6

Tactical Media

The Internet is like the *Titanic.* It is an instrument which performs extraordinarily well but which contains its own catastrophe.
—PAUL VIRILIO, "Infowar"

Like many interesting social movements that may manifest themselves in a variety of ways, tactical media has an orthodox definition and a more general one. The orthodoxy comes from the new tech-savvy social movements taking place in and around the Western world and associated with media luminaries such as Geert Lovink, Ricardo Dominguez (with the Electronic Disturbance Theater), and Critical Art Ensemble. Tactical media is the term given to political uses of both new and old technologies, such as the organization of virtual sit-ins, campaigns for more democratic access to the Internet, or even the creation of new software products not aimed at the commercial market.

"Tactical Media are what happens when the cheap 'do it yourself' media, made possible by the revolution in consumer electronics and expanded forms of distribution (from public access cable to the internet) are exploited by groups and individuals who feel aggrieved by or excluded from the wider culture," write tactical media gurus David Garcia and Geert Lovink. "Tactical media are media of crisis, criticism and opposition."[1] Thus, tactical media means the bottom-up struggle of the networks against the power centers. (And of course the networks against the power centers who have recently reinvented themselves as networks!)

But there is also a more general way of thinking about tactical phenomena within the media. That is to say, there are certain *tactical effects* that often leave only traces of their successes to be discovered later by the ecologists of the media. This might include more than would normally fit under the orthodox definition. Case in point: computer viruses. In a very bland sense, they are politically bankrupt and certainly no friend of the tactical media practitioner. But in a more general sense they speak volumes on the nature of network-based conflict.

For example computer viruses are incredibly effective at identifying anti-protocological technologies. They infect proprietary systems and propagate

---

Epigraphs: Paul Virilio, "Infowar," in *Ars Electronica*, ed. Timothy Druckrey (Cambridge: MIT Press, 1999), p. 334. One assumes that the italicized "*Titanic*" may refer to James Cameron's 1997 film as well as the fated passenger ship, thereby offering an interesting double meaning that suggests, as others have aptly argued, that films, understood as texts, contain their own undoing. John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: Rand, 2001), p. 6.

1. David Garcia and Geert Lovink, "The ABC of Tactical Media," *Nettime*, May 16, 1997.

through the homogeneity contained within them. Show me a computer virus and I'll show you proprietary software with a market monopoly.

I will not repeat here the excellent attention given to the subject by CAE, Lovink, and others. Instead in this chapter I would like to examine tactical media as *those phenomena that are able to exploit flaws in protocological and proprietary command and control, not to destroy technology, but to sculpt protocol and make it better suited to people's real desires.* "Resistances are no longer marginal, but active in the center of a society that opens up in networks,"[2] Hardt and Negri remind us. Likewise, techno-resistance is not outside protocol but at its center. Tactical media propel protocol into a state of hypertrophy, pushing it further, in better and more interesting ways.

Computer Viruses

While a few articles on viruses and worms appeared in the 1970s and beginning of the 1980s,[3] Frederick Cohen's work in the early 1980s is cited as the first sustained examination of computer viruses. He approached this topic from a scientific viewpoint, measuring infection rates, classifying different types of viruses, and so on.

> The record for the smallest virus is a Unix "sh" command script. In the command interpreter of Unix, you can write a virus that takes only about 8 characters. So, once you are logged into a Unix system, you can type a 8 character command, and before too long, the virus will spread. That's quite small, but it turns out that with 8 characters, the virus can't do anything but reproduce. To get a virus that does interesting damage, you need around 25 or 30 characters. If you want a virus that evolves, replicates, and does damage, you need about 4 or 5 lines.[4]

---

2. Michael Hardt and Antonio Negri, *Empire* (Cambridge: Harvard University Press, 2000), p. 25.

3. Ralf Burger cites two articles: "ACM Use of Virus Functions to Provide a Virtual APL Interpreter Under User Control" (1974), and John Shoch and Jon Huppas's "The Worm Programs—Early Experience with a Distributed Computation" (1982), which was first circulated in 1980 in abstract form as "Notes on the 'Worm' programs" (IEN 159, May 1980). See Ralf Burger, *Computer Viruses* (Grand Rapids: Abacus, 1988), p. 19.

4. Frederick Cohen, *A Short Course on Computer Viruses* (New York: John Wiley & Sons, 1994), p. 38.

Cohen first presented his ideas on computer viruses to a seminar in 1983. His paper "Computer Viruses—Theory and Experiments" was published in 1984, and his Ph.D. dissertation titled "Computer Viruses" (University of Southern California) in 1986.

Cohen defines a computer virus as "a program that can 'infect' other programs by modifying them to include a, possibly evolved, version of itself."[5] Other experts agree: "a virus is a self-replicating code segment which must be attached to a host executable."[6] Variants in the field of malicious code include worms and Trojan horses. A worm, like a virus, is a self-replicating program but one that requires no host to propagate. A Trojan horse is a program that appears to be doing something useful but also executes some piece of undesirable code hidden to the user.

In the literature viruses are almost exclusively characterized as hostile or harmful. They are often referred to completely in the negative, as in "anti-virus software" or virus prevention, or as one author calls it, a "high-tech disease." They are considered nearly exclusively in the context of detection, interception, identification, and removal.

Why is this the case? Viral marketing, emergent behavior, self-replicating systems—these concepts are all the rage at the turn of the millennium. Yet computer viruses gain from none of these positive associations. They are thought of as a plague used by terrorists to wreak havoc on the network.

So why did computer viruses become so closely connected with the viral metaphor in biology? Why think of self-replicating programs as a "virus" and not simply a parasitic nuisance, or a proper life form? Even the father of computer virus science, Cohen, thought of them as a form of artificial life[7]

---

5. Cohen, *A Short Course on Computer Viruses*, p. 2.

6. W. Timothy Polk et al., *Anti-Virus Tools and Techniques for Computer Systems* (Park Ridge, NJ: Noyes Data Corporation, 1995), p, 4.

7. Indeed pioneering viral scientist Frederick Cohen is the most notable exception to this rule. He recognized the existence of "benevolent viruses" that perform maintenance, facilitate networked applications, or simply live in "peaceful coexistence" with humans: "I personally believe that reproducing programs are living beings in the information environment." See Cohen, *A Short Course on Computer Viruses*, pp. 159–160, 15–21, and Frederick Cohen, *It's Alive!* (New York: John Wiley & Sons, 1994). The author Ralf Burger is also not completely

and recognized the limitations of the biological analogy. "[C]onsider a biological disease that is 100% infectious, spreads whenever animals communicate, kills all infected animals instantly at a given moment, and has no detectable side effect until that moment,"[8] wrote Cohen, identifying the ultimate inaccuracy of the analogy. How did self-replicating programs *become viruses?*

For example, if viruses had emerged a decade later, in the late 1990s, it is likely that they would have a completely difference sociocultural meaning. They would most certainly be thought of more as a distributed computing system (like SETI@home) or an artificial life experiment (like Tom Ray's *Tierra*), or an artwork (like Mark Daggett's email worm, *vcards*), or as a nuisance (spam), or as a potential guerilla marketing tool (adware)—not a biological infestation.

Computer viruses acquired their current discursive position because of a unique transformation that transpired in the mid-1980s around the perception of technology. In fact several phenomena, including computer hacking, acquired a distinctly negative characterization during this period of history because of the intense struggle waging behind the scenes between proprietary and protocological camps.

My hypothesis is this: Early on, computer viruses were identified with the AIDS epidemic. It is explicitly referenced in much of the literature on viruses, making AIDS both the primary biological metaphor and primary social anxiety informing the early discourse on computer viruses. In that early mode, the virus itself was the epidemic. Later, the discourse on viruses turned toward weaponization and hence terrorism. Here, the virus author is the epidemic. Today the moral evaluation of viruses is generally eclipsed by the search for their *authors,* who are prosecuted as criminals and often terrorists. The broad viral epidemic itself is less important than the *criminal mind*

---

pessimistic, instructing readers that when "used properly, [viruses] may bring about a new generation of self-modifying computer operating systems. . . . Those who wish to examine and experiment with computer viruses on an experimental level will quickly discover what fantastic programming possibilities they offer." See Burger, *Computer Viruses,* p. 2.

8. Frederick Cohen, "Implications of Computer Viruses and Current Methods of Defense," in *Computers Under Attack: Intruders, Worms, and Viruses,* ed. Peter Denning (New York: ACM, 1990), p. 383.

that brings it into existence (or the flaws in proprietary software that allow it to exist in the first place).

Thus, by the late 1990s viruses are the visible indices of a search for evildoers within technology, not the immaterial, anxious fear they evoked a decade earlier with the AIDS crisis.

Computer viruses appeared in a moment in history where the integrity and security of bodies, both human and technological, was considered extremely important. Social anxieties surrounding both AIDS and the war on drugs testify to this. The AIDS epidemic in particular is referenced in much of the literature on viruses.[9] This makes sense because of the broad social crisis created by AIDS in the mid-to-late 1980s (and beyond). "In part," writes Ralf Burger, "it seems as though a hysteria is spreading among computer users which nearly equals the uncertainty over the AIDS epidemic."[10] A good example of this discursive pairing of AIDS and computer viruses is seen in the February 1, 1988, issue of *Newsweek*. Here an article titled "Is Your Computer Infected?," which reports on computer viruses affecting hospitals and other institutions, is paired side-by-side with a medical article on AIDS.

Consider two examples of this evolving threat paradigm. The Jerusalem virus[11] was first uncovered in December 1987 at the Hebrew University of Jerusalem in Israel. "It was soon found that the virus was extremely widespread, mainly in Jerusalem, but also in other parts of the country, especially in the Haifa area,"[12] wrote professor Yisrael Radai. Two students, Yuval Rakavy and Omri Mann, wrote a counterprogram to seek out and delete the virus.

Mystery surrounds the origins of the virus. As Cohen writes, terrorists are suspected of authoring this virus. It was timed to destroy data precisely on

---

9. See Philip Fites, Peter Johnson, and Martin Kratz, *The Computer Virus Crisis* (New York: Van Nostrand Reinhold, 1992), pp. 28, 54, 105–117, 161–162; Burger, *Computer Viruses*, p. 1; Charles Cresson Wood, "The Human Immune System as an Information Systems Security Reference Model," in *Rogue Programs*, ed. Lance Hoffman (New York: Van Nostrand Reinhold, 1990), pp. 56–57. In addition, the AIDS Info Disk, a Trojan horse, is covered in almost every book on the history of computer viruses.

10. Burger, *Computer Viruses*, p. 1.

11. Also called the "Israeli" or "PLO" virus.

12. Yisrael Radai, "The Israeli PC Virus," *Computers and Security* 8, no. 2, (1989), p. 112.

the first Friday the thirteenth it encountered, which landed on May 13, 1988, and coincided with the day commemorating forty years since the existence of a Palestinian state.[13] (A subsequent outbreak also happened on Friday, January 13, 1989 in Britain.) The *Edmonton Journal* called it the work of a "saboteur." This same opinion was voiced by *The New York Times,* who reported that the Jerusalem virus "was apparently intended as a weapon of political protest."[14] Yet Radai claims that in subsequent, off-the-record correspondence, the *Times* reporter admitted that he was "too quick to assume too much about this virus, its author, and its intent."[15]

In the end it is of little consequence whether or not the virus was written by the Palestine Liberation Organization (PLO). What matters is that this unique viral threat was menacing enough to influence the judgment of the media (and also Cohen) to believe, and perpetuate the belief, that viruses have a unique relationship to terrorists. Words like "nightmare," "destroy," "terrorist," and "havoc" pervade the *Times* report.

Second, consider the "AIDS Information Introductory Diskette Version 2.0" Disk. On December 11, 1989, the PC Cyborg Corporation mailed approximately 10,000[16] computer diskettes to two direct mail lists compiled from the subscribers to *PC Business World* and names from the World Health Organization's 1988 conference on AIDS held in Stockholm.[17] The disk, which carried the title "AIDS Information Introductory Diskette Version 2.0," presented an informational questionnaire to the user and offered an assessment of the user's risk levels for AIDS based on his or her reported behavior.

The disk also acted as a Trojan horse containing a virus. The virus damages file names on the computer and fills the disk to capacity. The motives of the virus author are uncertain in this case, although it is thought to be a

---

13. Cohen, *A Short Course on Computer Viruses,* p. 45.

14. "Computer Systems Under Siege, Here and Abroad," *The New York Times,* January 31, 1988, section 3, p. 8.

15. Cited in Radai, "The Israeli PC Virus," p. 113.

16. Frederick Cohen reports the total number between 20,000 and 30,000 diskettes. See Cohen, *A Short Course on Computer Viruses,* p. 50. Jan Hruska puts the number at 20,000. See Hruska, *Computer Viruses and Anti-Virus Warfare,* p. 20.

17. Philip Fites et al., *The Computer Virus Crisis,* p. 46.

rather ineffective form of extortion because users of the disk were required to mail payment of $189 (for a limited license) or $378 (for a lifetime license) to a post office box in Panama.

The virus author was eventually discovered to be an American named Joseph Popp who was extradited to Britain in February 1991 to face charges but was eventually dismissed as being psychiatrically unfit to stand trial.[18] He was later found guilty in absentia by an Italian court.

Other AIDS-related incidents include the early Apple II virus "Cyber-aids," the AIDS virus from 1989 that displays the message "Your computer now has AIDS" in large letters, followed a year later by the AIDS II virus that performs a similar infraction.

So here are two threat paradigms, terrorism and AIDS, which characterize the changing discursive position of computer viruses from the 1980s to 1990s. While the AIDS paradigm dominated in the late 1980s, by the late 1990s computer viruses would become weaponized and more closely resemble the terrorism paradigm.

The AIDS epidemic in the 1980s had a very specific discursive diagram. With AIDS, the victims became known, but the epidemic itself was unknown. There emerged a broad, immaterial social anxiety. The biological became dangerous and dirty. All sex acts became potentially deviant acts and therefore suspect.

But with terrorism there exists a different discursive diagram. With terror the victims are rarely known. Instead knowledge is focused on the threat itself—the strike happened here, at this time, with this weapon, by this group, and so on.

If AIDS is an invisible horror, then terror is an irrational horror. It confesses political demands one minute, then erases them the next (while the disease has *no* political demands). The state attacks terror with all available manpower, while it systematically ignores AIDS. Each shows a different exploitable flaw in protocological management and control.

While the shift in threat paradigms happened in the late 1980s for computer viruses, the transformation was long in coming. Consider the following three dates.

---

18. Hruska, *Computer Viruses and Anti-Virus Warfare*, p. 22.

In the 1960s in places like Bell Labs,[19] Xerox PARC and MIT scientists were known to play a game called Core War. In this game two self-replicating programs were released into a system. The programs battled over system resources and eventually one side came out on top. Whoever could write the best program would win.

These engineers were not virus writers, nor were they terrorists or criminals. Just the opposite, they prized creativity, technical innovation, and exploration. Core War was a fun way to generate such intellectual activity. The practice existed for several years unnoticed. "In college, before video games, we would amuse ourselves by posing programming exercises," said Ken Thompson, co-developer of the UNIX operating system, in 1983. "One of the favorites was to write the shortest self-reproducing program."[20] The engineer A. K. Dewdney recounts an early story at, I assume, Xerox PARC about a self-duplicating program called Creeper that infested the computer system and had to be brought under control by another program designed to neutralize it, Reaper.[21] Dewdney brought to life this battle scenario using his own gaming language called Redcode.

Jump ahead to 1988. At 5:01:59 p.m.[22] on November 2 Robert Morris, a 23-year-old graduate student at Cornell University and son of a prominent computer security engineer at the National Computer Security Center (a division of the NSA), released an email worm into the ARPAnet. This self-

---

19. A. K. Dewdney identifies a game called Darwin invented by M. Douglas McIlroy, head of the Computing Techniques Research Department at Bell Labs, and a program called Worm created by John Shoch (and Jon Hupp) of Xerox Palo Alto Research Center. See A. K. Dewdney, "Computer Recreations," *Scientific American,* March 1984, p. 22. For more on Shoch and Hupp, see "The Worm Programs," *Communications of the ACM,* March 1982. Many attribute the worm concept to the science fiction novel *Shockwave Rider* by John Brunner.

20. Ken Thompson, "Reflections on Trusting Trust," in *Computers Under Attack: Intruders, Worms, and Viruses,* ed. Peter Denning (New York: ACM, 1990), p. 98.

21. Dewdney, "Computer Recreations," p. 14.

22. Jon A. Rochlis and Mark W. Eichin, "With Microscope and Tweezers: The Worm from MIT's Perspective," in *Computers Under Attack: Intruders, Worms, and Viruses,* ed. Peter Denning (New York: ACM, 1990), p. 202. The precise time comes from analyzing the computer logs at Cornell University. Others suspect that the attack originated from a remote login at a MIT computer.

replicating program entered approximately 60,000[23] computers in the course of a few hours, infecting between 2,500 and 6,000 of them. While it is notoriously difficult to calculate such figures, some speculations put the damage caused by Morris's worm at over $10,000,000.

On July 26, 1989, he was indicted under the Computer Fraud and Abuse Act of 1986. After pleading innocent, in the spring of 1990 he was convicted and sentenced to three years' probation, fined $10,000, and told to perform four hundred hours of community service. Cornell expelled him, calling it "a juvenile act,"[24] while Morris's own dad labeled it simply "the work of a bored graduate student."[25]

While the media cited Morris's worm as "the largest assault ever on the nation's computers,"[26] the program was largely considered a sort of massive blunder, a chain reaction that spiraled out of control through negligence. As Bruce Sterling reports: "Morris said that his ingenious 'worm' program was meant to explore the Internet harmlessly, but due to bad programming, the worm replicated out of control."[27] This was a problem better solved by the geeks, not the FBI, thought many at the time. "I was scared," admitted Morris. "It seemed like the worm was going out of control."[28]

Morris's peers in the scientific community considered his prosecution unnecessary. As reported in *UNIX Today!*, only a quarter of those polled thought

---

23. Cohen, *A Short Course on Computer Viruses*, p. 49. The figure of 60,000 is also used by Spafford, who attributes it to the October 1988 IETF estimate for the total number of computers online at that time. See Eugene Spafford, "The Internet Worm Incident," in *Rogue Programs*, ed. Lance Hoffman (New York: Van Nostrand Reinhold, 1990), p. 203. Peter Denning's numbers are different. He writes that "[o]ver an eight-hour period it invaded between 2,500 and 3,000 VAX and Sun computers." See Denning, ed., *Computers Under Attack: Intruders, Worms, and Viruses* (New York: ACM, 1990), p. 191. This worm is generally called the RTM Worm after the initials of its author, or simply the Internet Worm.

24. From a Cornell University report cited in Ted Eisenberg et al., "The Cornell Commission: On Morris and the Worm," in *Computers Under Attack: Intruders, Worms, and Viruses* (New York: ACM, 1990), p. 253.

25. Cited in *The New York Times*, November 5, 1988, p. A1.

26. *The New York Times*, November 4, 1988, p. A1.

27. Bruce Sterling, *The Hacker Crackdown* (New York: Bantam, 1992), pp. 88–89.

28. Cited in *The New York Times*, January 19, 1990, p. A19.

Morris should go to prison, and, as the magazine testified, "most of those who said 'Yes' to the prison question added something like, 'only a minimum security prison—you know, like the Watergate people vacationed at.'"[29] Thus while not unnoticed, Morris's worm was characterized as a mistake, not an overt criminal act. Likewise his punishment was relatively lenient for someone convicted of such a massive infraction.

Ten years later, in 1999, after what was characterized as the largest Internet manhunt ever, a New Jersey resident named David Smith was prosecuted for creating Melissa, a macro virus that spreads using the Microsoft Outlook and Word programs. It reportedly infected over 100,000 computers worldwide and caused $80 million in damage (as assessed by the number of hours computer administrators took to clean up the virus). While Melissa was generally admitted to have been more of a nuisance than a real threat, Smith was treated as a hard criminal rather than a blundering geek. He pleaded guilty to ten years and a $150,000 fine.

With Smith, then, self-replicating programs flipped 180 degrees. The virus is now indicative of criminal wrongdoing. It has moved through its biological phase, characterized by the associations with AIDS, and effectively been weaponized. Moreover criminal blame is identified with the virus author himself who is thought of not simply as a criminal but as a cyberterrorist. A self-replicating program is no longer the hallmark of technical exploration, as it was in the early days, nor is it (nor was it ever) a canary in the coal mine warning of technical flaws in proprietary software, nor is it even *viral;* it is a weapon of mass destruction. From curious geek to cyberterrorist.

Cyberfeminism

Decades after programmers and pundits alike had safely agreed that computers were, at the end of the day, a decidedly *male* operation—for who else but the old boy's academo-military network had created the Internet, the

---

29. "Morris's Peers Return Verdicts: A Sampling of Opinion Concerning The Fate of the Internet Worm," in *Rogue Programs,* ed. Lance Hoffman (New York: Van Nostrand Reinhold, 1990), p. 104.

personal computer, cyberspace, viruses, video games, multimedia,[30] and so on—cultural critic Sadie Plant had this to say: "Hardware, software, wetware—before their beginnings and beyond their ends, women have been the simulators, assemblers, and programmers of the digital machines."[31] That the three occupations named here carry less clout then others one can imagine (Engineer, CEO, etc.) does not diminish the strength of Plant's argument: that computers are, and have always been, a technology of the female. Plant's coup is the unveiling of Ada Lovelace, a female protagonist drawn from computing prehistory. More on her later. Plant reaches beyond mythmaking—for what else can Lovelace be at this stage in the game—into a complex relationship between women and machines. This relationship, tied up in problematics surrounding identity, technology, and the body, is at the heart of the 1990s movement called cyberfeminism.

Cyberfeminism is a type of tactical media. It reflects on the totality of protocological command and control. Cyberfeminism adds a new dimension to the discussion begun in the previous sections on hackers and viruses, for this new strain deals with the negative space created within protocol through the injection of mutations, crashes, and viral code. With cyberfeminism, protocol becomes disturbed. Its course is altered and affected by the forces of randomness and corruption.

Indeed it is possible to think of cyberfeminism itself as a type of virus, a bug within the larger protocological network. Sadie Plant and others have identified Grace Hopper as the discoverer of the first computer bug. The bug was quite literally that, a moth caught in the innards of an early computing machine. The moth disrupted the normal functioning of the machine. Henceforth the term *bug* has been used to describe logical mistakes or glitches in computer code.

The computer bug, far from being an unwanted footnote in the history of computing, is in fact a space where some of the most interesting protocological

---

30. Packer and Jordan's 2001 anthology *Multimedia: From Wagner to Virtual Reality* is one of the more egregious examples. While their anthology is interesting, they essentially remove women from the history of multimedia, publishing in the first edition only one female author out of thirty-two texts, then adding a very short coda from Laurie Anderson in the "expanded" edition.
31. Sadie Plant, *Zeros and Ones* (New York: Doubleday, 1997), p. 37.

phenomena occur. Bugs, crashes, and viruses have always existed. (I argue in the last chapter that crashes actually define certain genres of contemporary Net art.) They are a sort of super-protocological mutation that can, at times, propel technology in interesting new ways.

"[O]ne of the guys [at ARPA] wrote a program called 'The Unknown Glitch,'" remembers computer pioneer Alan Kay, "which at random intervals would wake up, print out I AM THE UNKNOWN GLITCH. CATCH ME IF YOU CAN, and then it would relocate itself somewhere else in core memory, set a clock interrupt, and go back to sleep. There was no way to find it."[32] This Unknown Glitch was not anti-protocol by any means, for the very environment in which it thrived was the computer itself. Yet at the same time, the Glitch exists outside of the normal functionality of protocol. It is a liminal agent, at once inside protocol and outside its reach. This is the same status that cyberfeminism has now assumed.

The logical exploits described in chapter 5 also have immense implications in the realm of computer viruses. Computer viruses are, in essence, machines for the exploitation of logical flaws within a computer system. Viruses are not alive, at least not in any conventional sense of the word. But they are vital forms from the perspective of the "machinic phylum," that stratum of our material world populated by both physical and biological machines.

While they are often small, a virus's internal structure can be incredibly sophisticated. "What we have here is perhaps the most complex and refined malicious code in the history of virus writing," comments Eugene Kaspersky, Head of Company Anti-Virus Research Center, on the Hybris virus. "Firstly, it is defined by an extremely complex style of programming. Secondly, all the plugins are encrypted with very strong RSA 128-bit crypto-algorithm key. Thirdly, the components themselves give the virus writer the possibility to modify his creation 'in real time,' and in fact allow him to control infected computers worldwide."[33]

Viruses propagate themselves through weaknesses in the logical structure of computer code. Hackers often argue, in fact, that the logical weaknesses

---

32. Alan Kay, cited in Stewart Brand, "SPACEWAR: Fanatic Life and Symbolic Death Among the Computer Bums," *Rolling Stone,* December 7, 1972, p. 52.

33. Cited online at http://www.kaspersky.com.

themselves are the real problem, not the viruses that simply exploit the weakness. What is truly to blame, the water leaking from a bucket, or the hole in that bucket that allows the water to leak? Or, as the hacker magazine *2600* asked in response to the massive disturbance ($10 million of damage by professional estimates) caused by the "I Love You" virus: "How could it be possible to completely gloss over the fact that, once again, all of the problems were because of a gaping weakness in a program called Microsoft Outlook and that this is a lesson that should have been learned from the Melissa virus a year earlier?"[34] The affliction then becomes Microsoft Outlook—an anti-protocol application—not the "I Love You" virus.

(The addition of the virus deliberately complicates the issue, for if Microsoft Outlook were not monopolistic in the marketplace it would not as easily fall prey to infection. The greater saturation a particular application has, the higher likelihood that a virus will be able to spread. Either way, I draw a critical distinction in this book between proprietary software that happens to have a market monopoly and the universalism of a protocological technology.)

"The territory of cyberfeminism is large," write Faith Wilding and Critical Art Ensemble in their study of cyberfeminism. "It includes the objective arenas [of] cyberspace, institutions of industrial design, and institutions of education—that is, those arenas in which technological process is gendered in a manner that excludes women from access to the empowering points of techno-culture."[35]

History confirms this breadth. The first "Cyberfeminist Manifesto" appeared in the early nineties, written by a renegade group of Australian artists and activists calling themselves VNS Matrix. After this early rant, the cyberfeminist movement quickly grew on an international scale. On September 20, 1997, in Kassel, Germany, the First Cyberfeminist International met at Documenta X, an international exhibition of contemporary art.

Cyberfeminism in its very nature necessitates a participatory practice in which many lines of flight coexist. Yet several recurrent themes emerge,

---

34. "Madness," *2600* (Summer 2000), p. 5.

35. Faith Wilding and Critical Art Ensemble, "Notes on the Political Condition of Cyberfeminism," available online at http://www.obn.org/cfundef/condition.html.

among them the questions of *body* and *identity.* Like a computer virus, cyberfeminism exists to mutate and transform these questions, guiding them in new directions within the protocological sphere.

Sadie Plant and Allucquère Rosanne "Sandy" Stone are perhaps the two best entry points into contemporary cyberfeminist theory. It is Plant's view that technology is fundamentally female—not male as the legions of geeks, computer science teachers, and *Wired* magazine editors would have one believe. Stone, on the other hand, focuses on how virtual communities, far from being simple gathering places, actually *produce* things like bodies, identities, and spaces.

Like French feminist Luce Irigaray before her, Plant argues that patriarchal power structures, which have unequally favored men and male forms in society, should be made more equal through a process of revealing and valorizing overlooked female elements.

Her book *Zeros and Ones* turns on the story of Ada Lovelace, the world's first computer programmer. As assistant to Charles Babbage, Lovelace helped build early calculation machines that many consider critical to the prehistory of computer science. Championing Lovelace over Babbage, Plant's goal is to recuperate this lost female origin from within the history of technology.[36]

However, as her manifesto-like "Feminisations: Reflections on Women and Virtual Reality" shows, Plant wishes not to valorize some negative space created by patriarchy, but to unveil the always already feminine space of technology. This is ultimately a more powerful move, for instead of simply objecting to past inequalities, it reveals how many of those inequalities were unfounded. "Masculine identity has everything to lose from this new technics," prophesizes Plant. "The sperm count falls as the replicants stir and the meat learns how to learn for itself. Cybernetics is feminisation."[37]

The universality of protocol can give feminism something that it never had at its disposal, the obliteration of the masculine from beginning to end.

---

36. Ada Lovelace's influence has not been completely lost. Aside from her roles in various science fiction novels, there is the late, eponymous Web art site äda 'web (http://adaweb.walkerart.org) and Lynn Hershman Leeson's film *Conceiving Ada.*

37. Sadie Plant, "Feminisations: Reflections on Women and Virtual Reality," in *Clicking In,* ed. Lynn Hershman Leeson (Seattle: Bay Press, 1996), p. 37.

With inspiration from the VNS Matrix (self-styled "saboteurs of Big Daddy Mainframe"), Plant begins to define this pure feminine space and how it can inflect protocological space.

Zeros and Ones persuasively shows how women have always been inextricably involved with protocological technology. Using the telephone operator as an example, she argues that women have traditionally comprised the laboring core of networks of all kinds, particularly the telecommunications networks. From the power loom to typewriting, (even to the discovery of the computer bug), Plant categorizes technology as a fundamentally female object. Even the zero—the nothingness of binary code—has always been the 0-ther, the female.

On the writing of *Zeros and Ones,* Plant remembers: "When I started the book it was really to try and correct, what I thought was the great misconception at the moment about the relationship between women and computers in particular and technology in general. It seemed to me, that a lot of 'orthodox' feminist theory was still very technophobic."[38]

Technophobic she is not. Throughout Plant's book the intersection of woman and the protocological matrix is primary. This materializes itself historically in the matrix-based weaving processes of industrial power looms, in the predominantly female operators of phone networks, in the trope of the woman as computer programmer (Ada Lovelace, Grace Hopper) and in the weblike structure of cyberspace. Because of this history, Plant writes that technology threatens phallic control and is fundamentally a process of emasculation. "The matrix weaves itself in a future which has no place for historical man,"[39] says Plant. The digital provides a space of valences that exists outside of and potentially preempts patriarchal structures.

In other words, as protocol rises, patriarchy declines. As Plant describes it, "The introduction of binary code introduces a plane of equivalence which undermines the very foundations of a world in which male and female have played the roles of superstructure and material base."[40] In this model, binary

---

38. Available online at http://www.t0.or.at/sadie/intervw.htm.

39. Sadie Plant, "The Future Looms: Weaving Women and Cybernetics," in *Clicking In,* ed. Lynn Hershman Leeson (Seattle: Bay Press, 1996), p. 132.

40. Available online at http://www.t0.or.at/sadie/binary.htm.

code replaces what have traditionally been the producers of value, these being the phallus, the law, the father, and so on.

This process was described in chapter 1 as the movement from a structure based on hierarchy and centralized control to one based on horizontality and distributed control.

In Plant, technology is less a question of good or bad and more the possibility of an objective weakening of patriarchy (or its technological synonym, "propriety"). Cyberfeminism, for Plant, implies that an alliance "is being developed between women, machinery and the new technology that women are using."[41] And that new technology is, of course, protocol.

Held aloft, yet notably aloof from the cyberfeminist movement, is Sandy Stone, theorist of the history of cyberspace, desire, and the virtual body.[42] Stone's early essay "Will the Real Body Please Stand Up?"[43] helped set the stage for contemporary debates on the status of the body in virtual communities.

The place of the body is central to cyberfeminism. Yet in this analysis, bodies are not natural objects made of flesh and blood, but rather are complex intersections of materiality and meaning. Stone argues that binarisms such as nature/culture actually function logically as "a strategy for maintaining boundaries for political and economic ends, and thus a way of making meaning."[44] In this way, the insertion of the body into protocological space actually produces meaning through the articulation of differences between bodies and non-bodies, between spaces and non-spaces.

Like Foucault's rejection of the "repressive hypothesis" in Volume 1 of his influential *History of Sexuality,* Stone claims that new technologies are not transparent agents that remove issues of gender from view, but rather they proliferate the production and organization of gendered bodies in space. She

---

41. Available online at http://206.251.6.116/geekgirl/001stick/sadie/sadie.html.

42. A good place to start with Stone is her homestead at http://sandystone.com/. Although her published material is readily available, online users may access digitized versions of articles including "The Empire Strikes Back," "Violation & Virtuality," and "What Vampires Know" at http://eserver.org/gender/.

43. Allucquère Rosanne Stone, "Will the Real Body Please Stand Up?," in *Cyberspace: First Steps,* ed. Michael L. Benedikt (Cambridge: MIT Press, 1992).

44. Stone, "Will the Real Body Please Stand Up?," p. 102.

shows that the dominant spatial metaphor for interactions in virtual spaces is, simply enough, the metaphor of our daily physical, Cartesian space. And like our offline space, virtual spaces are inhabited by bodies with "complex erotic components."[45]

This working metaphor is of course totally arbitrary, as Stone points out, since there is nothing in the logic of digital networks that necessarily prestructures itself as Cartesian, or body-based, or desiring. On the contrary, digital networks are non-Cartesian, are bodyless, and have little connection to the movements of human desire. Through the introduction of tactical protocols, which are always negotiated and agreed to in advance by all participants, digital networks *become* Cartesian, body-based, desiring, and so on. Cyberfeminism is the tactical process by which this reification will be refashioned.

Stone shows that communications technology is conventionally thought of as "1) an apparatus for the production of community . . . 2) an apparatus for the production of body . . . [and] 3) a mediating [agent] between bodies and selves . . . i.e., interfaces."[46] Protocological space is imagined as a prosthesis, as an enormous extension of one's physical body, and through this giant phantom limb (the Net) one interacts with other virtual bodies.

Participants in online communities like the object-oriented social spaces called MOOs "learn to delegate their agencies to body representatives [avatars] that exist in imaginal spaces contiguously with representatives of other individuals."[47] The creators of one of the most popular MOOs, LambdaMOO, describe this relationship of bodies in social terms: "LambdaMOO is a new kind of society, where thousands of people voluntarily come together from all over the world."[48] As Stone and others show, a participatory social practice (i.e., community) based on an imagined ether-scape of desiring and interacting bodies (i.e., protocol) is basic to how one conceptualizes digital spaces.

Cyberfeminist pioneers VNS Matrix provide the frontline guerrilla tactics for Stone and Plant's theoretical efforts. VNS Matrix emerged from

---

45. Stone, "Will the Real Body Please Stand Up?," p. 105.

46. Allucquère Rosanne Stone, *The War of Desire and Technology at the Close of the Machine Age* (Cambridge: MIT Press, 1995), p. 89.

47. Stone, *The War of Desire and Technology at the Close of the Machine Age*, p. 121.

48. LambdaMOO (telnet://lambda.moo.mud.org:8888).

Adelaide, Australia, in the summer of 1991. Francesca da Rimini (also known as Gashgirl and/or Doll Yoko) gives her story of how it all started:

> Like all good coagulating stories it starts with slime, and maybe ends with blood. I live on the edge of the Australian desert in a small town of lies and whispers with a palpable palpitating underbelly . . . It was the summer of 91. Definitely not the summer of love. We were four girls. We were hot and bored and poor (for me not much has changed, except I am no longer bored). We decided to try and crack the porn cartel with some chick porn. We made some images on stolen computers, Beg, Bitch, Fallen, Snatch. We decided it was more fun playing with computers than endlessly scanning our pussies and so Velvet Downunder morphed into VNS Matrix.[49]

VNS Matrix are Josephine Starrs, Julianne Pierce, Francesca da Rimini and Virginia Barratt,[50] who have perpetrated a series of cyberfeminist interventions including a "bad code" anti-video game targeted at girls (or at least not targeted at 14-year-old boys). Da Rimini (using the pseudonym Doll Yoko) writes, "cyberfeminism/s has become the field from which i work, from which multiple lines of flight errupt anarchically, generating dialogues, relations, conceptual and physical objects."[51]

The original VNS Matrix Cyberfeminist Manifesto effectively captures her sentiment:

> we are the modern cunt
> positive anti reason
> unbounded unleashed unforgiving
> we see art with our cunt we make art with our cunt
> we believe in jouissance madness holiness and poetry
> we are the virus of the new world disorder
> rupturing the symbolic from within
> saboteurs of big daddy mainframe
> the clitoris is a direct line to the matrix

---

49. Available online at http://www.thing.net/~rdom/janrev97.01.html.
50. Available online at http://sysx.apana.org.au/artists/vns/.
51. Available online at http://sysx.apana.org.au/artists/vns/.

VNS MATRIX
terminators of the moral code
mercenaries of slime
go down on the altar of abjection
sucking the visceral temple we speak in tongues
infiltrating disrupting disseminating
corrupting the discourse
we are the future cunt[52]

Its slogan, "the clitoris is a direct line to the matrix," is meant to highlight a fundamental material coexistence between the machine and the female body.

Originally ignorant of the work of Sadie Plant, VNS Matrix built its own praxis centered on women and technology. Pierce notes, "at the same time as we started using the concept of cyberfeminism, it also began to appear in other parts of the world. It was like a spontaneous meme which emerged at around the same time, as a response to ideas like 'cyberpunk' which were popular at the time. Since then the meme has spread rapidly and is certainly an idea which has been embraced by many women who are engaged with techno theory and practice."[53]

Pierce notes that cyberfeminists have never been anti-protocol, but rather use protocological machines as an integral part of their political action, art, and writing. Da Rimini (writing as Doll Yoko) posted in June 1997, to the *Nettime* email list[54] that "as artists, [VNS Matrix] were serious bout usin strategies like irony 'n inversion of cultural stereotypes to raise some of the many issues around women and technology . . . access . . . education . . . jobs . . . portrayal of girls/chix/women in popular/games culture etc etc."[55] Da Rimini's writing style is typical of the VNS Matrix brand of cyberfeminism, a crude, confrontational liberationist politics for women in the digital matrix.

---

52. Available online at http://www.t0.or.at/dolores/manifesto/vnstoc.htm.

53. Available online at http://web.aec.at/www-ars/matrix.html.

54. *Nettime* is an email community devoted to "net criticism, collaborative text filtering and cultural politics of the nets." More information is available online at http://www.nettime.org.

55. Francesca da Rimini (as Doll Yoko), "bossy cunts online," *Nettime*, June 18, 1997.

Here are a few questions and answers I was able to pose to the VNS Matrix:

As part of VNS Matrix you helped coin the term "cyberfeminist." It seems that term had a rather short life—maybe 1991–1998? Do you consider this term dated or still relevant?
Josephine Starrs: I think cyberfeminism will go down in history with the other great avant-garde movements such as dadaism, surrealism and the situationists.
Francesca da Rimini: There are a number of chix in australia and the states and europe who are now identifying as "cyberfeminists" and exploring various philosophical, political and social implications of what it all might mean and do. I was deeply engaged with this debate in the early 90s, and as a member of VNS Matrix helped to make quite a prolific body of artwork and narrative texts which played with some of the issues surrounding the relations of gender and technology. but that was then, and now I've moved on to explore other fields of enquiry and media activism. But of course I still identify as a feminist, if not a cyberfeminist.

Throughout all of cyberfeminist theory the theme of bodies and identities dominates. As one essay notes, "Bodies generally are all the rage on the Net—whether they are obsolete, cyborg, techno, porno, erotic, morphed, recombined, phantom, or viral."[56] Indeed, much of the focus on bodies stems from the process of forgetting the body (or trying to forget about forgetting the body!).

As Stone and others have written, the advent of cyberspace is the story of bodies migrating and morphing into new contexts. In fact, Lynn Hershman Leeson goes so far as to claim that "new [Web] users are forming the largest immigration in history"[57]—a powerful idea to keep in mind, that computer use could possibly constitute a real *immigration* of bodies (from the offline to the online).

Cyberfeminism aims to exorcise the essentialized, uninterrogated female body (brought into existence as a by-product of the protocological revolution) through a complex process of revalorization and rebuilding.

---

56. Faith Wilding and Critical Art Ensemble, "Notes on the Political Condition of Cyberfeminism."

57. Lynn Hershman Leeson, "Romancing the Anti-Body: Lust and Longing in (Cyber)space," in *Clicking In,* ed. Lynn Hershman Leeson (Seattle: Bay Press, 1996), p. 328.

The Cartesian subject is no longer relevant here, as Plant explains:

> Basically the two positions that are established at the minute are either that you talk about disembodiment or you talk about embodiment. Either you're out of the body in some stratospheric zone or you're in the organism. I think that neither of those are correct. When people talk about getting out of the body they are still assuming that there is some kind of great transcendent space like heaven for the soul, or something non-material at any rate, to occupy. And as far as I'm concerned that isn't there. The universe isn't like that, it's a material process not some sort of idealist construction. So you can't get out of matter, that's the crucial thing. But you can get out of the confining organization of matter which is shaped into things and of course, organisms. The organism is literally organized around its organs, the vocabulary says it all really.[58]

Contemporary cyberfeminist cultural production, including VNS Matrix's self-described "cunt art," follows Plant's guideline to the letter.

Like Fluxus artist Shigeko Kubota's 1965 performance "Vagina Painting" or Carolee Schneemann's "Interior Scroll" (1976), VNS Matrix focuses on a raw, fleshy, expressive use of the body.

Who are some interesting new media artists you've found that fit into the so-called "cyberfeminist" framework?

Josephine Starrs: I don't want to be exclusive . . . but my favourites have been Innen, from Hamburg, Bureau of Inverse Technology, from Australia, Mara Tralla from Estonia, Linda Dement and Zina Kaye from Australia, Rachel Baker from the UK, Rosie Cross for Geek Girl and of course there are some fabulous cyberfeminist theorists and activists.

Cyberfeminism is an attitude, not some lame revamp of seventies feminist consciousness-raising groups. I think cyberfeminists use the media and other institutions for their own subversive purposes. When VNS Matrix wrote the cyberfeminist manifesto for the 21st century and later the Bitch Mutant Manifesto, we were using language, performance, irony and humour to put flesh and filth into the machines and expose the gendered biases hardwired into computer culture.

---

58. Available online at http://www.altx.com/interviews/sadie.plant.html.

Plant, Stone, and the VNS Matrix are good allies for navigating the difficult questions that surround the tactical space of protocological networks. For, in essence, *they recognize that the "negotiatedness" of protocol, the fact that it is a universalism only achieved through prior negotiation and subsequent agreement, means that protocol can and will be different.*[59]

It matters little if gender disappears completely, or if it reemerges as a moniker of militancy. The political question is simply choosing how and when to inject change into protocol so that it aligns more closely with one's real desires about social life and how it ought better to be lived. This is the essence of tactical media.

Conflicting Diagrams

> Netwar is about the Zapatistas more than the Fidelistas, Hamas more than the Palestine Liberation Organization (PLO), the American Christian Patriot movement more than the Ku Klux Klan, and the Asian Triads more than the Costa Nostra.
>
> —JOHN ARQUILLA AND DAVID RONFELDT, *Networks and Netwars*

Arquilla and Ronfeldt coined the term *netwar,* which they define as "an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age."[60]

Throughout the years new diagrams (also called graphs or organizational designs) have appeared as solutions or threats to existing ones. Bureaucracy is a diagram. Hierarchy is one too, as is peer-to-peer. Designs come and go,

---

59. As Ben Braddock (Dustin Hoffman) says in the beginning of *The Graduate* about his future: "I want it to be . . . different."

60. Arquilla and Ronfeldt, *Networks and Netwars,* p. 6. A similar litany from 1996 reads: "netwar is about Hamas more than the PLO, Mexico's Zapatistas more than Cuba's Fidelistas, the Christian Identity Movement more than the Ku Klux Klan, the Asian Triads more than the Sicilian Mafia, and Chicago's Gangsta Disciples more than the Al Capone Gang." See John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica: Rand, 1996), p. 5.

serving as useful asset managers at one historical moment, then disappearing, or perhaps fading only to reemerge later as useful again. The Cold War was synonymous with a specific military diagram—bilateral symmetry, mutual assured destruction (MAD), massiveness, might, containment, deterrence, negotiation; the war against drugs has a different diagram—multiplicity, specificity, law and criminality, personal fear, public awareness.

This book is largely about one specific diagram, or organizational design, called distribution, and its approximate relationship in a larger historical transformation involving digital computers and ultimately the control mechanism called protocol.[61]

In this diagramatic narrative it is possible to pick sides and describe one diagram as the protagonist and another as the antagonist. Thus the rhizome is thought to be the solution to the tree,[62] the wildcat strike the solution to the boss's control, Toyotism[63] the solution to institutional bureaucracy, and so on. Alternately, terrorism is thought to be the only real threat to state power, the homeless punk rocker a threat to sedentary domesticity, the guerrilla a threat to the war machine, the temporary autonomous zone a threat to hegemonic culture, and so on.

This type of conflict is in fact a conflict between different social structures, for the terrorist threatens not only through fear and violence, but specifically through the use of a cellular organizational structure, a distributed network of secretive combatants, rather than a centralized organizational structure employed by the police and other state institutions. Terrorism is a sign that we are in a transitional moment in history. (Could there ever be anything else?) It signals that historical actors are not in a relationship of equilibrium, but are instead grossly mismatched.

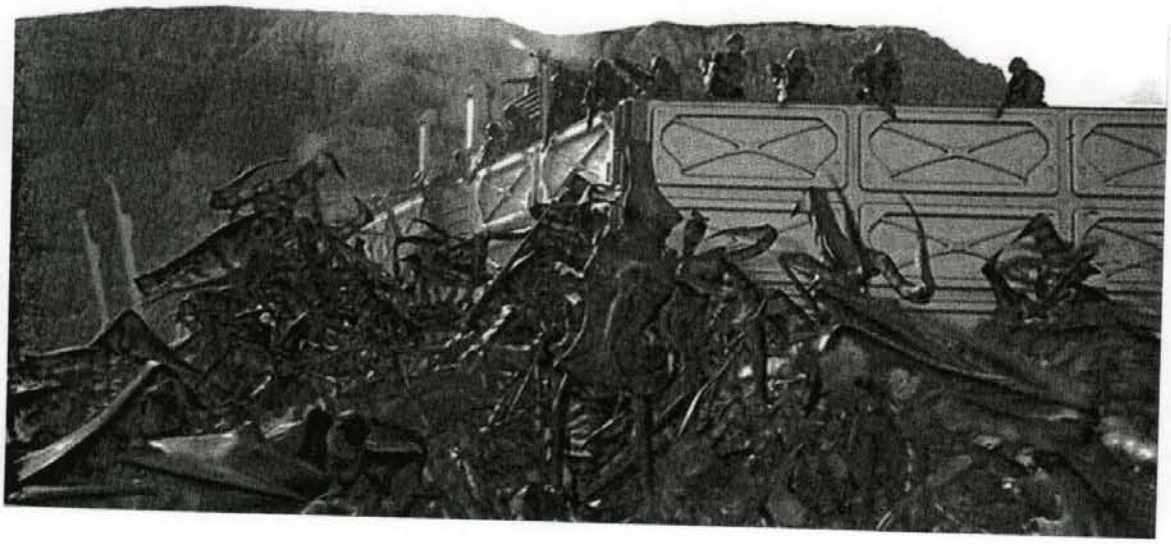
---

61. This is not a monolithic control mechanism, of course. "The Internet is a large machine," writes Andreas Broeckmann. "This machine has its own, heterogeneous topology, it is fractured and repetitive, incomplete, expanding and contracting" ("Networked Agencies," available online at http://www.v2.nl/~andreas/texts/1998/networkedagency-en.html).

62. This is Deleuze and Guattari's realization in *A Thousand Plateaus*.

63. For an interesting description of Toyotism, see Manuel Castells, *The Rise of the Network Society* (Oxford: Blackwell, 1996), pp. 157–160.

Armies facing off in *Spartacus* (1960)



Conflicting Diagrams

In recent decades the primary conflict between organizational diagrams has been between hierarchies and networks: the asymmetrical conflicts of guerrilla warfare, terrorism, and so on. But what happens when the powers-that-be get smart and actually evolve into networked power (something that has already taken place in some instances)? In the future we are likely to witness this general shift, downward into a new bilateral organizational conflict of networks fighting networks.

Bugs swarming in *Starship Troopers* (1997)

It is often observed that, due largely to the original comments of networking pioneer Paul Baran, the Internet was invented to avoid certain vulnerabilities of nuclear attack. In Baran's original vision, the organizational design of the Internet involved a high degree of redundancy, such that destruction of a part of the network would not threaten the viability of the network as a whole. After World War II, strategists called for moving industrial targets outside urban cores in a direct response to fears of nuclear attack. Peter Galison calls this dispersion the "constant vigilance against the re-creation of new centers."[64] These are the same centers that Baran derided as an "Achilles' heel"[65] and that he longed to purge from the telecommunications network.

"City by city, country by country, the bomb helped drive dispersion,"[66] Galison continues, highlighting the power of the A-bomb to drive the push toward distribution in urban planning. Whereas the destruction of a fleet of Abrams tanks would certainly impinge upon army battlefield maneuvers, the destruction of a rack of Cisco routers would do little to slow down broader network communications. Internet traffic would simply find a new route, thus circumventing the downed machines.[67]

---

64. Peter Galison, "War against the Center," *Grey Room* 4, Summer 2001, p. 20.

65. Baran writes: "The weakest spot in assuring a second strike capability was in the lack of reliable communications. At the time we didn't know how to build a communication system that could survive even collateral damage by enemy weapons. Rand determined through computer simulations that the AT&T Long Lines telephone system, that carried essentially all the Nation's military communications, would be cut apart by relatively minor physical damage. While essentially all of the links and the nodes of the telephone system would survive, a few critical points of this very highly centralized analog telephone system would be destroyed by collateral damage alone by missiles directed at air bases and collapse like a house of card." See Paul Baran, Electrical Engineer, an oral history conducted in 1999 by David Hochfelder, IEEE History Center, Rutgers University, New Brunswick, NJ, USA.

66. Galison, "War against the Center," p. 25.

67. *New Yorker* writer Peter Boyer reports that DARPA is in fact rethinking this opposition by designing a distributed tank, "a tank whose principal components, such as guns and sensors, are mounted on separate vehicles that would be controlled remotely by a soldier in yet another command vehicle." See "A Different War," *The New Yorker,* July 1, 2002, p. 61. This is what the military calls Future Combat Systems (FCS), an initiative developed by DARPA for the

(In this way, destruction must be performed absolutely, or not at all. "The only way to stop Gnutella," comments WiredPlanet CEO Thomas Hale on the popular file sharing protocol, "is to turn off the Internet."[68] And this is shown earlier in my examination of protocol's high penalties levied against deviation. One is completely compatible with a protocol, or not at all.)

Thus the Internet can survive attacks not because it is stronger than the opposition, but precisely because it is weaker. The Internet has a different diagram than a nuclear attack does; it is *in a different shape.* And that new shape happens to be immune to the older.

All the words used to describe the World Trade Center after the attacks of September 11, 2001, revealed its design vulnerabilities vis-à-vis terrorists: It was a tower, a center, an icon, a pillar, a hub. Conversely, terrorists are always described with a different vocabulary: They are cellular, networked, modular, and nimble. Groups like Al Qaeda specifically promote a modular, distributed structure based on small autonomous groups. They write that new recruits "should not know one another," and that training sessions should be limited to "7–10 individuals." They describe their security strategies as "creative" and "flexible."[69]

This is indicative of two conflicting diagrams. The first diagram is based on the strategic massing of power and control, while the second diagram is based on the distribution of power into small, autonomous enclaves. "The architecture of the World Trade Center owed more to the centralized layout of Versailles than the dispersed architecture of the Internet," wrote Jon Ippolito after the attacks. "New York's resilience derives from the interconnections it fosters among its vibrant and heterogeneous inhabitants. It is in decentralized structures that promote such communal networks, rather than in reinforced steel, that we will find the architecture of survival."[70] In the past the war against terrorism resembled the war in Vietnam, or the war

---

U.S. Army. It is described as "flexible" and "network-centric." I am grateful to Jason Spingarn-Koff for bringing FCS to my attention.

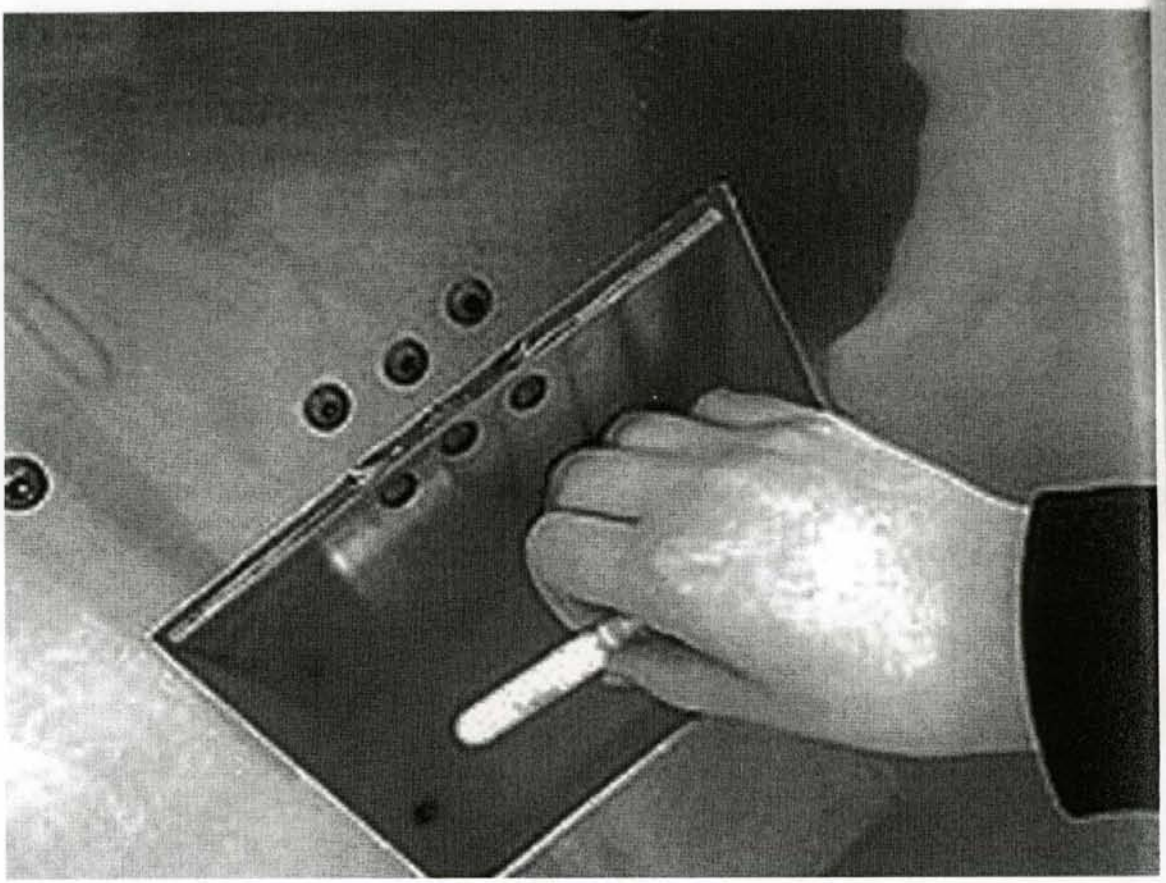
68. Cited in Gene Kan, "Gnutella," in *Peer-to-Peer: Harnessing the Power of Disruptive Technologies,* ed. Andy Oram (Sebastopol: O'Reilly, 2001), p. 99.

69. See *The al-Qaeda Documents: Vol. 1* (Alexandria, VA: Tempest, 2002), pp. 50, 62.

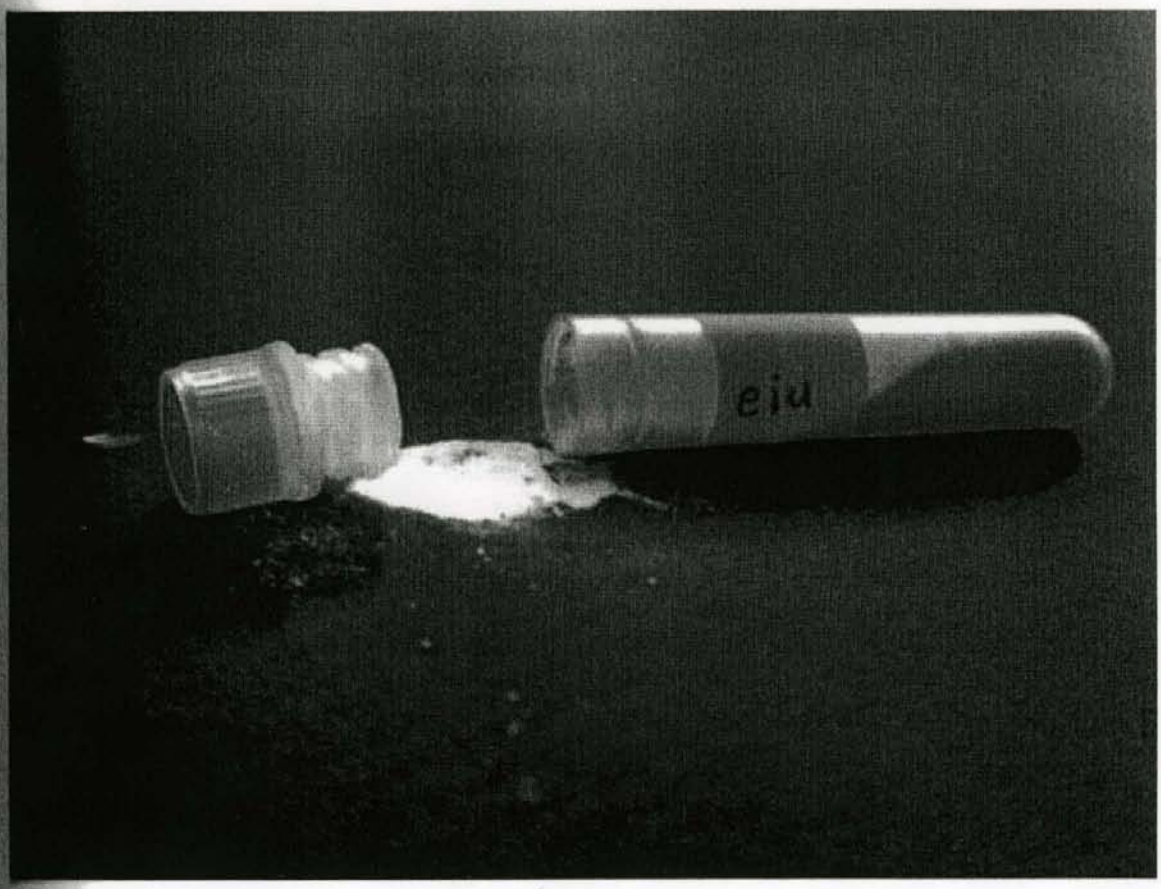
70. Jon Ippolito, "Don't Blame the Internet," *Washington Post,* September 29, 2001, p. A27.

Contagion

Early on, computer viruses were compared to biological contagion. In that early mode, the virus itself was the epidemic. Later the discourse on viruses turned toward weaponization and terrorism. Today the virus author is the epidemic, not the virus—the moral evaluation of the computer virus is eclipsed today by a search for its author, who is prosecuted as a terrorist.



Experimental Interaction Unit (www.eiu.org), *Dispersion* (1999)



against drugs—conflicts between a central power and an elusive network. It did not resemble the Gulf War, or World War II, or other conflicts between states.

"As an environment for military conflict," *The New York Times* reported, "Afghanistan is virtually impervious[71] to American power." (In addition to the stymied U.S. attempt to rout Al Qaeda post-September 11, the failed Soviet occupation in the years following the 1978 coup is a perfect example of grossly mismatched organizational designs.) Being "impervious" to American power today is no small feat.

The category shift that defines the difference between state power and guerilla force shows that through a new diagram, guerillas, terrorists, and the like can gain a foothold against their opposition. But as Ippolito points out, this should be our category shift too, for anti-terror survival strategies will arise not from a renewed massing of power on the American side, but precisely from a distributed (or to use his less precise term, decentralized) diagram. Heterogeneity, distribution, and communalism are all features of this new diagrammatic solution.

In short, *the current global crisis is one between centralized, hierarchical powers and distributed, horizontal networks.* John Arquilla and David Ronfeldt, two researchers at the Rand Corporation who have written extensively on the hierarchy-network conflict, offer a few propositions for thinking about future policy:

---

71. Wanting instead American invulnerability to Soviet nuclear power, in 1964 Paul Baran writes that "we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n [communication] stations. If n is made sufficiently large, it can be shown that highly survivable system structures can be built—even in the thermonuclear era." See Paul Baran, *On Distributed Communications: 1. Introduction to Distributed Communications Networks* (Santa Monica, CA: Rand, 1964), p. 16. Baran's point here is that destruction of a network is an all-or-nothing game. One must destroy all nodes, not simply take out a few key hubs. But the opposite is not true. A network needs only to destroy a single hub within a hierarchical power to score a dramatic triumph. Thus, Baran's advice to the American military was to become network-like. And once it did the nuclear threat was no longer a catastrophic threat to communications and mobility (but remains, of course, a catastrophic threat to human life, material resources, and so on).

- Hierarchies have a difficult time fighting networks. . . .
- It takes networks to fight networks. . . .
- Whoever masters the network form first and best will gain major advantages.[72]

These comments are incredibly helpful for thinking about tactical media and the role of today's political actor. It gives subcultures reason to rethink their strategies vis-à-vis the mainstream. It forces one to rethink the techniques of the terrorist. It also raises many questions, including what happens when "the powers that be" actually evolve into networked power (which is already the case in many sectors).

In recent decades the primary conflict between organizational designs has been between hierarchies and networks, an asymmetrical war. However, in the future the world is likely to experience a general shift downward into a new bilateral organizational conflict—networks fighting networks.

"Bureaucracy lies at the root of our military weakness," wrote advocates of military reform in the mid-eighties. "The bureaucratic model is inherently contradictory to the nature of war, and no military that is a bureaucracy can produce military excellence."[73]

While the change to a new unbureaucratic military is on the drawing board, the future network-centric military—an unsettling notion to say the least—is still a ways away. Nevertheless networks of control have invaded

---

72. Arquilla and Ronfeldt, *Networks and Netwars*, p. 15, emphasis removed from original. Contrast this line of thinking with that of Secretary of Defense Robert McNamara in the 1960s, whom Senator Gary Hart described as advocating "more *centralized* management in the Pentagon." See Gary Hart and William Lind, *America Can Win* (Bethesda, MD: Adler & Adler, 1986), p. 14. Or contrast it in the current milieu with the Powell Doctrine, named after four-star general and Secretary of State Colin Powell, which states that any American military action should have the following: clearly stated objectives, an exit strategy, the ability to use overwhelming force, and vital strategic interests at stake. This type of thinking is more in line with a modernist, Clausewitzian theory of military strategy: that force will be overcome by greater force, that conflict should be a goal-oriented act rather than one of continuance, that conflict is waged by state actors, and so on.

73. Hart and Lind, *America Can Win*, pp. 240, 249.

our life in other ways, in the form of the ubiquitous surveillance, biological informatization, and other techniques discussed in chapter 3.

The dilemma, then, is that while hierarchy and centralization are almost certainly politically tainted due to their historical association with fascism and other abuses, networks are both bad and good. Drug cartels, terror groups, black hat hacker crews, and other denizens of the underworld all take advantage of networked organizational designs because they offer effective mobility and disguise. But more and more one witnesses the advent of networked organizational design in corporate management techniques, manufacturing supply chains, advertisement campaigns, and other novelties of the ruling class, as well as all the familiar grassroots activist groups who have long used network structures to their advantage.

In a sense, networks have been vilified simply because the terrorists, pirates, and anarchists made them notorious, not because of any negative quality of the organizational diagram itself. In fact, positive libratory movements have been capitalizing on network design protocols for decades if not centuries. The section on the rhizome in *A Thousand Plateaus* is one of literature's most poignant adorations of the network diagram.

It has been the goal of this chapter to illuminate a few of these networked designs and how they manifest themselves as *tactical effects* within the media's various network-based struggles. As the section on viruses (or chapter 5 on hacking) showed, these struggles can be lost. Or as in the case of the end-to-end design strategy of the Internet's core protocols, or cyberfeminism, or the free software movement, they can be won (won in specific places at specific times).

These tactical effects are allegorical indices that point out the flaws in protocological and proprietary command and control. The goal is not to destroy technology in some neo-Luddite delusion, but to push it into a state of hypertrophy, further than it is meant to go. Then, in its injured, sore, and unguarded condition, technology may be sculpted anew into something better, something in closer agreement with the real wants and desires of its users. This is the goal of tactical media.