Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism

Stefan Helmreich
New York University

This article analyzes computer security rhetoric, particularly in the United States, arguing that dominant cultural understandings of immunology, sexuality, legality, citizenship, and capitalism powerfully shape the way computer viruses are construed and combated. Drawing on popular and technical handbooks, articles, and Web sites, as well as on e-mail interviews with security professionals, the author explores how discussions of computer viruses lean on analogies from immunology and in the process often encode popular anxieties about AIDS. Computer security rhetoric about compromised networks also uses language reminiscent of that used to describe the "bodies" of nation-states under military threat from without and within. Such language portrays viruses using images of foreignness, illegality, and otherness. The security response to viruses advocates the virtues of the flexible and adaptive response—a rhetoric that depends on evolutionary language but also on the ideological idiom of advanced capitalism.

As networked computing becomes increasingly essential to the operations of corporations, banks, government, the military, and academia, worries about computer security and about computer viruses are intensifying among the people who manage and use these networks. The end of the 1990s saw the emergence of a small industry dedicated to antivirus protection software, and one can now find on the World Wide Web a great deal of information about how viruses work, how they can be combated, and how computer users might keep up with ever-changing inventories and taxonomies of the latest viruses. According to various experts, some tens of thousands of viruses have come into existence since the first viruses were written and distributed in the late

AUTHOR'S NOTE: This article has benefited from comments by Marianne de Laet, Timothy Lenoir, Lisa Lynch, Emily Martin, Heather Paxson, and Renato Rosaldo. I thank the different editors of this journal who saw this project through: Olga Amsterdamska, Ellsworth Furhman, and Christopher McDermott. I am also grateful to the anonymous reviewers who helped this article materialize in the pages of this journal.

Science, Technology, & Human Values, Vol. 25 No. 4, Autumn 2000 472-491

1980s, and the number of new viral strains is growing exponentially (see Hruska 1998; Ducklin 1999; Symantec 1999). Professional and popular discussions of computer viruses capitalize on analogies to biological viruses and describe the need for individual or networked computer protection in language borrowed from immunology, and in terms that figure computer systems as self-contained bodies that must be protected from outside threat. These discussions often import from popular and medical discourse ideas and anxieties about sexual contamination in populations, and sometimes proffer "safe sex" tips for computer use. Computer security rhetoric about compromised networks also employs language reminiscent of that used to describe the "bodies" of nation-states under military threat from without and within. Such language describes viruses using images of foreignness, illegality, and otherness. In an age of emergent electronic commerce, viruses are also viewed as irrational threats to the integrity of the evolving virtual marketplace. Security professionals have begun to speak of computer systems as requiring defense protocols that embody the virtues of flexibility and adaptability—virtues connected to market ideals of advanced capitalist production and also to contemporary descriptions of the immune system (see Harvey 1989; Martin 1994).

In this article, I examine these discursive tendencies in computer security rhetoric, particularly as it has been elaborated in the United States from the late 1980s to the present. I draw on information about computer viruses from technical and popular handbooks, articles, and Web pages from this period as well as on interviews I conducted with five experts in the field of computer security in the mid-1990s. These people are all professors at U.S. universities and a couple engage in private consulting about digital security; none have previous histories as hackers.[1] The points of view communicated in the texts and interviews with which I work are dominant establishment views (as opposed to the views of virus writers—though they may share larger cultural frames, they may diverge on key beliefs about capitalism, community, etc.); the texts on which I rely are generated by and meant for an audience concerned with legitimate business, government, military, and academic activity.

Computer technology is a particularly interesting object for science studies because it exemplifies the ways that social and cultural practices and beliefs can be packed into artifacts that acquire associations with stability and objectivity (see Forsythe 1993). Many science studies scholars have demonstrated how computation itself materializes out of socially specific assumptions about logic, reason, and calculation (Collins 1990, 1998; Suchman and Trigg 1993; Star 1995; Turkle 1995). Anthropologists and cultural historians have examined how Cold War politics, masculinity, and ideals about democracy and individualism have been woven into the very construction of these machines

(Pfaffenberger 1988; Schaffer 1994; Edwards 1996; Adam 1998). I take such works as theoretical starting points.

As a cultural anthropologist, I am most keenly interested in how symbols and meanings from one social realm get transferred to another. Following Marilyn Strathern, I understand the term culture to consist in part "in the way people draw analogies between different domains in their worlds" (1992, 47; on metaphor, see Lakoff and Johnson 1980). I hope to show how culturally specific worries about contamination, foreignness, and the stability of markets have come to structure the way computer professionals think about and respond to threats to computer security. And I am interested in how this has happened through the importation of biological language into discourses about digital technology. Speaking in a biological register allows computer security rhetoric to lean on the authority of natural science, and also permits conceptions of bodies, nations, and economies to be articulated in the idiom of organic nature, an idiom that can often obscure the historical and cultural specificity of such conceptions (see Yanagisako and Delaney 1995). I mean in this article to offer an example of how a technical artifact emerges from a matrix of meanings from the culture in which it is produced; that is, how a technology is culturally as well as socially constructed. My arguments grow out of a larger anthropological project I undertook among the community of scientists working in Artificial Life, a brand of theoretical biology motivated by the notion that life is an abstract process that can be modeled, simulated, and even realized in a variety of media, most notably computers. For some researchers in this field, computer viruses can be seen as elementary forms of life, a point to which I will return at the end of this article.

Sex, Drugs, and Computer Viruses

A computer virus is a length of unwelcome computer code that can be attached to any legitimate software application. Security expert Eugene Spafford defines a virus as "a segment of machine code (typically 200-4000 bytes) that will copy itself (or a modified version of itself) into one or more larger 'host' programs when it is activated. When these infected programs are run, the viral code is executed and the virus spreads further" (1994, 250). The code that viruses contain can produce relatively harmless outcomes (like the periodic display of silly messages) or more serious ones (like slowing computer performance, damaging files, erasing hard disks, or crashing systems). Computer viruses, on the analogy to biological viruses, are understood to pirate the replicative material of their hosts and use it to make copies of themselves; computer code is thought of as akin to biogenetic code, and computer viruses are a kind of parasite on legitimate code (Sophos 1998). As one security expert I interviewed put the comparison between biological and computer viruses, “Both are comparatively simple self-replicating entities that require the presence of a host to replicate, and that sometimes damage their host by their actions. Both spread in various ways in populations, and both have some varieties that take various steps to make them difficult to recognize and eliminate.” Computer viruses are usually introduced into a network of computers through one computer, which might be the originary node of the virus, or a site where a disk previously infected through another personal computer is inserted.[2] Importantly, viruses can also be transmitted over the Internet—through downloads from the Web or in e-mails that have attached executable files. The biological metaphor is often extended beyond comparisons with the infection of an individual, placing viruses within the larger context of an evolving population. Spafford writes, “Computer viruses exhibit ‘species’ with well-defined ecological niches based on host machine type, and variations on the species. These species are adapted to specific environments and will not survive if placed in a different environment” (1994, 262).

Experts in computer security explicitly understand the protection of computers against viruses through metaphors of health and immunity. The mission statement of Symantec, a company that produces antivirus software, opens: “In our health-conscious society, viruses of any type are an enemy. . . . Just as proper diet, exercise and preventative health care can add years to your life, prudent and cost-effective anti-virus strategies can minimize your exposure to computer viruses” (Symantec 1999). And Peter J. Denning, speaking of viruses, writes in *Computers Under Attack: Intruders, Worms, and Viruses*, “Intrusions can be controlled by a combination of technical safeguards—a sort of network immune system—and hygienic procedures for using computers” (1990b, xiv). Noting that “Analogies with food and drug safety are helpful,” Denning catalogues some of these “hygienic procedures.” But the parallels to safe sex rhetoric in the age of AIDS are more evident and should be fairly clear:

> Never insert a diskette that has no manufacturer’s seal into your PC. Never use a program borrowed from someone who does not practice digital hygiene to your own standards. Beware of software obtained from public bulletin boards . . . don’t execute programs sent in electronic mail—even your friends may have inadvertently forwarded a virus. (1990c, 291)

During 1989 U.S. Congressional Hearings on the topic of computer virus legislation, California Representative Wally Herger made the link to HIV explicit, commenting that “Some have called [the computer virus] the AIDS of the computer world" (Committee on the Judiciary, House of Representatives 1990, 16). Andrew Ross (1991) has commented on the traffic between computer virus and HIV imagery and has noted how the industry of computer protection technology has elaborated on the immune system trope by making available "prophylactic software" (a term Denning uses) like Flu Shot +, Virusafe, Vaccinate, and Disk Defender.[3] The metaphorical link between computer viruses and sexually transmitted diseases in computer virus discourse goes back to the very first viral program written; it was set loose in a program called "vd" (Levy 1992, 313). One of the men I interviewed told me that "We tried to use the analogy of AIDS and its impact on sexual practices as an analogy to viruses and their impact on 'safe computing.' " Another researcher said that "The computer/network, in the mathematical theory, does have a 'body' that can be considered on some analogy to a biological system," and that "Epidemiological models of disease propagation in human populations happen to fit what we know of computer virus propagation fairly well—though the transmission mechanisms are physically very different." As professionals working in security, my informants argued that such mechanisms were well characterized, and that laypersons were just as uninformed and superstitious about them as they were about the mechanisms that transmitted real viruses. One said, "I had one friend say that the Internet Worm had mutated and was now infecting IBMs. This is baloney." According to the researchers with whom I corresponded, rumors about viruses mutating to adapt to new operating systems are common among many users, and echo some of the misconceptions that have surrounded ideas about HIV transmission and about HIV as infinitely adaptable (see also Rosenberger 1996). Viruses may be able to alter many different sorts of programs, but cannot cross over from, say, an IBM to a Macintosh, as many laypeople hold.[4]

The language of risk pervasive in medical AIDS discourse appears in these rhetorics, as do anxieties that the "at-risk" population is not careful enough in their practices. Spafford writes, "The population of users of PCs further adds to the problem, as many are unsophisticated and unaware of the potential problems involved with lax security and uncontrolled sharing of media" (1994, 251). In *The Whole Internet User's Guide and Catalog*, Ed Krol cautions the reader, "Believe that it is your workstation's responsibility to protect itself, and not the network's job to protect it" (1992, 38). This language puts responsibility for protection squarely on users, even as they are enjoined to follow the advice of experts—advice based on an image of users as incautious innocents or as individuals who willfully and irresponsibly jeopardize the integrity of the bounded body. Once individuals make a choice to link up to a network, they have to look out for themselves: "Even common 'public domain' or 'free' software can be risky. You have to decide how much risk you are willing to live with" (Krol 1992, 41). In this language, social intercourse, like sexual intercourse, puts the body at risk. Computers are understood as individuals with boundaries. Questions like "What If My Computer Is Violated?" (Krol 1992, 42) sexualize the intrusion of a computer, marking a vulnerable system as symbolically feminine, implying that a safe computer might be thought of as an impenetrable masculine body (see Crimp 1988 on how early medical AIDS discourse identified gay male bodies as always already "at-risk" because of their imagined "penetrability").

Much of the expert panic around viruses has been articulated in specifically biological language: "The problem with research on computer viruses is their threat. True viruses are inherently unethical and dangerous. . . . To experiment with computer viruses is akin to experimenting with smallpox or anthrax microbes—there may be scientific knowledge to be gained, but the potential for disastrous consequences looms large" (Spafford 1994, 263). Viruses are spreading in populations, reaching "epidemic numbers" (Spafford 1994, 249): "The spread of viruses through commercial software and public bulletin boards is another indication of their widespread replication. Although accurate numbers are difficult to derive, reports over the last few years indicate an approximately yearly doubling in the number of systems infected by computer viruses" (Spafford 1994, 262). "It is important to realize that often the chain of infection can be complex and convoluted. With the presence of networks, viruses can also spread from machine to machine as executable code containing viruses is shared between machines" (Spafford 1994, 256). These statements bespeak an anxiety about public space, about individuals threatened by others. The "public bulletin board"—the primary site where the infectious "uncontrolled sharing of media" took place in the mid-1990s (just before the rise of the Web)—is haunted by the image of public bathrooms, or perhaps even public bath houses, playing on popular anxieties about the transmission of AIDS in needle sharing or public sex. Computers are imagined as pristine, autonomous entities that exist prior to their embedding in networks—an idea that echoes the liberal conception of society as made up of individuals who exist prior to the society of which they are a part, an ideology deeply written into U.S. political culture. The Internet body politic is supposed to be made of rational actors, agents who enter responsibly into a kind of Rousseauian social contract.

Defending the Body

In the imaginary I have outlined, the body is an autonomous self to be protected. Connection to the net must be done carefully, for it holds the threat of plunging the user into a disorderly and dangerous universe of encounters with strangers that are almost sexual in their character. These figurations of connection, in which all connection is risk, lead to efforts to supply the computer with "the digital equivalent of an immune system" (Taubes 1994, 887) where the version of the immune system imagined is of the kind that protects the body as a fortress under siege (for a history of this image in immunology and popular culture, see Martin 1994). Keeping the self stable is the imperative here. In "Self-Nonself Discrimination in a Computer," computer scientist Stephanie Forrest and colleagues write that "The problem of protecting computer systems can be viewed generally as the problem of learning to distinguish self from other. We describe a method for change detection which is based on the generation of T cells in the immune system . . . the method might be applied to the problem of computer viruses" (Forrest et al. 1994, 202). The authors continue,

> The problem of ensuring the security of computer systems includes such activities as detecting unauthorized use of computer facilities, guaranteeing the integrity of data files, and preventing the spread of computer viruses. In this paper, we view these protection problems as instances of the more general problem of distinguishing self (legitimate users, corrupted data, etc.) from other (unauthorized users, viruses, etc.). We introduce a change-detection algorithm that is based on the way that natural immune systems distinguish self from other. . . . The algorithm we have just presented takes its inspiration from the generation of T cells in the immune system. The immune system is capable of recognizing virtually any foreign cell or molecule. To do this, it must distinguish the body's own cells and molecules which are created and circulated internally from those that are foreign. (Pp. 202, 210-11)

One scientist I interviewed summarized this view of the immune system: "An immune system might be described as a system specialized for detecting undesirable foreign replicators. Depending on the level at which the metaphor is applied, either a single computer or an entire network or internetwork might be regarded as the 'body.' "

There is an interesting tension here, for this person's words suggest that the boundaries of bodies are negotiated and not given. One expert I interviewed went further and suggested that the drawing of boundaries between computers in a network was a complete artifact of how such computers are used socially. Depending on their purposes, people might decide that a local area network is the unit to be protected from viruses or that it is simply one computer. Because of this multiplicity of possible boundaries, he also felt that the notion of a computer immune system was impractical: "You would basically be designing another operating system with this sort of built into it. I don't think you can run it on top of a system as an application." This dissenting opinion has done little to quell the proliferation of immune system metaphors, however. In June 1999, Symantec unveiled DIS, a "Digital Immune System." Less a piece of software than a link to the Symantec company, the DIS is basically a subscription to Symantec's antivirus services that automates the detection of infected programs in a subscriber's system and sends the culpable viral strains to Symantec for an electronic assessment and cure (see Yassin 1999). The picture of computer networks as immunological selves to be protected from what my informant called "undesirable foreign replicators" plugs us into the next level of metaphor at work here: that of the network as akin to the body of a nation-state, a nation-state under attack from without and within.

Defending the Body of a Nation-State

To underscore the ways in which networks are analogized to nation-states, I want to turn briefly to some imagery from the popular press that explicitly figures the Internet as akin to the early, expanding United States. In the mid-1990s, construals of the Internet as an information space (a term used in *Science* in August 1994) became fantastically popular in the United States, and attention focused on how the "electronic frontier" might be tamed and turned into a democratic space. Attention and anxieties centered on how the railroad tracks of the frontier would be turned into the clean lanes of the "information superhighway," where the values of individualism and free trade could thrive. Threats to the orderly development of a civil cybersociety loomed on a landscape populated with outlaws and hackers. *Scientific American* described it this way:

> Some say the Internet may become an information superhighway, but right now it is more like a 19th-century railroad that passes through the badlands of the Old West. As waves of new settlers flock to cyberspace in search of free information or commercial opportunity, they make easy marks for sharpers who play a keyboard as deftly as Billy the Kid ever drew a six-gun. Old hands on the electronic frontier lament both the rising crime rate and the waning of long established norms of open collaboration. (Wallich 1994, 90)

Other early writing capitalized on the frontier metaphor. In T*he Whole Internet Catalog and User's Guide*, Ed Krol wrote, "When the West was young, there was a set of laws for the United States, but they were applied differently west of the Mississippi river. Well, the network is on the frontier of technology, so frontier justice applies here too" (1992, 35). The ethics of using the Internet "are very close to the frontier ethics of the West, where individualism and preservation of lifestyle were paramount" (Krol 1992, 35). And journalist Mitchell Waldrop pronounced, "Like a quiet country village that's suddenly become a sprawling, brawling boom town, it's rapidly being transformed by an influx of new user groups and commercial interests" (1994, 879). As the "mining" of information (Waldrop's image) gets underway in earnest, "The ranchers are going to be coming in and putting up barbed wire" (quoted in Waldrop 1994, 879). Images of a pristine, wild, and anarchic nation predominate. These are images of a particularly American imagination, stalked by fears of encroachment on individual freedoms. This discourse exists alongside a sense that the frontier must be tamed, and that individuals must enter into reasonable contractual social relations (see Sardar 1996; Lockard 1997).

Who exactly threatens the harnessing of a cowboy ethic to liberal contractual individualism? Those who immaturely use the Internet for their own selfish or disruptive ends, those in the frontier who refuse to stop playing cowboy, or those who have interests in launching attacks against orderly colonization. Here I want to return to the images of this nation-state as a body, to places where the language of self-nonself discrimination takes on decidedly gendered and racialized echoes, places where viruses are described as undesirable others to a Euro-American nation.

Emily Martin (1992) argues that the mainstream media represents the immune system as an embattled nation-state structured by cross-cutting hierarchies of race, class, gender, and sexuality. Antibodies fight off invading viruses and infections, which are often figured in metaphor as racial or ethnic others to a dominant white identity. She suggests that some of the agents low in the immune system hierarchy (e.g., macrophages) are personified as feminized, racialized other to the dominant actors in the immune system (T cells, figured as strong white male heroes) and that they are pegged as potential traitors to the cause of the body as nation-state because of their "sympathy" to the viruses they are trying to combat (macrophages often "inadvertently shelter" HIV from higher level agents in the immune system).[5] Rhetoric about computer network immune systems and the threats to them similarly image the system as a beleaguered nation or community under threat from within and without—in this latter case, from what one of my informants called "undesirable foreign replicators." Employing language reminiscent of political categories used to describe populations of guest workers and immigrants in the United States and in Western European countries, Eugene Spafford notes that "the most successful viruses to date exploit a variety of techniques to remain resident in memory once their code has been executed and their host program has terminated" (1991, 737, italics added). And Denning expresses concern over "the health of [computer] systems and their protection against disruption by external agents" (1990b, vi). Viruses, low on the biological totem pole, are also often figured as dirty and are given names like "Festering Hate."[6] Such "undesirable foreign replicators" reproduce themselves wantonly, and fill valuable computer space with irrational code. They can be "predatory" and "territorial" (Spafford 1994, 262), and, like many racially marked undocumented workers in the United States, they are illegal. Viruses that have not yet been understood or contained are considered to be "in the wild." All of these notions are freighted with highly sexualized and racialized images of viruses as crafty, hyperfecund, and primitive. These irrational characteristics are culturally other to the political definition of U.S. citizenship as the realization of a rational, social, contractual self.

Because of the semantic superimposition of community and immune system effected in descriptions of computer networks, the hygienic practices that keep computer networks healthy are often close to those that are salutary to the body of the modern nation-state.[7] In early reflections on this topic, Donna Haraway discusses the metaphorical valences of computer immune systems to constructions of the nation-state. She writes,

> like the body's unwelcome invaders, the software viruses are discussed in terms of pathology as communications terrorism, requiring therapy in the form of strategic security measures. There is a kind of epidemiology of virus infections of artificial intelligence systems, and neither the large corporate or military systems nor the personal computers have good immune defenses. Both are extremely vulnerable to terrorism and rapid proliferation of the foreign code that multiplies silently and subverts their normal functions. (1991, 212, note 4)

Consider also the titles of some early books about computer viruses: Lance Hoffman's *Rogue Programs: Viruses, Worms, and Trojan Horses* (1990) and Alan Lundell's *Virus! The Secret World of Computer Invaders that Breed and Destroy* (1989). *Times* September 1988 article titled "Invasion of the Data Snatchers" (Elmer-DeWitt 1988) played on the same themes of xenophobia and bodily invasion that were the subject of the original 1950s movie *Invasion of the Body Snatchers*.

In security experts' discussions of viral threats to computer networks, they take for granted that it is in the interest of all of society to shield computer networks and the organizations they support from political and social threat. In *Computers Under Attack: Intruders, Worms, and Viruses* (1990b), Denning discusses what he calls "threats to our networks of computers" and to the "integrity and privacy of information entrusted to computers" but doesn't stop to ask in whose interests these networks work. Denning states that "the concern over these forms of intrusion—break-ins, worms, and viruses—arises from the possible dangers to stored information on which our work depends" (1990b, xiv). He never specifies to whom the "our" in this sentence refers, though his examples show that he has primarily government, military, and business audiences in mind, audiences whose purposes may not be universally shared.

It is crucial to note that computer viruses are of course not accidents; they are created by real people with real motives. As one of my informants argued, "The metaphor hides the fact that computer viruses are created by human beings for the explicit purpose of invading the programs of other human beings without their knowledge." And another added, "I'm sure there are as many [motives] as there are perpetrators—revenge by the disgruntled employee, prowess, scaring people, trying to get noticed, teaching the establishment a lesson, getting even with those who steal your software, etcetera." He continued, pointing out that the production of viruses is done by those who are not interested in participating in dominant definitions of social interaction on the Internet: "Computer viruses are intended to interfere with coordination of action. As such they are an antisocial creation of other human beings, and as such they are very much a part of human societies." These "antisocial" human beings have not been factored out of the discussion on computer viruses—far from it. Since the early 1990s, these people have been the focus of what Andrew Ross (1991) has called a "moral panic" about computer viruses. Predominantly young, white, male, and middle-class, these so-called "hackers" often occupy categories of privilege in the United States. But it has taken little ideological work (in the media and courtroom) to designate these people as a counter-cultural class dedicated to undermining national security and the sanctity of property rights. Like the viruses they write, they are considered immature, primitive, and annoying. One of my informants said, "I think most virus writers are in the same mental state as twelve- to seventeen-year-old males, 'proving' something to whomever in order to get attention, peer-group approval, or whatever." Another said, "The self-proclaimed virus authors that we know of naturally claim pure and lofty motives, but they can largely be dismissed as immature publicity seekers." One book on security announces, "There's rather a race between the brave and gallant people who analyze the viruses and write clever programs to detect and eliminate the known viruses, and the foul-smelling scum who devise new types of viruses that will escape detection by all the current virus checkers" (Kaufman, Perlman, and Speciner 1995, 23). Media coverage of the "Melissa" virus, released in 1999 and written by a thirty-year-old white male programmer named David Smith (an employee for an AT&T subcontractor), emphasized the possibility that the virus was named after Smith's favorite topless dancer, a rhetorical flourish that highlighted the programmer's immaturity. This focus on the trivial aspects of the motivations of virus writers detours attention away from the possibility that viruses may be written by people who have more complex political motives. Infantilizing them dismisses any real grievances they may have (see Taylor 1999). And some have indeed had complex political or economic complaints. As one Web page for an antivirus research center noted,

> The NCSA [the National Computer Security Association for the United States] found that Bulgaria, home of the notorious Dark Avenger, originated 76 viruses . . . [in 1987], making it the world's single largest virus contributor. Analysts attribute Bulgaria's prolific virus output to an abundance of trained but unemployed programmers; with nothing to do, these people tried their hands at virus production, with unfortunately successful results. (Symantec 1999)

The origins of viruses may not necessarily be sited in pathological persons, then, but in the relationships that obtain between political economic systems and those who wish to critique or disrupt the concretization of such systems in computer networks.

In the United States, the entrance into the hacking world of nonwhite, working-class people in the early 1990s was met with descriptions that ignored any political critique that might be implicit in their actions, centering attention rather on their racially marked "attitude." In 1992, *The New York Times* ran a story about the emergence of a new nonwhite, nonsuburban class of hackers. Titled "Computer Savvy, with an Attitude," this article described rival groups of Latino and black hackers who had infiltrated the networks of Southwestern Bell and TRW as engaged in "a cybernetic version of 'West Side Story' " (Tabor and Ramirez 1992, B1), an image that equated the practices of these hacker cliques to those of frustrated teenagers of color seeking an outlet in violent gang activity. The book that was eventually written about one of these groups made the link explicit in its title: *Masters of Deception: The Gang that Ruled Cyberspace* (Slatalla and Quittner 1996). One section of an early *Scientific American* article about computer security was entitled "The Cyber-Neighborhood Goes Downhill," a phrase with decidedly racial resonances. In worried tones, the author wrote that "anyone who can scrounge up a computer, a modem and $20 a month in connection fees can have a direct link to the Internet and be subject to break-ins—or launch attacks on others" (Wallich 1994, 90).

This entrance into the information superhighway of people who refuse to plug their actions into the rules of rational democracy has pressed computer security experts to speak in the language of law. A discourse of "legitimacy" has emerged to discuss how "illegal" viruses might be detected. One method that has been proposed for protecting the integrity of computer networks and for ensuring that they are only used by law-abiding citizenry is to instantiate a set of legalistic programming strictures that can smoke out the offending viruses. “Authentication practices” are “processes by which we assure ourselves that an agent is one previously identified as trustworthy. . . . They include recognition of familiar faces, voices, or signatures, login protocols on computers, and cryptographic protocols” (Denning 1990c, 5). Viruses can be screened and will be known by their inability to provide the legal signals of their authenticity.[8] The newest software brings legal imagery together with biological imagery. An antiviral technique called signature-based analysis examines viral signatures, which are “the fingerprints of computer viruses—distinct strands of code that are unique to a single virus, much as DNA strands would be unique to a biological virus” (Symantec 1999).

Because computer viruses are written by real agents, they can stand not only as symbolic threats to the health of the nation’s body but also as more literal ones. In November 1988, a person at Cornell University launched a viral attack on the Internet, reaching parts of the Department of Defense’s ARPAnet. And in 1987, a virus was found in the Hebrew University library network in Jerusalem. It was set to erase all files and paralyze the University on May 13, 1988, the 40th anniversary of the last day Palestine was recognized as a political entity. The potential for political uses of computer viruses is quite real. Denning warns that “we can expect steady increases in acts of crime, espionage, vandalism, and even political terrorism by computer in the years ahead” (1990b, iii). (The fact that viruses can be set like time bombs—as in the Hebrew University example—strengthens metaphorical constructions of viruses as information terrorism.) “Several new viruses are appearing every day. Some of these are undoubtedly being written out of curiosity and without thought for the potential damage. Others are being written with great purpose, and with particular goals in mind—both political and criminal” (Spafford 1994, 259). The U.S. government sees the threat to national security: “As an indication of the severity of the problem, the federal government has helped form a SWAT team called the Computer Emergency Response Team [CERT]” (Symantec 1999). The national imagery superimposed onto descriptions of computer networks has a more concrete realization in actual projects to protect national information infrastructures. In the late 1990s, the National InfraGard Program—a computer security consortium of U.S. businesses, academia, and government agencies—was formed in response to an FBI directive “to gain the assistance of local computer security professionals in determining how to better protect critical information in the public and private sectors” (Internet Security Systems 1999). This “nationalization” of computer security concerns builds on CERT, which has articulated its mission in national terms, arguing for “the importance of information to national security”:

> Historically, military networks and computers were unreachable by nonmilitary participants. The Internet, however, provides a cost-effective way for military and government units to communicate and participate in achieving objectives. Use of the Internet means that individuals, multinational companies, and terrorist organizations all can gain access to important information resources of governments and military forces. Thus, it is important to address Internet security concerns as a key component of defensive information warfare. Because the Internet is global, it can be an avenue of attack for offensive information warfare by many governments. One of the battlefields for a future military offensive could very well involve the Internet. Intruder technology . . . could be used by a government as a weapon against information resources, or used randomly by a terrorist organization against civilian targets. (CERT 1999)

Viruses could be a key "intruder technology"; their biological description is already militarized: "As well as self-replicating code, a virus normally contains a 'payload.' The former is like the propulsion unit of a missile; the latter is like the warhead it delivers" (Sophos 1998). Certainly it would not be surprising if national military agencies started using viruses as military tools. One of the people I interviewed told me that "the U.S. government has let contracts for research into the use of viruses as weapons in military situations." And he said that viruses might be used in commercial competition too: "It has been suggested that software manufacturers could benefit from targeting viruses at competitors' products, or enforcing time limits/payment dates and such."

The complex meanings and practices that shape the U.S. race, gender, and class-stratified nation-state have in some measure been encrypted into discourse about how immune systems might protect computer networks. The computer virus that threatens those networks is imagined either as a foreign agent who has infiltrated the body of the state, or as a marginalized member of the nation itself who poses an internal threat and may be politically aligned with foreign agents, coded as "terrorists." It is no wonder, given the strong metaphorical association of networks with nation-states, that the FBI has stepped in. These metaphors may also increasingly structure the actual threats to which networks are subject; resistance to national and market forces may indeed begin to speak in the language assigned it by the dominant discourse.

Flexibility, Computer Immunology, and Advanced Capitalism

In "The End of the Body?" (1992) and *Flexible Bodies* (1994), Emily Martin discusses how images of the human immune system are transforming under the political economic changes associated with advanced capitalism. She contends that the immune system is becoming a mirror for an economic system characterized by the geographically and temporally flexible and specific responses of decentralized capital to global fluctuations in interest and exchange rates, labor laws, and markets (see Harvey 1989). Martin claims that the logic of advanced capitalist flexible specialization is taking up residence in our very bodies and that our health and fitness as laborers will be increasingly measured in terms of our ability to psychologically and—most importantly for her argument—biologically adjust to rapid change. She argues that prevailing structures of domination organized around race, class, gender, and sexuality will be reinscribed in new and more insidious ways, with people who diverge from the normative identity of the male, white, middle-class healthy person designated as having inflexible and insufficiently specific immune systems. Images of the body as an agile, adaptive entity are being crafted in concert with a new economic order characterized by perpetual innovation and flexible specialization.

Recent suggestions about how best to protect computers against viruses have capitalized on analogies to evolution, and these analogies have highlighted the notion of adaptability. The idea is to make operating systems more diverse and flexible so as to continually "outsmart" or "outevolve" new viruses. Computer scientist Danny Hillis once noted that

> so long as formats like UNIX [a network operating system] become a universal standard, we'll have awful problems with viruses no matter how many vaccines and quarantines we come up with. What we want in networked computing is a diversity of operating standards. We want each computer to be a slight variant of the standard, maybe one that is slowly evolving. (Kelly 1991, 18-19)

The diversity Hillis speaks of in computer operating systems is already coming about as the software companies that manufacture these systems engage in niche marketing and attempt to bring open-source operating systems like Linux into engagement with market dynamics. The solution to the problem of giving computer operating systems immunity to viruses, solved initially in terms of the biological metaphor, is played out on the field of flexibly specific capitalist production, from where it can double back to confirm the validity of the biological metaphor. But Hillis and others are not the only ones enthusiastic about evolutionary metaphors. The notion of adaptability has been taken to heart by people who have been writing defenses against what are called "polymorphous viruses." According to Symantec, an antivirus research center, "Like the human AIDS virus that mutates frequently to escape detection by the body's defenses, the polymorphic computer virus likewise mutates to escape detection by anti-virus software that compares it to an inventory of known viruses" (Symantec 1999). What is needed, according to companies like Internet Security Systems (1999), is "Adaptive Security Management."

Emily Martin (1994) claims that two visions of the immune system exist—one as a flexible and responsive system modeled on late capitalist economic formations, and one as a bounded and defensive unit modeled on the militaristic nation-state—and at first glance they appear logically contradictory. The flexibility of global capital and the rigidity of a stiffly hierarchical militaristic state seem to Martin initially incompatible. But as David Harvey (1989) has pointed out, and as Martin recognizes, flexible strategies of capital investment and production rely on the existence of strict differences between and within nations. Crossing borders to take advantage of differences in labor laws and exchange and interest rate fluctuations requires that nations have somewhat stable boundaries, and that these be stabilized by traditional nationalist rhetoric.

A prescient passage from Denning about the integrity of computer systems in the age of flexible specialization reveals how both flexibility and stability must be maintained at the same time: "As electronic networking spreads around the globe, making possible new international interactions and breaking barriers of language and time, so rise the risks of damage to valuable information and the anxiety of attacks by intruders, worms, and viruses" (1990b, iii). By "electronic networking," Denning refers to the practices that make possible the international flow of flexible capital and by "risks of damage to valuable information," he is invoking the model of the computer as an immune system nation-state needing militaristic protection of its integrity. We can understand why the FBI and multinational corporations have begun to work together here; the state is invested in keeping national economic markets in place, as are companies that leap from context to context to exploit differences between labor and financial markets (see Harvey 1989; Maurer 1995).

The Cultural Inflections of Computational Infection

Models of computer networks as immune systems threatened by "computer viruses" make sense only when biological organisms and computers are both envisioned as "coded texts" pasted together with the glue of information. Such links promise to be tightened as computer viruses begin to be theorized as entities interesting to biology proper. In the field of Artificial Life, scientists look to computer viruses as elementary life forms in a new silicon kingdom of living things. As Ada Rogers put it in a popular article in *Newsweek*, "In the most radical view, viruses are an artificial life form. They live, breed, evolve, procreate, and die" (1995, 65). In his article on computer viruses, Eugene Spafford (1991) lists a number of ways that viruses might count as alive, specifying, among other things, their capacities to "self-reproduce," to store informatic self-representations (which is what he takes DNA in carbon life to do), and to enter into functional interactions with an environment. Though Spafford ultimately maintains that admitting computer viruses into the realm of the living would require an unacceptable redefinition of life, a redefinition he thinks would cheapen organically embodied organismic (including human) life, he follows in this list a canonical set of criteria used by Artificial Life researchers (see Farmer and Belin 1992), a list that I have argued elsewhere is already crafted (because of its informatic definition of life) to include computer programs on the threshold of life. Viruses, of course, fascinate not only because they are thought of as a liminal form of life but also because they are associated with death and disorder, the cessation of life activity (see Ansell Pearson 1997).

Computers are increasingly webbed together. And computer viruses are traversing that Web in ever greater numbers, with, according to experts, increasing costs to the organizations whose networks they damage.[9] As a new space of technologically mediated interaction and communication emerges, we see people spinning old and new metaphors together to talk about threats to their newly found work and play spaces. As argued in this article, these metaphors often encode ideas drawn from multiple contexts in the larger U.S. political culture, a culture driven by inequalities of gender, sexuality, race, and class, categories that have long been naturalized and biologized. Rhetorics around computer viruses often reinscribe such biologization by providing a new medium—a medium of information—in which to retell such tales about human bodies, sex, nation-states, and the helical binaries of self and other.

Notes

[1] I interviewed these people over the Internet, soliciting their answers to a standardized questionnaire. All have chosen to remain anonymous.

[2] Because a virus is just code, it can be transmitted via any sort of software.

[3] Note, however, that the imagery here is of vaccines, imagery that does not presently have resonances with existing strategies for fighting AIDS.

[4] Indeed, a genre of Web pages dealing with "computer virus hoaxes" has recently emerged. According to these pages, rumors of viruses, usually disseminated in chain-letter e-mail, can be as bad as viruses themselves, clogging network traffic and diverting processing power (e.g., see http://www.hoaxkill.com).

5. Martin also argues that these images get used to construe working-class bodies as unfit and self-destructive with inept immune systems, and homosexual male bodies with HIV as emasculated because of a low count of the masculinely personified (in textbook and lab language) T4 cells (1992, 131).

6. Viruses are in fact named capriciously, at the whim of the writer or discoverer, but phrases like this show up again and again. Others I've found are "Dark Avenger," "Vampiro," and "Genocide." People who write viruses often favor names that suggest threat, and in so doing, themselves deploy dominant rhetorical strategies for talking and thinking about viruses.

7. The body of the nation-state under siege is often gendered female. In computer virus discourse, this is often evoked with warnings that computer networks must be protected against the "penetration" of viral code (see Levy 1992, 314). We could read this another way, of course, as a homophobic image in which the heterosexual masculinity of the nation-state must be protected.

8. I'm reminded of cultural critic Paul Gilroy's discussion of law, authenticity, and identity in Britain in *'There Ain't No Black in the Union Jack'* (1987), in which he demonstrates how ideologies of legality become interlocked with and create racial categories in such a way as to designate incumbents of those categories as racially and ethnically "other" to hegemonic groups.

9. Symantec (1999) reports that "computer viruses have cost companies worldwide nearly two billion dollars since 1990, with those costs accelerating, according to an analysis of survey data from IBM's High Integrity Computing Laboratory and Dataquest."

References

Adam, Alison. 1998. *Artificial knowing: Gender and the thinking machine*. London: Routledge.

Ansell Pearson, Keith. 1997. *Viroid life: Perspectives on Nietzsche and the transhuman condition*. London: Routledge.

Collins, Harry. 1990. *Artificial experts: Social knowledge and intelligent machines*. Cambridge, MA: MIT Press.

———. 1998. Socialness and the undersocialized conception of society. *Science, Technology, & Human Values 23* (4): 494-516.

Committee on the Judiciary, House of Representatives. 1990. Computer virus legislation. Hearing before the Subcommittee on Criminal Justice of the Committee on the Judiciary, House of Representatives, 101st Congress, first session on H.R. 55 and H.R. 287, Computer Virus Eradication Act of 1989. Washington, DC: U.S. Government Printing Office.

Computer Emergency Response Team. 1999. Security of the Internet. Available: http://www.cert.org/encyc_article/tocencyc.html

Crimp, Douglas, ed. 1988. *AIDS: Cultural analysis/cultural activism*. Cambridge, MA: MIT Press.

Denning, Peter J. 1990a. Computer viruses. In *Computers under attack: Intruders, worms, and viruses*, edited by Peter J. Denning, 285-92. Reading, MA: ACM Press (Addison-Wesley).

———. 1990b. Preface and introduction. In *Computers under attack: Intruders, worms, and viruses*, edited by Peter J. Denning, iii-xv. Reading, MA: ACM Press (Addison-Wesley).

———. 1990c. Worldnet. In *Computers under attack: Intruders, worms, and viruses*, edited by Peter J. Denning, 3-10. Reading, MA: ACM Press (Addison-Wesley).

Ducklin, Paul. 1999. The ABCs of computer security. April. Available: http://www.sophos.com/virusinfo/articles/abc_en.html

Edwards, Paul. 1996. *The closed world: Computers and the politics discourse in cold war America*. Cambridge, MA: MIT Press.

Elmer-DeWitt, Philip. 1988. Invasion of the data snatchers. *Time*, 26 September, 62-67.

Farmer, Doyne, and Alletta d'A. Belin. 1992. Artificial life: The coming evolution. In *Artificial life II*, edited by Christopher G. Langton, Charles Taylor, J. Doyne Farmer, and Steen Rasmussen, 815-40. Redwood City, CA: Addison-Wesley.

Forrest, Stephanie, Alan S. Perelson, Lawrence Allen, and Rajesh Cherukuri. 1994. Self-nonself discrimination in a computer. In *Proceedings of 1994 IEEE computer society symposium on research in security and privacy*, 202-12. Los Alamitos, CA: IEEE Computer Society Press.

Forsythe, Diana. 1993. Engineering knowledge: The construction of knowledge in artificial intelligence. *Social Studies of Science 23*:445-77.

Gilroy, Paul. 1987. *'There ain't no black in the Union Jack.'* Chicago: University of Chicago Press.

Haraway, Donna. 1991. The biopolitics of postmodern bodies: Constitutions of self in immune system discourse. In *Simians, cyborgs, and women: The reinvention of natur*e, 203-30. New York: Routledge.

Harvey, David. 1989. *The condition of postmodernity: An enquiry into the origins of cultural change*. Cambridge, MA: Blackwell.

Hoffman, Lance J., ed. 1990. *Rogue programs: Viruses, worms, and Trojan horses*. New York: Van Nostrand Reinhold.

Hruska, Jan. 1998. The future of computer viruses. October. Available: http://www.sophos.com/virusinfo/whitepapers/futurevi.html

Internet Security Systems. 1999. Company press release: ISS pledges support for the FBI and National Infrastructure Protection Center's InfraGard program. June 1. Available: http://biz.yahoo.com/bw/990601/ga_interne_1.html

Kaufman, Charlie, Radia Perlman, and Mike Speciner. 1995. *Network security: Private communication in a public world*. Upper Saddle River, NJ: Prentice Hall.

Kelly, Kevin. 1991. Designing perpetual novelty: Selected notes from the second artificial life conference. In *Doing science*, edited by John Brockman, 1-44. New York: Prentice Hall.

Krol, Ed. 1992. *The whole Internet user's guide and catalog*. Sebastopol, CA: O'Reilly and Associates.

Lakoff, George, and Mark Johnson. 1980. *Metaphors we live by.* Chicago: University of Chicago Press.

Levy, Steven. 1992. *Artificial life: The quest for a new creation*. New York: Pantheon.

Lockard, Joseph. 1997. Progressive politics, electronic individualism and the myth of the virtual community. In *Internet culture*, edited by David Porter, 219-31. New York: Routledge.

Lundell, Alan. 1989. *Virus! The secret world of computer invaders that breed and destroy.* Chicago: Contemporary Books.

Martin, Emily. 1992. The end of the body? *American Ethnologist* 19 (1): 121-40.

———. 1994. *Flexible bodies: Tracking immunity in American culture from the days of polio to the age of AIDS*. Boston: Beacon Press.

Maurer, Bill. 1995. Complex subjects: Offshore finance, complexity theory, and the dispersion of the modern. *Socialist Review 25* (3, 4): 113-45.

Pfaffenberger, Bryan. 1988. The social meaning of the personal computer: Or, why the personal computer revolution was no revolution. *Anthropological Quarterly* 61 (1): 39-47.

Rogers, Ada. 1995. Is there a case for viruses? *Newsweek*, 27 February, 65.

Rosenberger, Rob. 1996. Computer viruses and "False Authority Syndrome." Available: http://ourworld.compuserve.com/homepages/virus_myths

Ross, Andrew. 1991. Hacking away at the counterculture. In *Technocultur*e, edited by Constance Penley and Andrew Ross, 107-34. Minneapolis: University of Minnesota Press.

Sardar, Ziauddin. 1996 alt.civilizations.faq: Cyberspace as the darker side of the west. In *Cyberfutures: Culture and politics on the information superhighway*, edited by Ziauddin Sardar and Jerome R. Ravetz, 14-41. New York: New York University Press.

Schaffer, Simon. 1994. Babbage's intelligence: Calculating engines and the factory system. *Critical Inquiry* 21 (1): 203-27.

Slatalla, Michele, and Joshua Quittner. 1996. *Masters of deception: The gang that ruled cyberspace*. New York: Harperperennial Library.

Sophos. 1998. Introduction to computer viruses. May. Available: http://www.sophos.com/virusinfo/articles/virusesintro.html

Spafford, Eugene. 1991. Computer viruses—a form of artificial life? In *Artificial life II*, edited by Christopher Langton, Charles Taylor, Doyne Farmer, and Steen Rasmussen, 727-45. Redwood City, CA: Addison-Wesley.

———. 1994. Computer viruses as artificial life. *Artificial Life 1* (3): 249-66.

Star, Susan Leigh, ed. 1995. *The cultures of computing.* Oxford, UK: Basil Blackwell.

Strathern, Marilyn. 1992. *Reproducing the future: Anthropology, kinship, and the new reproductive technologies*. New York: Routledge.

Suchman, L. A., and R. H. Trigg. 1993. Artificial intelligence as craftwork. In *Understanding practice: Perspectives on activity and context*, edited by S. Chaiklin and J. Lave, 144-78. Cambridge, UK: Cambridge University Press.

Symantec. 1999. Computer viruses: An executive brief. Available: http://www.symantec.com

Tabor, Mary B. W., and Anthony Ramirez. 1992. Computer savvy, with an attitude. *The New York Times*, 23 July, B1, B7.

Taubes, Gary. 1994. Devising software immune systems for computers. *Science* 265:887.

Taylor, Paul A. 1999. *Hackers: Crime in the digital sublime*. London: Routledge.

Turkle, Sherry. 1995. *Life on the screen: Identity in the age of the Internet.* New York: Simon & Schuster.

Waldrop, M. Mitchell. 1994. Culture shock on the networks. *Science* 265:879-81.

Wallich, Paul. 1994. Wire pirates. *Scientific American 270* (3): 90-101.

Yanagisako, Sylvia, and Carol Delaney. 1995. Naturalizing power. In *Naturalizing power: Essays in feminist cultural analysis*, edited by Sylvia Yanagisako and Carol Delaney, 1-22. New York: Routledge.

Yassin, Rutrell. 1999. Viruses get quarantined. May 13. Available: http://www.techweb.com/wire/story/TWB19990513S0013

Stefan Helmreich is Assistant Professor of Science and Society at New York University. He was trained in cultural anthropology at Stanford University, from which he received his Ph.D. in 1995. He is the author of Silicon Second Nature: Culturing Artificial Life in a Digital World *(updated edition with a new preface, California 2000), an ethnography of the Artificial Life community centered at the Santa Fe Institute for the Sciences of Complexity.*