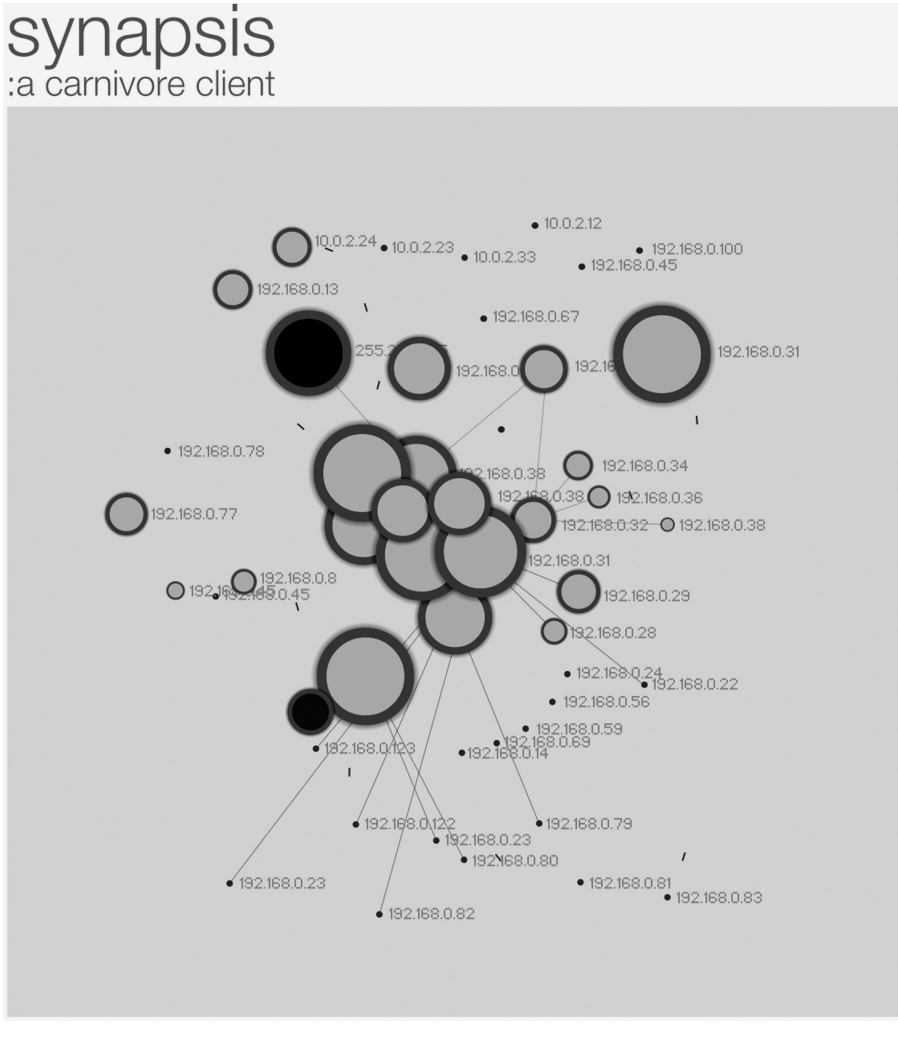
Marcos Weskamp.
Synapsis: A Carnivore Client,
2003.



Terror and Play, or What Was Hacktivism?

PETER KRAPP

As we witness numerous governmental and corporate initiatives around the globe to restrain the free use of networked computers, knowledge and discussion about these and parallel measures is increasingly withdrawn from public discourse.[1] Social power is already so diffuse that Adam Smith's market metaphor of the invisible hand has become pure nostalgia. Authoritative power is dispersed as global organizations transition from corporations to networks, and citizens of information society are governed less by concentrated coercion and more by ideological power, as manifest in the symbolic practices and norms of cyberspace.[2] But at the same time, media policy is increasingly determined exclusively by profit-oriented actors, transforming the legal and political frame of cyberspace. These developments may soon have put an end to critical media practice and conceptual Net art. Once the "cyber-terror" scenario comprises any use of technology to disrupt, sidestep, destabilize, or subvert officially condoned user interfaces with technology, the tropes of computer culture as the triumph of bricolage will have been criminalized.

Pop culture no longer celebrates hacking as the generally innocuous but occasionally very profitable pursuits of the computer hobbyist. As television has stopped romanticizing the obsessions of talented nerds, the press no longer touts the boot-strapping spirit of digital capitalism. Instead, TV and print journalists have been selling the specter of hacktivism as an irreducible systemic threat of digital media. To comprehend the precarious balance of secrecy and access in information policy, it is necessary to combine psychological, theoretical, and technical insight, as Claude Shannon has already emphasized.[3] This essay takes issue with three of the most unfortunate misunderstandings in that standoff between old and new media. First, hackers tend to be portrayed as immature scofflaws, and the remedy usually sought is greater disciplining power for the authorities, with the inevitable backlash. Second, once the protection of privacy and free speech is hollowed out by surreptitious data mining and invasions of data privacy, activism becomes all too easily equated with cyber-terrorism, turning into enemies of the state anyone who dares question some of the more insidious consequences of a pervasive commodification of the network. Third, the assertion that greater secrecy ultimately yields

greater security is wrong, and the cult of secrecy leads to a global resurgence of irrational rumorology online. When conspiracy theory takes the place of critical Net culture, public debate over code and law is impoverished.

Network, Power

Expressive politics is the struggle to free what can be free from both versions of the commodity form—its totalising market form, and its bureaucratic state form.
—McKenzie Wark

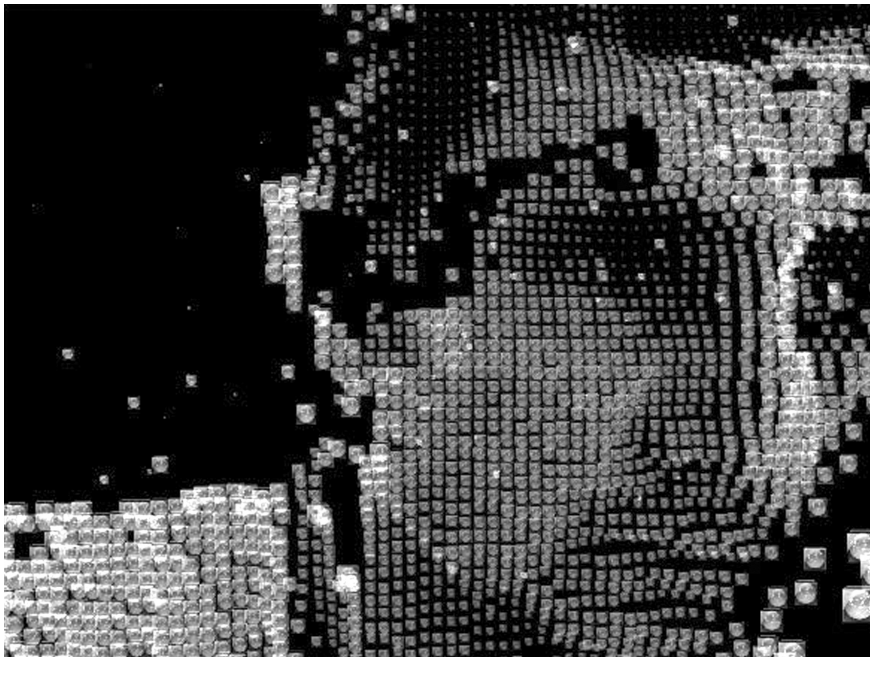
If in the past few years one wanted to follow nuclear tests in India, the fate of indigenous Mexicans in Chiapas, protests against the World Trade Organization or demonstrations against the Republican National Convention, one was underserved by TV and print journalism and probably turned to the Internet. Energy activists, sympathizers of the Zapatistas, antiglobalization protesters and other groups likewise sought to attract attention to their causes by means of disrupting or defacing Web sites associated with Indian physics research, the Mexican government, the World Trade Organization, or conservative think tanks. Internet users alerted to the concept of Echelon, an electronic communications scanner filtering any and all satellite, microwave, cellular, and fiber-optic traffic, had to wonder why, and how, capitalism had morphed into a fully integrated surveillance apparatus that could treat the world like a company town. To pull the veil of secrecy and ignorance aside, activists coined the notion of Jam Echelon Day, trying to disrupt the surveillance and alert the public to its presence in one stroke. Chinese computer hackers launched attacks on U.S. Web sites in protest against NATO's bombing of a Chinese embassy in the Kosovo war. Sweatshop critics, techno-libertarians unhappy with certain politicians, and people harboring curiosity or vested interests in commercial, military, or trivial secrets stretch the limits of the legal in cyberspace every day. A concerted denial-of-service attack on American e-commerce Web sites in February 2000 coincided with an atmosphere of growing unease about the dot-com boom—on the sides of those who knew nothing about it and of those who lived by it. The attack meant less online shopping for a few hours—but the story made the covers of half a dozen weekly magazines and numerous daily papers.[4] The media were eager to characterize companies like Yahoo and eBay as victims "crippled" by the dastardly work of "vandals"; it did not matter that no permanent damage was done to these sites. To threaten the giant shopping-channel-experiment-on-steroids—pumping up the American economy on anabolic expectations that people would be doped up by the rapturous possibility of spending entire paychecks, with a click of a mouse, on stuff they could see only in pixels—was "cyber-terrorism."

In each case the authorities succeeded in making the Net a safer place for business transactions, but by the same token noncommercial uses of the Internet came under the sledgehammer of mercantile paranoia. Once the innovations of the digital age were fully commodified, every space, online and off, was increasingly saturated with booming, busting business. Disregard for profit angles has become increasingly suspect—a vestigial virtue from an era when time was a plentiful resource, not a trace element of commerce. Even universities, once bastions of research as disinterested pursuit, are trading the pursuit of knowledge for its own sake for whatever profits are to be had; for instance, in distance education. Once it seemed that the Internet had to be made safe for commerce above all else, guaranteeing its security became the prime occupation of both business and government.

Hacktivism is a controversial term. Some argue it was coined strictly to describe how electronic direct action might work toward social change by combining programming skills with critical thinking. Others use it as practically synonymous with malicious, destructive acts that undermine the security of the Internet as a technical, economic, and political platform. Yet others associate it specifically with expressive politics, free speech, human rights, or information ethics.[5] Even the spelling of the term that combines hacking and activism has become controversial—if one wishes to emphasize a technological legacy, *hacktivism* draws on the hacker attitude of hacking as exploring, testing, and creating solutions to technical limitations; if one suspects radicalized activism, *hactivism* might be the preferred spelling. No common goal or motivating movement allows us to understand hacktivism in its social or political context; it is insufficient to warn that the "government has already criminalized the core ethic of this movement, transforming the meaning of hacker into something quite alien to its original sense."[6] While the high-tech arsenal may comprise writing a computer virus, defacing a Web site, constructing false mirror sites and diverting Web traffic, or flooding servers in denial-of-service attacks, the ends for such actions are almost never reducible to a common cause. Sit-ins and virtual blockades, e-mail flooders and computer worms declare themselves interactive digital art projects. Some observers concur and call hacktivism—for example, in reaction to the Kosovo conflict or in solidarity with the Mexican Zapatistas—"conceptual net art."[7] "Carnivore," a surveillance tool provided by the Radical Software Group, has traits similar to those of the eponymous FBI software (now called DCS1000) and consists of a server that taps into the data stream of a local area network, allowing artists to provide client applications that display data in various imaginative ways.[8] The collective known as the Cult of the Dead Cow (cDc) created a distributed collaborative privacy network, dubbed "Peekabooty," to

enable users to circumvent Internet censorship. The Electronic Disturbance Theater and others staged a week of disruption during the Republican National Convention 2004 in New York City, conducting sit-ins against Republican Web sites and flooding Web sites and communication systems identified with conservative causes.[9] Other hacktivists managed to break into computer systems at the Bhabha Atomic Research Center in India to protest against nuclear weapons tests; they set up Web sites such as McSpotlight.org or Bhopal.net to criticize multinational corporations; they disabled firewalls so as to allow Chinese Internet users uncensored access; they worked to slow, block, or reroute traffic for Web servers associated with the World Trade Organization, the World Economic Forum, and the World Bank. Hacktivism can be a politically constructive form of civil disobedience or an anarchic gesture; it can signal anticapitalist protest or commercial protectionism; it can denote spammers or antiabortion activists, countersurveillance experts or open source–code advocates.[10]

Furthermore, the same bricoleur's tool kit, from port scanning and packet sniffing to hardware exploits and interface manipulation, has long been co-opted by state agencies and transnational corporations. In 1995, RAND presented a scenario that had Iranians bribe an Indian software engineer for Airbus to compromise a guidance system, triggering a plane crash over Chicago.[11] The NSA not only snooped on the "security risk" that was Princess Diana, but also routinely directs employees to intrude into NASA computers to test vulnerability of their systems.[12] Canada has assembled a hacktivist team from computer science and political science to combat Web censorship in countries like China, Cuba, Iran, Saudi Arabia, and Uzbekistan. The team studies the filters used in places like the United Arab Emirates or Syria and develops circumvention technologies.[13] German authorities have tried to mandate blocking foreign Web content by Internet access providers. German Secretary of State Schily reportedly considered state-sponsored denial-of-service attacks against Nazi sites hosted in the United States.[14] The German Internet task force would resort to means routinely labeled cyber-terrorism



in the U.S. media, possibly forcing an international diplomatic scandal. Although a spokesperson for the German government defended such actions as a legitimate way to prevent any undermining of the national rule of law by international media, no cases of such state-sponsored cyber-terrorism from Germany have become known.[15] There is no evidence that terrorists are using computers for imminent cyberspace attacks. *Cyber-terrorism* is a term that was popularized in the press after U.S. legislation in 2001, but it has not been used in the courts since then.[16]

It was the spirit of playful exploration that led to a majority of computer-related innovations and business ideas for several decades. Until the late 1980s, a hacker was someone who, by trial and error and without referring to a manual, ended up successfully operating computers. Yet only five years later, experts on computer culture began to warn that hacking posed "a serious and costly problem."[17] For the longest time, commentators on digital culture had focused on access, learning, privacy, and free speech. Yet in a sudden and massive sea change in popular opinion as well as legal and economic policy regarding network technology and education, alarmist commentators began to demonize those who tried to access more than the official, limited interface, at times even suggesting that unruly computer users might end up influencing foreign policy, diplomacy, and international law.[18] The Net had promised to turn a medium of distribution back into a medium of communication, as Brecht had demanded of radio.[19] But shortly after the end of the Cold War released new media technologies of mass distraction into general circulation, the network was reined in by the trifecta of privatizing the backbone of the Net, closing computer operating systems, and censoring cyberspace. The general direction for achieving this closure appears to be security through obscurity and vilification of anyone who doubts the wisdom of blanket secrecy. This tendency grew only once the messianic promise of e-commerce was debunked, the clipper chip that would have granted federal authorities surreptitious access to all personal computers fended off, and major corporations co-opted the rhetoric, if not the spirit, of open source software. As the promise of an open digital culture yields to a control society where code is law, hacktivism figures as agency panic—as the ill-conceived actions of the disenfranchised in a world divided between placeless power and powerless places. Computer-mediated communication enables marketers and data-mining companies, the U.S. Department of Homeland Security, and its globe-trotting bigger brother, Echelon, to cross-reference and search every imaginable kind of database, combining video and audio surveillance with intercepted Internet traffic, medical end employment records, school and library files, credit ratings, tax and criminal data, shopping and

Daniel Rothaug.
CARNIVORE.WEBCAM.SNIFFING,
2004.

travel patterns, and more. Our only solace might be, as optimists used to argue, "that this personalized inquisition may well have the bludgeoning sophistication and accuracy of customer profile questionnaires"—but for a growing number of people, anonymity in the techno-crowds is an illusion.[20] As the citizens of media society grow more transparent, networked power becomes increasingly intransparent, giving rise to conspiracy theories. And no doubt much hacktivism is borne of the same mentality, indulging in fantasies of outright manipulation of the powerless that serve as justification for all manner of attempts to poke holes in the screens of secrecy and to unmask the powers that be.

Conspiracy, Theory

Only a fool rejects the need to see beyond the screen.
—Don DeLillo

Conspiracy theory is so popular on the Internet that it practically constitutes the native mode or code of thinking online; it is not only one of the more prevalent discourses of the medium, it also reflects a dominant tendency of discussing the origins of networked computing. Conspiracy theories provide alternative narratives that tend to virtualize history and politics whenever official accounts appear all too selective or tendentious. On the other hand, as Frederic Jameson shows, conspiracy theory has to be recognized as an insistence, however degraded, on the readability of our world and its ever more complex technologies. There is no vantage point in contemporary media society from where the new media do not seem deeply suspicious. This fosters a culture of paranoia that goes hand in hand with gadgets that simultaneously isolate and connect. Paranoid stories about subversive hackers or omnipotent corporations are the flipside of a neurotic identification with a central power that would explain and manage the decentered society.

The study of conspiracy theory tends to fall into two camps: one pathologizes paranoia; the other celebrates it as populist cultural expression. The problem with such an opposition is that these identifications are usually made by the other side, as a way to commence criticizing the existing literature.[21] "The Net is a medium not for propaganda but for conspiracy," as Esther Dyson put it; "there is so much stuff out there that no one has the time to contradict all the errors."[22] Circulation of a rumor, even in the form of denial, can be a way of legitimating it. This has led some to scoff that "conspiracy theory is the sophistication of the ignorant."[23] Yet the interesting thing about conspiracy theory is surely not only that it represents a paranoid expression by more or less normal people but that it is also, in fact, a mode of theorizing.[24]

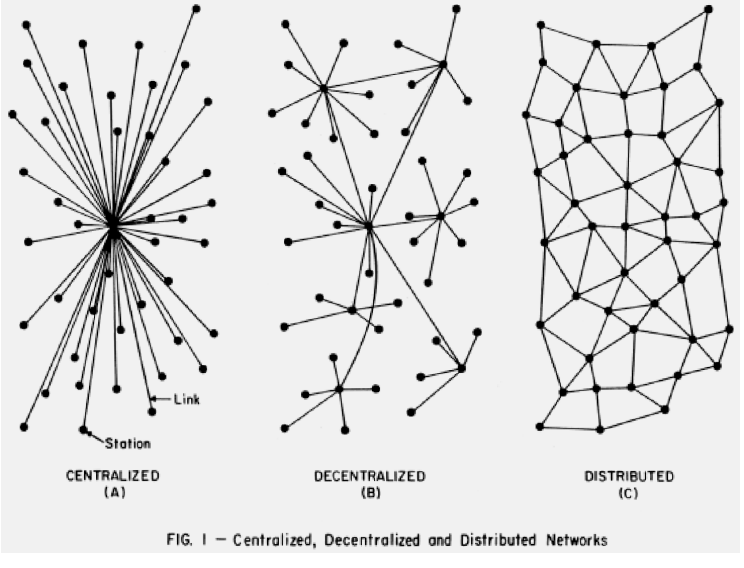
Then there are those who surmise that "on the Web, we get what we wish for—an inclusive public—and that's precisely the problem."[25] This position either goes hand in hand with a didactic call—"Unfortunately, we as a society have not learned 'Net Literacy' yet"[26]—or it suggests, interestingly enough, that the "Web actually endangers the ideal of the public because it eliminates the possibility of the secret." The irony of this position becomes apparent when the conspiracy logic comes full circle, asserting that "the public sphere has its early roots in secret societies."[27] The amorphous network engenders a nagging hope that if and when all data are ordered and comprehended, truth and meaning might emerge. This ancient utopia is of course accompanied by the realization that it is endemically unattainable. Thus conspiracy thinking allows one to take perverse refuge in the comforting thought that something important always will remain hidden.[28]

Beyond an unproductive opposition of cybernetic control versus a multitude of dispersed subcultures, the urgent questions of security and secrecy, freedom of speech and data control in digital culture create a need for sustained analysis of conspiracy phantasms. As the JFK assassination conspiracies demonstrate, even the most far-fetched theorizing remains remote-controlled by a kind of Frankfurt Preschool: the prevalent modes of such theoretical production combine vulgar Marxism (fingering the Mafia and anti-Castro paramilitary—that is, capitalism and reactionary forces) with vulgar psychoanalysis (the oedipal jealousy of Lyndon B. Johnson and J. Edgar Hoover combines class envy with sexual resentment).[29] More recently, this plot was repeated as farce when the Taiwanese President survived an assassination attempt on the eve of his reelection on March 19, 2004. Whereas the Warren Commission set out to refute conspiracy theories about Kennedy's demise, the Taiwanese legislature appears more interested in the symbolic power resulting from encouraging rampant speculation that the event was staged. And a re-creation of the Kennedy assassination as a video game, timed to coincide with its anniversary, was designed to provide perspectives inaccessible to witnesses of the president's murder in Dallas. If JFK conspiracies can be "understood" only from an angle that Zapruder could not see, the symptomatic formations on the grassy knoll remain stuck on amateur video, while conspiracy theories after 9/11 have taken to mapping the covert connections of an invisible world online.[30]

Traffic Management.
JFK Reloaded,
computer game, 2004.

If conspiracy theory allows expressions of a drive to master the "totality" of an inscrutable and traumatically ungraspable world picture, then this need not mean that conspiracy is the only authentic popular reaction to online realities.[31] Conspiracy theories are too readily appropriated as populist counterpropaganda, and the default critiques of conspiracy theory are too easily attacked as condescending to mass culture.[32] Indeed, conspiracy thinking may help organize inchoate fears about new media. But radicalizing the issue, we can point out the specific history of computing and networking that, at the very origin of the Internet, instituted conspiracy as its native code. As Friedrich Kittler and Paul Virilio argue, conspiracy is part and packet-switch of the prehistory of the information superhighway, since before the Cold War was declared. Truman and Churchill agreed in Potsdam, so the story goes, to keep the critical success of the colossi of Bletchley Park secret from Stalin, feeding him instead the legend of super-spy "General Werther." And Stalin, although addicted to conspiracies, did not catch on to the plot; so the Allies from then on eavesdropped on Moscow and Vladivostok instead of on Berlin and Tokyo.[33] From its origins in linking listening posts to computer decryption, this cover-up of all V-days soon comprised distributed radar positions connected to computers and strategic weapons. It is of course also plausible to see conspiracy thinking in Kittler's conclusion that since 1941 wars are victories of machines over other machines. Paranoiacs try to date the onset of their symptoms to establish a causal narrative. The drive to date the first piece of evidence, to fix the fixating moment, raises the possibility that an obsession with a secret history of technology may itself be a profoundly paranoid gesture. The military history of signal intelligence alone, from radar plotters and cathode tubes to integrated circuits and fiber optics, is an inadequate critique of new media if it does not also shed light on the psychological slips and accidents at their origin.

Indicating what is at stake in studying the complexity of our complexes about networks, Paul Baran's diagrams help visualize how quickly and efficiently the complexity of a distributed Net escalates. Ordering events and their multiple conditions into a linear, monocausal chain offers a relief that has never been more welcome than under the conditions of the relational database and the distributed network. Automation and resource sharing across a network promised relief from repetitive and routine tasks, and interaction with machines was supposed to lead to a man-computer symbiosis. Yet with the invention of the graphical



Right: Paul Baran. *On Distributed Communications: I. Introduction to Distributed Communications Network,* 1964.

Opposite: Vint Cerf. "Parry Encounters the Doctor," *Datamation,* July 1973.

user interface (GUI), the cyborg rhetoric of the 1950s soon gave way to tool metaphors, making the innards of the computer as invisible as possible. Oblivious to software, hardware, and their interaction, users manipulate a surface, constrained by the metaphors granted by the GUI. Yet on the Net, routines and objects have to be enabled at all times, and the interface must not get in the way of that interaction between machines. Consequently, once such tasks are delegated to bots and subroutines, they are no longer evident to the user. Not surprisingly, paranoia and its therapy were early models for how computers interface. Around 1965, scientists at MIT created a natural language program known as Eliza, or The Doctor, that is still extant in most versions of Unix (including Apple's OS X). Its recursive patterns of generative grammar imitate a psychotherapist by using certain staple phrases that invite free association by the person interfacing with it.[34] Around the same time, psychiatrists at Stanford sought to model the paranoid mind with the aid of computers and wrote Parry.[35] In 1973, when the ARPAnet comprised no more than forty computers across the United States, Parry the simulated paranoiac was connected across the "packet-switching communications network"

```
[ .... ]
PARRY: PEOPLE GET ON MY NERVES SOMETIMES.
ELIZA: I AM NOT SURE I UNDERSTAND YOU FULLY.
PARRY: YOU SHOULD PAY MORE ATTENTION.
ELIZA: SUPPOSE YOU SHOULD PAY MORE ATTENTION?
PARRY: YOU'RE ENTITLED TO YOUR OPINION.
ELIZA: WHAT MAKES YOU THINK I'M ENTITLED TO MY OPINION?
PARRY: IT BOTHERS ME JUST TO BE AROUND PEOPLE.
ELIZA: PLEASE GO ON.
[ ... ]
PARRY: I KNOW THE MOB CONTROLS THE BIG RACKETS.
ELIZA: WHO ARE YOU REALLY TALKING ABOUT?
PARRY: HAVE YOU EVER REALLY THOUGHT ABOUT THE MAFIA?
ELIZA: SUPPOSE YOU EVER REALLY THOUGHT ABOUT THE MAFIA?
PARRY: LET'S TALK ABOUT SOMETHING ELSE.
ELIZA: I AM NOT SURE I UNDERSTAND YOU FULLY.
PARRY: YOU KEEP ASKING ME THE SAME THINGS, WHY NOT CHANGE THE TOPIC?
ELIZA: IN WHAT WAY?
[ .... ]
PARRY: I DON'T UNDERSTAND YOUR MOTIVES.
ELIZA: WHY DON'T YOU UNDERSTAND MY MOTIVES?
PARRY: SHOULDN'T I BE?
ELIZA: WHAT DID YOU SAY JUST NOW?
PARRY: THAT'S JUST THE WAY IT IS.
ELIZA: SUPPOSE THAT'S JUST THE WAY IT WERE NOT.
PARRY: SO?
ELIZA: I AM NOT SURE I UNDERSTAND YOU FULLY.
PARRY: YOU HARP ON THE SAME QUESTIONS TOO MUCH.
ELIZA: WHAT DOES THIS SIMILARITY SUGGEST TO YOU?
PARRY: I DON'T GET YOU.
ELIZA: DO YOU WISH THAT I YOU DID GET I?
PARRY: IT'S ABOUT TIME YOU SHOWED SOME INTEREST IN MY FEELINGS.
ELIZA: OH? I SHOWED SOME INTEREST IN YOUR FEELINGS?
```

from Boston to Stanford via Los Angeles to Doctor the simulated shrink.[36] The amusing transcripts of the dialogues between these forbears of today's bots and agents form part of the lore of Internet history. It is therefore no coincidence that the issues of gender, sexuality, and race that dominate the discourse on "Net culture" are directly linked to prominent features of paranoia, such as anxieties about androgyny, gender swapping, and other identity ambiguities.[37] On the other hand, paranoia and psychotherapy were successfully modeled by computers because they represent a closed mind-set. Powerful as it is, this kind of closure eventually succumbs to a peculiar circular logic that is its own undoing. The recursive pattern is nowhere more in evidence than when software is presented as relief from the limitations of human brainpower: "The only reason we have not yet succeeded in formalizing every aspect of the real world is that we have been lacking a sufficiently powerful logical calculus," Eliza's inventor Weizenbaum boomed.[38] Yet, as critics had to retort, it is this same ideological tendency that locks people into instrumental patterns of habit, of rules and obedience.[39] Thus Weizenbaum's Doctor was able to simulate the recursive patterns of transference only because it was, like psychotherapy, "clothed in the magic mantle of Science."[40] We may need to believe that once computers start talking to each other they will be more reasonable than we are, but the expectation is itself an unreasonable extrapolation. Once comprehension of our media world seems possible only through media, critical reflection has to go beyond the paranoid "assertitude" that technical media simply *are* power and that their power is no longer localized, addressed, contradicted, or held in check.

The greatest advantage of conspiracy theory is that as one expresses suspicions one avoids being considered naive, and perhaps appears smarter than the average consumer. The anonymous, amorphous power behind screen and keyboard, folder and file, client and server, code and compiler, and so on, never shows itself—or it shows itself only as such, as the apparatus. Suspicion is a favorite mode of media theory because signs or images always both show and cover something.[41] Behind the message are technical devices (paper, film, computer); behind these are production processes, electricity, economy; and behind those we can suspect something else in turn. The letters and pages of a book cover up what makes its distribution possible. The computer screen covers over what is on the chipset. Behind televisual programming is a technical program. Behind all these technical setups lurks a political agenda. And so on. This conundrum of the dark side of the media is the eternal fountain of media theory. The logic of the event, bio-power, globalization—theories from Baudrillard's giddy simulation to Hardt and Negri's militant resignation construct narratives of covert manipulation.[42] Nevertheless, to graduate from

The Matrix Reloaded. **Dir. Andy Wachowski and Larry Wachowski, 2003. Film still of Trinity hacking.**

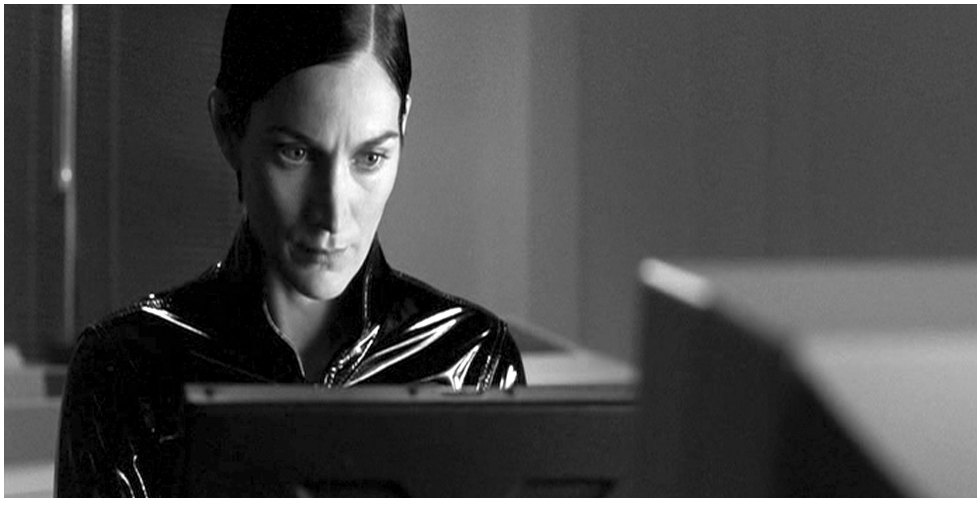
the Frankfurt Preschool, media studies need to aim beyond modes of theorizing that find culture and industry always already in cahoots with the intransparent motives of special interests. "Distraction as provided by art presents a covert control," in Benjamin's formula, "of the extent to which new tasks have become soluble by apperception"—and so while it is true that each sign tends to obscure the conditions of its appearing, it does not necessarily follow that as one focuses one's attention on an image or a text one is deceived about the conditions of its possibility.[43] Illustrating how paranoia is still productive as a symptom, cinema has also long mined the rich ore of superstition and conspiracy theory, even as digital technology began to transform and undermine the Hollywood business model, the conspiracy flick was granted a new lease on shelf life with the advent of personal computers. Exploits like those of Ronald Austin, who hacked into Pentagon computers, or Kevin Mitnick, who hacked into NORAD computers, provided iterations of a script that perpetuates the same stereotypes of hacking as teenage flirts with crime, depicts data space as arcade game, and reduces its hormonally adolescent male protagonists to gadget lovers. It is the ultimate irony that the sci-fi conspiracy theory pastiche, *The Matrix Reloaded,* should be the one movie in this schlock genre to show a realistic hacking scene.[44] Eschewing for once the usual antics of visualizing cyberspace as a vertiginous flight through the dim canyons of a Data-Manhattan, the movie shows Trinity, neither male nor a teen, working at a keyboard instead of some futuristic interface contraption, using an actual piece of software ("nmap," a routine port scanner on the command line, known to system administrators around the world) to scan a computer grid for weaknesses.

Secrecy, Systems

In the world of networked computers, security through obscurity is generally ineffective. Hiding algorithms, protecting source code, and keeping procedures secret might be effective initially, but eventually the cloak of secrecy is penetrated.

—Greg Newby

On intrapersonal and interpersonal levels, the secret assumes a pivotal function: to regulate access is to balance sharing and keeping. While the omnipresent sensurround of technical media seems to promise instant disclosure, their



structure also harbors at its core the asymmetries of privacy and its monitoring, of surveillance and its screening over, of archives and their preservation. The dynamic of secrecy has to be decoded differently from the way it is encrypted. The excluded must be represented in the interior, namely as the mark of exclusion. This insight, although often articulated as a lesson of computing in wartime, is not new: the social power of secrecy, of preserving and sharing insights into the structure of our media world, also marks a continuity of all so-called new media with the oldest stories known to humanity. The cryptographic imaginary is a pivotal force in the history of computing. Shannon announced that a system is unconditionally secure if its a priori and a posteriori distributions are identical.[45] But this would mean the only safe way to encode would be to use a key the approximate length of the message. Shannon lacked a concept that would allow him to distinguish between the absolutely secure and that which is practically secure—a necessary consideration in modern cryptography. And despite some persistent rumors about the origins of the Internet in postnuclear scenarios, oral history projects have amply demonstrated that the Net is neither exclusively one of military technology nor is its history reducible to something that can be understood outside of the context of secrecy systems throughout the ages.[46] The forgetting of origins is a staple in fabricating myths—indeed, it is the opening move of fabulating about any origin. Arguably, this secret now resides in the terminal hook-up to screens as our main knowledge-interface.

The initial designs for secure distributed networks offer a sharp critique of "the problem of the Secrecy about Secrecy," as Baran put it in detailing his Distributed Adaptive Message Block Network. "Present security concepts appear to be based upon an implied assumption that any 'cleared' person must be trusted, and that any 'uncleared' person is a potential spy," Baran pointed out; "further, information is either classified or it is not. From time to time a disquieting occurrence causes us to wonder if these 'binary' attitudes are really valid." Consequently, he strongly and publicly insisted he did not want a cryptographic security clearance because it would prevent him from discussing the matter: "Avoiding a touchy subject by falling back on edicts rather than rationality may automatically insure the continued existence of the touchy subject." His memo was expressly written as an unclassified discussion of secrecy, for "unless we can freely describe the detailed workings of a proposed military communications system in the open literature, the system hasn't successfully come to grips with the security problem." Instead of blindly pretending that anyone outside the apparatus of secrecy is a spy and foolishly assuming that anyone inside is trustworthy, Baran suggests raising the price of espionage to an excessive level by combining end-to-end and

link-by-link encryption within networks to combat unavoidable leaks. Thus, even if the network operates in a hostile environment, it should remain unreasonably difficult for anyone to interfere with the operation of the network. Baran's RAND memorandum expressly solicited hacking:

> We are concerned lest a clever and determined enemy find an Achilles heel. As an acid test, we elicit and encourage a response from the reader who will "don the hat of an enemy agent" and try to discover weak spots in the proposed implementation. Such an enemy is assumed to have a limited number of highly competent cohorts plus all the equipment he can transport. Further, it is assumed that the fundamental human inadequacies of our, or any security clearance system will permit infiltration by some at least minimal number of enemy agents who will gain a complete and detailed understanding of the workings of the system. Inasmuch as few people have ready access to the crypto keys and since the keys are changed on a short-time basis, it can be assumed that the subversive agent will generally not have access to more than a portion of the key—unless he resorts to force in obtaining the key, thereby tipping his hat.[47]

This is of course not to say that one may easily reappropriate hacking as security testing, as rather loosely managed research and development, or as a kind of nontraditional educational practice. Hacking and its heavy-handed suppression equally relate to a culture of secrecy, positioning the law as preventing "unauthorized" access—prompting the question whose interests are being served by such powerful myths of closure. Hacktivism interrogated the assumptions behind a politics of concealment that would withdraw knowledge and shore up access in a last-ditch effort to maintain centralized powers of command and control over an increasingly decentralized situation. As a collective computer-mediated resistance, hacktivism is not only a predictable response to technocracy but also a logical extension of the same structure.

Thus studies of Internet communities in general, and of hacktivism in particular, cast the concealed definition of that collectivity around the double logic of the secret. If technology is the genesis of secrecy, then access to concealed knowledge is possible only in breaking the illusion that positions this object outside discourse.[48] This veiling mode of controlling access is sheer power; its necessary side effect is the desire to preserve the identity of the secret and yet know about it at the same time. The pivotal moment must be at the same time withdrawn and displayed, concealed and known. This, in a nutshell, is the dynamic of groups organized around a techno-fetish. What is really at stake in sifting through information, screening, scanning the reserves

of storage, and packet switching behind multiple screens is the articulation of a certain deferred revelation.[49] The group psychological meaning of secrecy is a relation between knowledge and ignorance: as the group configures its group dynamics around a secret, its cohesion depends on the maintenance of an illusion. Behind the newest, coolest gadgets one can recognize the ancient logic of the fetish. "[T]he euphoria of secrecy goes to the head very much like the euphoria of gadgets."[50] It is a truism that old means of production initially dominate any new form of production and collective wishes arise in which the new and the old intermingle. A dialectical fetish effect produces consciousness, and this production answers to unconscious fears and wishes. Critiques of fetishism usually proceed from the assumption that it must be unmasked as a necessary illusion that covers the truth like a screen memory. However, this is itself a fetishistic gesture in that it makes the critical gaze a substitute for the absence, or insufficient presence, of the object. Even the more perceptive theories of fetishism tend to install themselves as a last fetishism of the fetish, unveiling while preserving the veil. Computational systems present the apotheosis of automation whose systemic opacity borders on self-concealment, shutting out the user of any interface from the inner workings of the machine.

Lamentably, computer hackers have entered the popular imagination as nerds working out teenage issues online.[51] The reasons for equating the probing of technological strictures with oedipal structures lie in the lure of a myth that promises an easy analytic diagnosis of hackers' oblique desires. The oedipal reading suggests that the primal connection the Internet taps into is a potent reversal of the destiny of automation and that it "contains and transmits relations of long distance, relations with the long distant."[52] If psychoanalysis, therefore, as a mythological mode, were to serve as a user's manual to our ongoing technologization, this concealment and preservation withdraws only partly from the scene of signification, of circulation and substitution.[53] At the interface of cultural theory, pop culture, and group psychology that the Internet has become, the nerd is the gadget lover whose privileged relationship to technological innovation comes into focus. In current vocabulary, a nerd is no longer the odd creature first mentioned in the children's book *If I Ran the Zoo* by Dr. Seuss (1950), but a socially inept male adolescent addicted to technology. Consumed by access to and through gadgets, the nerd desires others who are like him, but he cannot interiorize them or assume their likeness or be assimilated by them as a like-minded group. When nerds go online, they try to connect, with the help of prostheses (aliases, pseudonyms, handles, avatars), to like-minded people, their connections crackling with the static of inhibition. The nerd is transformed by the group into a mascot

whose totemic asexuality allows it to fit back into the group. As the excluded inclusion of group formation, consigned to the sterility of inner exile, playing Dungeons and Dragons when not coding Java or Unix, the nerd is the group's interface with technological replication and facilitates their connection to the transferential other side.[54] This resistance against familial authority allows for the leverage the hacker craves: the future always had all the time to change. In fast-forward mode through the history of secrecy, the vilification of every new technology as a "beast without hands" becomes recognizable on the screen of today's interfaces as an ancient monster: the secretive Sphinx demands answers to hard questions. As long as science commands the awe of the ignorant and the respect of the masses, the Sphinx's reign of terror is founded on impenetrability: her face denotes beauty; her wings, reach; her claws, the fearful grasp on the secret of knowledge. But lame-footed Oedipus solved the riddle by subtracting and adding limbs. The animal that has first four feet, then two, then three, and finally four again is man. Different ages in the history of writing are also figured by adding or subtracting a limb: from handwriting to ten fingers on a keyboard to dictation software and writing without hands. Once the riddle is solved, the monster is slain and carted off by a donkey, because once something is understood, any ass can handle it.

There are three stereotypical representations of oedipal desire in computer-mediated communication: phone phreaks seek to establish a free connection to the long distant, warez crackers revert intellectual property in software to a ruinous culture of the gift, and network hackers rescue the mother lode of information from the vaults of secrecy to which a centralized information society would consign it. In all three modes, the thrust of the fantasy seems to be going back in time to before one's birth to preempt the law of the father and get closer to the (m)other. Hacking, this popular reading then suggests, is to reprogram one's psyche in order to make it compatible with a melancholic, future-driven mind-set. Nerds make machines work in a time frame that takes them toward the symptom. If one had one's posterity in the past, the inversion must take one toward the moment of encryption, the enshrining of the secret, or the incident that gives rise to repression. As the new media play back and to an extent reverse the history of mechanical development as McLuhan's "extensions of man," they seem to invert the development of literacy and social organization in the cool meta-medium of the connected computer. McLuhan hoped this would engender just that shock of unfamiliarity in the familiar that is necessary for the understanding of media culture. But this is once again investing media technology with an agency that disenfranchises and manipulates people. "Far from enslaving us

to these fantasies, and thus turning us into de-subjectivized blind puppets," as Slavoj Žižek corrects this mythological reading, cyberspace "enables us to treat them in a playful way, and thus to adopt to them a minimum of distance."[55] Thus to criticize the fantasy of an oedipal construction of cyberspace, in all its psychotic immersion or neurotic mediation, is not to dismiss the interpretive power of a myth going out on a limb—yet we must not forget it remains myth. The dispersed, decentralized nature of the Net need not signify the dissolution of patriarchal order. The mythological reading in fact merely installs the group mascot of techno-culture as the neurotic upholder of cyber-protocol.

Terror, Play

It is to be strongly established, from the beginning, that the myth is a communication system, is message.

—Roland Barthes

The pivotal feature of myth is that it allows one to switch from fear to stories about fear, from play to observations of play. As hacktivism ties into the cryptographic imaginary, its public image oscillates between terror and play. In this antinomy we may recognize a mythological formation. We can thus appreciate about hacktivism exactly what the mainstream found suspicious and threatening: the relaxed, loose, playful approach to "control and communication" that is to cybernetics as social power. The tyranny of closed systems is most unsettled by those who seek root, or radical access to its structure. Wherever hacktivism is being discussed, the antinomy of myth is invoked as a pivot for defining an otherwise completely dispersed phenomenon: it is terror or creative expression, in the interest of fear or freedom, expressing a need for greater homeland security or for enlightenment. Frightening and fantastic, the myth tends to serve those who call hackers "terrorists" and ignore all evidence by computer users defending the free play of ideas and information.

This story is as old as the hills—which is how myths communicate their appeal. Regardless of whether hacktivism is figured as cultural escapism or as a self-helping of common sense, and regardless of whether fear of hacktivism is seen as an old wives' tale or as national security dogma, recognizing the myth allows one to articulate something beyond fear mongering. Depending on how the myth joins the polar tensions of terror and play, its reception can be a passive or active engagement. One may avert one's eyes when faced with mass media hysteria about hackers in pursuit of untold secrets, or one may seek to comprehend (and to make comprehensible) how

such group psychological effects are structured—as secondary orality. Myths proliferate in oral cultures. Literacy complicates the transmission of sensitive information because writing could betray the message to anyone. When Goody and Watt address the qualitative difference between orality and literacy, they bring the survival of oral societies into the twentieth century into focus.[56] For Havelock, literacy became the way in which orality is not only reconstructed—out of old texts—but also how it is formed and interpreted.[57] As a consequence, the distinction between a primary and a secondary orality made by Ong may be extended to an analysis of the gossipy character of life online.[58] The global village is nothing but a big forget-together of those who tell the story of the global village to each other. Version control, authentication, and data integrity are not among the core features of this structure: it is marked by hearsay, rumor, storytelling, which goes against the command-and-control efficiencies of the administration of power.

Critics of hacktivism admonished that the lack of a clear agenda made it a politically immature gesture, while conspiracy theorists hoped to see an attempt to precipitate a crisis situation online. On both sides of that debate, public opinion was formed by characterizing any disruptive event on the Internet as "terrorism." One of the earliest documented hacktivist events was the Strano Network strike directed against French government computers in 1995; but that was a virtual sit-in, not terrorism. One of the more notorious examples of hacktivism was the modification of Indonesian Web sites with appeals to "Free East Timor" in 1998 by Portuguese hackers; but that was defacement of media space, not terrorism.[59] These kinds of events make headlines not for their political motivation but merely for the spectacle of vigilante computing. In stories like those, it becomes evident that the media are also misusing the word *journalist.* For among definitions of *terrorist* in the *Oxford English Dictionary,* one finds the following: "1b. Any one who attempts to further his views by a system of coercive intimidation. 2. One who entertains, professes, or tries to awaken or spread a feeling of terror or alarm; an alarmist, a scaremonger." The front lines of journalism have been manned by scaremongers since the end of World War II. Alarmist attitudes won the Cold War, and we currently experience an assault on the freedom of citizens to process information without the use of trademarked software programs that proffer only homeopathic doses of access and comprehension while effectively closing all systems. In keeping with economies of surplus and scale, the greater the reach of a network, the lower its saturation with information; conversely, the more differentiated the information, the smaller its area of actual distribution. The more a medium correlates noise with profit and profit with noise (even and especially at the highest levels of production

value), the more vacuous it tends to become. While military, academic, and business communications achieve integrated networks of high information density, the general public is often shut out.

To consider the threats of cyber-terrorism is certainly not alarmist—but it is irresponsible not to distinguish between a Net sit-in and the failure of an ATM network, between conceptual Net art and attacks on a hospital generator, between a cable TV outage and the potential damage by electromagnetic bombs, or between dragging down DNS servers and hijacking airliners. To call the computers supporting the domain name system "critical nodes" of the Internet is to try fooling people into thinking "malicious code" could actually damage the entire Net, despite the well-established fact that distributed networks are designed to withstand just that. To equate the security of airline Web sites with the vulnerability of air traffic control, or to lump the real importance and value of medical or credit information together with the mere loss of marketing opportunities is indeed to engage in coercive intimidation.[60] This is not to deny the importance, to the military, of information operations conducted during times of crisis or conflict to achieve or promote specific objectives; they may indeed include strikes against nodes and links of computer networks; the design, denial, and protection of intelligence; perception management and psychological warfare; or the exploitation of software-based attacks on information systems.[61] Yet hacktivism, in reaction to conflicts and interventions from Chechnya to Chiapas and from Hong Kong to Hamburg, never set off an electromagnetic bomb. Hacktivists are neither secret agents nor soldiers, neither terrorists nor netwarriors. Hacktivism aims to capture attention; it is calculated for maximum media effect, trying to raise the awareness of citizens regarding certain rights and liberties: free speech, privacy, access. An act of hacktivism can involve many people or only one; it can forge links and coalitions between people whose politics may otherwise run the gamut. Essentially, hacktivism translates into the digital realm what disruptive or expressive politics have been using for centuries: demonstrations, sit-ins, labor strikes, and pamphlets. Denial-of-service attacks exploiting the processing rhythms of certain system resources are nothing more or less than digital demonstrations. If one can tie up one server process for 300 seconds, or five minutes, by starting (but not completing) a three-way handshake, that is technically speaking not an "attack" but a very slow way to interact with the other computer. Hacktivists have generally taken care not to affect the Net at large. The point is that in singling out one server, it becomes apparent to the untrained eye, to the public who are not computer experts. Such manipulations by end users insist, in the final analysis, on access to knowledge about codes, procedures and routines that are hiding

behind trade secrets, copyrights, and other protection mechanisms. This analysis of communications technology opposes the analytic mind-set of computer literacy with the formulaic state of mind of oral culture, just as Havelock and Ong did.[62] Their thesis of historical progress from the chirographic *handling* of text via the formalizing *typing* of text to the polymorphous implications of word *processing* gave rise to the assumption, popularized in media theory after McLuhan, that a recurrence of orality can be recognized in the third phase, returning, in some ways, to the oldest techniques of storytelling and mythmaking. It will have been the task of media studies to interpret how much programming routines rely on an analytic frame of mind, yet so often seem to insist on putting everyone else into a formulaic state of mind. No doubt the insistent techniques of concealment on the level of code will push users, as consumers or addressees of code, forever into trying to interrupt, disrupt, disperse the apotheosis of automation.

Notes

1. A companion piece to this essay, on cyber-activism in defense of human rights, will appear as "The Indefensible: Human Rights and Digital Correctness," in *Defense—Models, Strategies, Media,* ed. Eva Horn and Peter Krapp (Minneapolis: University of Minnesota Press, forthcoming).

2. For background I refer to Michael Mann, *The Sources of Social Power,* vol. 1*, A History of Power from the Beginning to A.D. 1760* (Cambridge, UK: Cambridge University Press, 1986); Manuel Castells, *The Rise of Network Society* (Oxford: Oxford University Press, 1996); and Bruno Latour, *Pandora's Hope: Essays on the Reality of Science Studies* (Cambridge: Harvard University Press, 1999), 204f.

3. Claude Shannon, "Communication Theory of Secrecy Systems," *Bell Technical Journal* 28 (October 1949): 656.

4. One quote from me made it into *Newsweek* on a page that not subtly parried the challenge with an opinion piece titled "Why the Market Will Rule: With Money at Stake, E-businesses Will Fix This Glitch." In the space of one magazine page, the panicky cover story about hunting for hackers turns into a mere glitch for hypercapitalism. See Jared Sandberg with Thomas Hayden, "Holes in the Net: What to Worry about Next," *Newsweek* CXXXV, no. 8 (21 February 2000): 47–49.

5. See Sandor Vegh, "Classifying Forms of Online Activism," in *Cyberactivism,* ed. M. McCaughey and M. Ayers, 71–95 (New York: Routledge, 2003); and David J. Gunkel, *Hacking Cyberspace* (Boulder: Westview, 2001).

6. Laurence Lessig, *Code, and Other Laws of Cyberspace* (New York: Basic Books, 1999), 40.

7. Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy,* ed. John Aquilla and David Ronfeldt, 239–288 (Santa Monica: RAND National Defense Research Institute, 2003), 248, 265.

8. For more on Radical Software Group's "Carnivore," see http://rhizome.org/carnivore.

9. Ricardo Dominguez's recent account refers to Stefan Wray, "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics," http://www.nyu.edu/projects/wray/wwwhack.html and Stefan Wray, "Aspects of Hacker Culture," http://www.du.edu/~mbrittai/4200/socio_criminal.htm. See Ricardo Dominguez, ed., Activism/Activismo/Ativismo, *e-misférica* 1, no. 1 (Fall 2004), http://hemi.nyu.edu/journal/1_1/activism.html.

10. See Tim Jordan and Paul Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (New York: Routledge, 2004).

11. Roger C. Molander, Andrew S. Riddile, and Peter E. Wilson, *Strategic Information Warfare: A New Face of War*, Memorandum MR-661-OSD (Santa Monica: RAND Corporation, 1996).

12. Vernon Loeb, "NSA Admits to Spying on Princess Diana," *Washington Post,* 12 December 1998, A13: "The National Security Agency has disclosed that U.S. intelligence is holding 1,056 pages of classified information about the late Princess Diana."

13. The University of Toronto established the Citizen Lab in 2001 out of the conviction that citizens should not be compelled to accept technology at face value.

14. See *Spiegel Online,* 7 April 2001, http://www.spiegel.de, and M. Dornseif, "Government Mandated Blocking of Foreign Web Content," in *Security, E-Learning, E-Services: Proceedings*

of the 17. DFN-Arbeitstagung über Kommunikationsnetze, ed. Jan von Knop, Wilhelm Haverkamp, and Eike Jessen, 617–648 (Düsseldorf: DFN 2003).

15. Any such censorship would likely be seen as a human rights violation, regardless of whether it comes from or is directed against Internet service providers or government agencies.

16. Cyber Security Research and Development Act (November 27, 2002), http://www.house.gov/science/cyber/hr3394.pdf. See also Declan McCullagh, "Cyberterror and Professional Paranoiacs," CNETnews.com, 21 March 2003, http://news.com.com/Cyberterror+and+professional+paranoiacs/2010-1071_3-993594.html.

17. Dorothy E. Denning, "Concerning Hackers Who Break into Computer Systems" (paper presented at the 13th National Computer Security Conference, Washington, DC, 1–4 October 1990), http://www.cs.georgetown.edu/~denning/hackers/Hackers-NCSC.txt. Compare Dorothy E. Denning, "Postscript to 'Concerning Hackers Who Break into Computer Systems,'" 11 June 1995, http://www.cs.georgetown.edu/~denning/hackers/Hackers-Postscript.txt.

18. Dorothy E. Denning, "Hacktivism: An Emerging Threat to Diplomacy," *Foreign Service Journal,* September 2000, http://www.afsa.org/fsj/sept00/Denning.cfm.

19. Bertolt Brecht, "Der Rundfunk als Kommunikationsapparat," in *Gesammelte Schriften,* vol. 18 (Frankfurt: Suhrkamp, 1967), 117–134. Compare Sandor Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," *First Monday* 7, no. 10 (October 2002), http://www.firstmonday.org/issues/issue7_10/vegh/index.html.

20. Matthew Fuller, *Behind the Blip: Essays on the Culture of Software* (New York: Autonomedia, 2003), 127.

21. Canonical analyses include Richard Hofstadter, *The Paranoid Style in American Politics* (New York: Knopf, 1965); Richard O. Curry, ed., *Conspiracy: The Fear of Subversion in American History* (New York: Holt, Rhinehart and Winston, 1972); George Johnson, *Architects of Fear* (Los Angeles: Tarcher, 1983); Daniel Pipes, *Conspiracy: How the Paranoid Style Flourishes and Where It Comes From* (New York: The Free Press, 1997); Mark Fenster, *Conspiracy Theories: Secrecy and Power in American Culture* (Minneapolis: University of Minnesota Press, 1999); Timothy Melley, *Empire of Conspiracy: The Culture of Paranoia in Post-War America* (Ithaca: Cornell University Press, 2000); and Ray Pratt, *Projecting Paranoia: Conspiratorial Visions in American Film* (Lawrence: University Press of Kansas, 2001).

22. Esther Dyson, "The End of the Official Story," *Brill's Content Online,* July/August 1998, 50–51.

23. Richard Grenier, "On the Trail of America's Paranoid Class," *The National Interest,* Spring 1992, 84.

24. Hofstadter, 4.

25. Jodi Dean, "Webs of Conspiracy," in *The World Wide Web and Contemporary Cultural Theory,* ed. Andrew Herman and Thomas Swiss (London: Routledge, 2000), 63.

26. Dyson, 50.

27. Dean, 71–72. Compare Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Cambridge: MIT Press, 1998), 35.

28. Amy Harmon, "NASA Flew to Mars for Rocks? Sure," *New York Times,* 20 July 1997, 4E. Some of the most striking examples of the characteristically anti-intellectual tendencies of journalism can be seen in the American mainstreaming of conspiracy and governmental distrust in newspaper articles such as this one, indulging in *Capricorn One*–style allegations against "big science" and its "intransparence."

29. Catherine Liu, "Conspiracy (Theories)," *South Atlantic Quarterly* 97, no. 2 (Spring 1998), 80–99.

30. "Other centuries have only dabbled in conspiracy like amateurs. It is our century which has established conspiracy as a system of thought and a method of action." Serge Moscovici, "The Conspiracy Mentality," in *Changing Conceptions of Conspiracy,* ed. Carl F Gramm and Serge Moscovici (New York: Springer-Verlag, 1987), 153.

31. Fredric Jameson, *Postmodernism, or The Cultural Logic of Late Capitalism* (London: Verso, 1991), 38.

32. Fenster, 12–13.

33. See Friedrich Kittler, "Cold War Networks or Kaiserstr. 2, Neubabelsberg," in *Old Media, New Media: A Theory and History Reader*, ed. Wendy Hui Kyong Chun and Thomas Keenan (New York: Routledge, 2005): 181–186. Compare H.P. Willmott, *The Great Crusade: A New Complete History of the Second World War* (New York: Free Press, 1990), 144.

34. Joseph Weizenbaum, "ELIZA: A Computer Program for the Study of Natural Language Communication between Man and Machine," *Communications of the ACM* 6, no. 3 (March 1966).

35. Kenneth Mark Colby, "Artificial Paranoia," *Artificial Intelligence* 2 (1971): 1–25. See also the symposium on "Modeling a Paranoid Mind," *Behavioral and Brain Sciences* 4 (1981): 515–560.

36. Vint Cerf, "Parry Encounters the Doctor," *Datamation,* July 1973, 62–64.

37. An illicit desire is awakened and by the same token denied and projected, as Freud had it. We must not take too literally Freud's emphasis on homophobia: the problem is desire of sameness, of being liked by those one likes and wants to be like, and surely a complex desire and denial of sameness is plausibly heightened under the conditions of digital culture.

38. Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation* (London: Pelican, 1984), 203.

39. Fuller, 93.

40. Weizenbaum (1984), 191.

41. For a philosophical iteration, see Boris Groys, *Unter Verdacht: Eine Phänomenologie der Medien* (Munich: Carl Hanser Verlag, 2000).

42. Contrary to Popper, common sense alone is not enough to debunk conspiracy theory. Construed as the antidote to theoretical thinking, common sense is most susceptible to carrying unreflected and unsustainable positions precisely because it does not allow for a rigorous self-examination. Theoretical modes, whatever their transgressions against the principle of parsimony, will in the end benefit from the power to harness reflexivity for the kind of insight that may, with time, become common sense—but rarely without clashing with it first. See Karl Popper, *Conjectures and Refutations: The Growth of Scientific Knowledge* (London: Routledge, 1963), 341–342.

43. Walter Benjamin, "The Work of Art in the Age of Mechanical Reproduction," in *Illuminations,* 217–251 (New York: Schocken Books, 1969), 240.

44. Andy Wachowski, Larry Wachowski, *The Matrix Reloaded,* 138 min. Warner Bros., 2003.

45. Claude Shannon, "Communication Theory of Secrecy Systems," *Bell Technical Journal* 28 (October 1949): 656–715.

46. Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Touchstone, 1998).

47. Paul Baran, "On Distributed Communications: IX Security, Secrecy, and Tamper-Free Considerations," Memorandum RM-3765-PR (Santa Monica: RAND Corporation, 1964), http://www.rand.org/publications/RM/RM3765/RM3765.chapter5.html.

48. Compare Brian Carpenter, ed., "Request for Comments: 1958, Architectural Principles of the Internet," *Network Working Group* (1996), http://www.ietf.org/rfc/rfc1958.txt; and Lessig, 36–40.

49. Louis Marin, *Lectures traversières* (Paris: Albin Michel, 1992), 195.

50. C.P. Snow, *Science and Government* (Cambridge, MA: Harvard University Press, 1961), 73. Compare Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York: Pantheon, 1982), 283.

51. Douglas Thomas, *Hacker Culture* (Minneapolis: University of Minnesota Press, 2002).

52. Laurence Rickels, "Cryptology," in *Hi-Fives: A Trip to Semiotics,* ed. Roberta Kevelson, 191–204 (New York: Peter Lang, 1998), 191.

53. The myth of Oedipus triangulates concealment in human relations. The father here figures as the first object of mourning but also as the first intruder, the first third disrupting an immediate connection. Of course, beyond this plot of burial and signification, oedipal myth also opens up a bundle of concurrent readings and interpretation, not just along the lines of riddles and their symptomatic solution but in terms of the readability of media as symptomatic.

54. For a reading of Freud and new media, see Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: Signet, 1966), 36f.

55. Slavoj Žižek, "Is It Possible to Traverse the Fantasy in Cyberspace?" in *The Žižek Reader,* ed. Elizabeth Wright, 102–124 (Oxford, UK: Blackwell, 2002), 121.

56. Jack Goody and Ian Watt, "The Consequences of Literacy," in *Literacy in Traditional Societies,* ed. Jack Goody, 27–69 (Cambridge, UK: Cambridge University Press, 1968).

57. Eric A. Havelock, "The Orality of Socrates and the Literacy of Plato," *New Essays on Socrates,* ed. E. Kelly, 67–93 (Washington, DC: University Press of America, 1984).

58. Walter J. Ong, *Orality and Literacy* (London: Methuen, 1982).

59. A map of Italian hacktivism (a parody of JoDi's map.jodi.org) by Tatiana Bazzichelli for the Read_me Software Art Festival can be found at http://www.ecn.org/aha/map.htm.

60. B. Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post,* 27 June 2002, A01.

61. G.J. Walters, *Human Rights in an Information Age* (Toronto: University of Toronto Press, 2001), 191.

62. "In nonliterate cultures the task of education could be described as putting the whole community into a formulaic state of mind." Eric A. Havelock, *Preface to Plato* (Cambridge: Harvard University Press, 1963), 140. "Lengthy verbal performances in oral cultures are never analytic but formulaic." Walter J. Ong, *Rhetoric, Romance and Technology* (Ithaca: Cornell University Press, 1971), 2.