Work and play, all of life comes under the demand to perform—or else. Hacking, from coding to cracking, is a crucial conduit of this challenge, for computer networks are the panopticons of the performance stratum and "1"s and "0"s the units of its normative code. The place of sedentary discipline has been occupied and displaced by the nomadic power of performance, and this power is wiring around the world.

Yet as the site of power moves from physical locations into digital networks and as universal knowledge gives way to situated knowledges, new forms of resistance also emerge. Long-entrenched practices of political activism—street protests, strikes, sit-ins, boycotts—are becoming less and less effective and in their place have arisen practices of "electronic civil disobedience" and "hacktivism." Critical Art Ensemble puts the difference between traditional civil disobedience (CD) and electronic civil disobedience (ECD) this way: "ECD is a nonviolent activity by its very nature, since the oppositional forces never physically confront one another. As in CD, the primary practices of ECD are trespass and blockage. Exits, entrances, conduits and other key spaces must be occupied by the contestational force in order to bring pressure on legitimized institutions engage in unethical or criminal actions. [. . .] ECD is CD reinvigorated. What CD once was, ECD is now" (18). Both traditional and electronic civil disobedience are nonviolent, noncriminal activities, but while the first relied on grass-roots communities, the second depends on transitory coalitions.

In the wake of BARC and other related incidents, the term "hacktivism" has emerged to describe the growing number of coalitions between computerized activists and politicized hackers. Hacktivism has thus far relied primarily on tactics of trespass and blockage. But Stefan Wray warns against defining hacktivism too definitively: "at this point there is no consensus or agreement. Maybe the entire notion of hacktivism confuses and challenges sets of values and hacker codes of ethics. Quite possibly there is some re-thinking happening and we might begin to see a new set of ethical codes for hacking." He nonetheless defines hacktivism as localized events ranging from "relatively harmless computerized activism to potentially dangerous resistance to future war," while suggesting that it could be subsumed in a generalized resistance occurring at different locations and levels of activity. The name of that generalized resistance might be minor interhacktivity or

interhacktivism, the challenging of the challenge to perform or else.

Milw0rm has been called a hacktivist group, as has another group, the Electronic Disturbance Theater, of which Wray is a founding member. Like milw0rm, Electronic Disturbance Theater (EDT) has been involved in a number of interhacktivist incidents. While EDT also hacks sociotechnical systems, their interhacktivity has centered on the plight of indigenous peoples of Chiapas, Mexico, as well as a computer program called FloodNet. Inspired by the use of electronic media by Zapatista rebels in Chiapas, EDT came together as a group to conduct acts of electronic civil disobedience and has launched numerous hacks against selected Web sites.

Unlike milw0rm's mass hack, in which a few crackers attacked many sites, EDT's minor interhacktivity involves many people protesting a few sites. For this purpose, EDT member Bret Stalbaum created FloodNet, a Java applet designed to overload Web servers. FloodNet causes targeted pages to reload automatically, over and over and over. A handful of FloodNet users might have little effect on a server's performance; thousands of users acting simultaneously, however, could effectively overload a system. The MO of EDT is thus to stage virtual sit-ins using the interhacktive potential of the Web.

On April 10, 1998, EDT organized a virtual sit-in against the Mexican government (fig. 4). The event was publicized on the internet before rather than after the hack, as EDT invited anyone interested in participating to visit the EDT Web site. This site contained the FloodNet interface and, through it, visitors interhacked with the targeted site, the homepage of Mexican President Ernesto Zedillo. EDT later announced that more that 8,000 international participates took part in this first tactical use of FloodNet. "The Web site of an institution or symbol of Mexican neo-liberalism is targeted on a particular day. A link to FloodNet is then posted in a public call for participation in the tactical strike. Netsurfers follow this link; then simply leaving their browser open will automatically reload the target webpage every few seconds. The intent is to disrupt access to the targeted Web site by flooding the host server with requests for that Web site" ("Tactical").

On June 18, 1999, EDT staged their latest virtual sit-in, this time targeting six separate sites, those of Bolsa Mexicana de Valores, Grupo Financiero Bital, Grupo Financiero Bancomer, Banco de Mexico, Banamex, and the SOA. As in the protest directed at President Zedillo's Web site, participants visited the EDT site and followed instructions for setting up their browsers. They then used an online

Fig. 4

form to choose the site they wished to target, write in their own brief message, and send it on (fig. 5). During the six hour protest, FloodNet sent their message to the targeted site for as long as the user kept her or his browser open. During this recent protest, EDT reports that there were over 18,000 requests made from 46 countries.

EDT also reports that some 1,300 requests were made that day from .mil addresses in the U.S., in other words, from American military computers, including those of DISA, the Defense Information Systems Agency. EDT and DISA are well acquainted, the hacktivist group having gained the agency's attention for their actions against President Zedillo and for targeting the White House and the Pentagon to protest the U.S. government's support of the Mexican state. The military visitors were apparently monitoring the virtual sit-in and, according to EDT, inadvertently joined it.

The Department of Defense (DoD) has likewise gotten the attention of Electronic Disturbance Theater. In September of 1998, after EDT had announced it would stage a virtual sit-in of the Pentagon, DoD was ready and waiting with a counter-measure. According to Susan Hansen, a Pentagon spokesperson, "The Defense Department was aware of the group's threat, and we did take actions" (cited in Friel). Those actions involved "Hostile Applet," a Java script developed by DoD specifically to combat FloodNet. When FloodNet users tried to access the Pentagon servers, the government machines detected the attempt and responded by blocking access and returning fire with Hostile Applet. EDT reports that upon activation, "the Pentagon site would open the same blank window over and again on the FloodNet user's browser. This crashed the browser instantly" ("Countermeasures"). According to EDT member Ricardo Domingeuz, on some systems flying coffee cups appeared along with the words "ack, ack," allusions to the Java script and the sound of anti-aircraft guns.[6]

While EDT's virtual sit-ins provide an example of hacktivism, the DoD response can be read as an act of counter-hacktivism. Some have argued that DoD's use of Hostile Applet was an illegal act, as DoD acted against U.S. citizens; others have questioned what this action portends for the future of privacy on the Web. Through programs such as DISA, the U.S. government is undoubtedly developing other

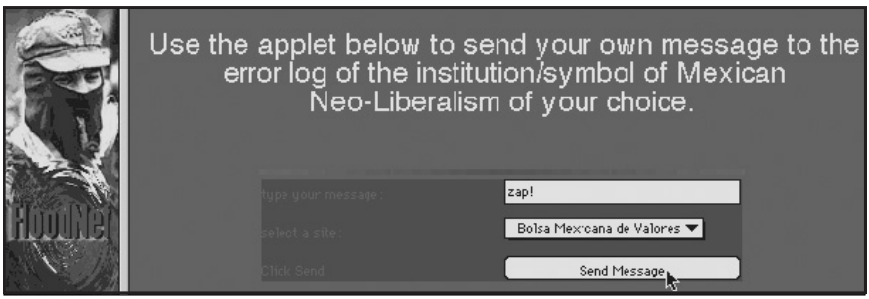

Fig. 5

counter-measures to what it perceives as a threat to national security. At the same time, EDT's use of FloodNet has also been criticized. Participants of these virtual sit-ins risk having their IP addresses collected by authorities and having their systems crashed. In addition, the very effectiveness of FloodNet depends on slowing down traffic on the internet. EDT has responded to these criticisms by pointing out that analogous risks are run with tradition civil disobedience tactics. All these arguments and counter-arguments suggest one thing: look for more confrontations between major and minor interhacktivities.

!nt3rh4ckt!v!ty

In these pages I have tried to crack the concept that interactivity is primarily a matter of human-computer interaction. Interactivity is always already socio-technical. It takes place not only at the interface between a person and a personal computer, but also at the contested borders of social and technological systems. Further, I have argued that interactivity must also be situated in terms of an emergent formation of power and knowledge, what I call the performance stratum. The power of performance is virtual and nomadic rather than actual and sedentary, and interactivity embodies this virtuality and nomadicity. *There is a demand to become interactive*, to become wired, to multitask, channel surf, and navigate quickly among different systems. At the same time, I have suggested that along side the power of performance there arises new forms of resistance, and it is here that the notion of interhacktivity becomes most interesting.

Interhacktivity refers to hacking that tampers with interactivity, that targets technical systems as a means of affecting social systems. But there are interactive hacks and interactive hacks, so I have sought to distinguish them in terms of major and minor interhacktivites. Major interhacktivities, such as the PairGain hoax, may experiment with discourses and practices and, as with the DoD Hostile Applet, may even connect to a political situation, but they do so to bolster dominant social norms and events. By contrast, minor interhacktivities, such as those of milw0rm (fig. 6) and Electronic Disturbance Theater, utilize technical experimentation and political linkage in order to challenge such norms and events. But what most distinguishes minor interhacktivities—not only from their major analogs but also from one another—is their attempt to create a collective machine for generating radically new discourses and practices, resistant words and political actions that belong to the future as much as the present.

I'd like to close by briefly considering the collective machines generated by milw0rm and EDT. As mentioned earlier, milw0rm followed up their cracking of the BARC servers with a mass hack that replaced 300 homepages with a single anti-nuclear, pro-peace page. But though they successfully infiltrated diverse socio-technical systems, the collective machine milw0rm created basically functioned as a postal service: it delivered a message. Political as this message was, its efficacy remained very limited, for recipients were given no means of taking action against

the Indian and Pakistani institutions denounced by milw0rm. The mass hack may have disrupted some servers, but it did not serve to create a collective machine through which others could channel forces of the future and, as milw0rm sought, put "the power back in the hands of the people."

EDT was much more successful in building a futural collective machine. FloodNet provided a means for thousands to take action against specific sociotechnical systems. Users not only received messages and information about the situation in Chiapas, they could compose and send their own messages to the institutions in question. But the messages were really less important than their *sending*, their flooding and overloading of the targeted servers, where they functioned as search queries posted over and over again. In fact, as EDT points out, few if any people were likely actually to read the messages. The search results would likely appear

Fig. 6

only in the error logs, usually accessible only to system administers. In this respect, EDT suggests that FloodNet can also be read as a work of conceptual art. Imagine that the message you sent was simply "human rights." Posted again and again to the server's search engine, it might be received as:

<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server

<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server
<human_rights> not found on this server

In this case, the message would be an accurate descriptive statement of the affected sociotechnical system. But, again, what's crucial in minor interhacktivity is not the radical messages themselves; rather, it's the construction of a new interactive machine. Taking a cue from milw0rm's messages of mixed characters and, more generally, the crackers' penchant for alphapunctnumerical writing, I'll sign off by retagging the object of my interests here: the name of this futural machine is !nt3rh4ckt!v!ty.

Notes

[1] "Transactivity" refers to interactive economic transactions, such as buying a book at Amazon.com or trading stock online at E*trade.

[2] My primary source for this information on t3k-9 and IronLogik is Adam L. Penenberg's article "Hacking Bhabha." Penenberg interviewed t3k-9 and IronLogik in an Internet Relay Chat, a forum in which it is nearly impossible for anyone to trace its participants.

[3] JF, "Badaboom? BIG BADABOOM!!"

[4] Ira Winkler writes: "The hackers supposedly broke in as a protest against India's nuclear tests. But all it's done is let India know that its computers are vulnerable. Oh, that really hurt India. That hack has, however, denied intelligence agencies worldwide a source of valuable data. [. . .] Legitimate hackers get lumped together with nuclear terrorists; the real terrorists get a better road map for nuclear weapon information."

[5] I examine this formation in "Laurie Anderson for Dummies" and in the forthcoming text *"Perform or Else: Performance, Technology, and the Lecture Machine*." Marcuse's theory of the performance principle is found in *Eros and Civilization*. Deleuze discusses the shift from discipline to what he calls "control" in "Postscript to the Societies of Control."

[6] Personal e-mail with the author.

Works Cited

Critical Art Ensemble. *The Electronic Disturbance*. Brooklyn, NY: Autonomedia, 1994.

Deleuze, Gilles. "Postscript to the Societies of Control." October 59: 3-7.

___, and Félix Guattari. *Kafka: Toward a Minor Literature*. Trans. Dana Polan.

Minneapolis: U of Minnesota P, 1986.

Domingeuz, Ricardo. E-mail correspondence. 24 June 1999.

Electronic Disturbance Theater. "Countermeasures." <http://www.thing.net/~rdom/zapsTactical/countrmesr. htm>.

___. "Tactical FloodNet Brief Description." <http://www.thing.net/~rdom/zapsTactical/workings.htm>.

Friel, Brian. "DoD launches Internet Counterattack." *GovExec.com*. 18 September 1998. <http://www.govexec. com/dailyfed/0998/091898b1.htm>.

Gaw, Jonathan. "N.C. Man Pleads Guilty in Online Securities Hoax." *latimes.com*. 22 June 1999. <http://www.latimes.com/HOME/BUSINESS/WALLSTCA/t000056019.htm>.

JF, hacked homepage. "Badaboom? BIG BADABOOM!!" Archived on Antionline. <http://www.antionline.com/ archives/pages/www.barc.ernet.in/>.

Lyotard, Jean-François. *The Postmodern Condition: A Report on Knowledge.* Trans. Geoff Bennington and Brian Massumi. Minneapolis: U of Minnesota P, 1979.

Marcurse, Herbert. 1955. *Eros and Civilization: A Philosophical Inquiry into Freud.* New York: Vintage. 1961.

McKenzie, Jon. "Laurie Anderson for Dummies." *The Drama Review* 41.2 (Summer 1997): 30-50.

McKenzie, Jon. *Perform or Else: Performance, Technology, and the Lecture Machine.* Manuscript.

Penenberg, Adam L. "Hacking Bhabha." *Forbes.com*. 16 November 1998.<http://www.forbes.com/tool/html/98/nov/1116/feat.htm>.

Winkler, Ira. "Hackers Can't Play 007: How Meddling Amateur 'Spies' Can Endanger National Security." *ZDTV*. 17 June 1998. <http://www.zdnet.com/zdtv/cybercrime/spyfiles/story/0,3700,2113079,00.html>.

Wray, Stefan. "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics." November 1998. <http://www.nyu.edu/projects/wray/wwwhack.html>.