Networks, Control, and Life-Forms

Alexander Galloway
Dept. of Culture & Communication
New York University
New York, NY 10003
212-998-5423
galloway@nyu.edu

Eugene Thacker
Literature, Culture & Communication
Georgia Institute of Technology
Atlanta, GA 30332-0165
404-385-2766
eugene.thacker@lcc.gatech.edu

ABSTRACT
In this paper we explore the technological, philosophical and political aspects of networks through a series of condensed, interrelated analyses.

Categories and Subject Descriptors
K.4.1 Public Policy Issues

General Terms
Human Factors

Keywords
Networks, politics, Internet, computers and society, netwars, multitude, cyberculture.

INTRODUCTION
Networks have the property of being everywhere in general, and yet nowhere in particular. For instance, in a very literal sense, it is hard to point to the Internet, or to global financial networks, or to one's own social network – but these networks nevertheless exist, and they are 'there.' This property of being both ubiquitous and absent does not mean that there is any kind of mystical or vital core to networks; it is, rather, reminder of how networks exist topologically. Indeed, with the ongoing expansion of wireless and mobile technologies, networks are increasingly becoming the very air we breathe. In such cases, it becomes difficult to decisively separate networks as a technology from other types of networks (social, economic, biological).

In recent decades the primary conflict between organizational designs has been between hierarchies and networks, an asymmetrical war. However, in the future we are likely to experience a general shift downward into a new bilateral organizational conflict--*networks fighting networks*.[1] We suggest that networks must increasingly be understood as simultaneously technical and political topologies. There are as many lessons to be learned from the failures of networks, as there are from their successes. In a sense, a network fails only when it works too well, when it provides too little room for change within its grand robustness, as the computer virus example illustrates. *In this way, networks only fail when they succeed.*

EPIDEMIC AND ENDEMIC
One of the results of the American-led war on terror has been the increasing implosion of the differences between emerging infectious diseases and bioterrorism. Not so long ago, a distinction was made between emerging infectious disease and bioterrorism based on their cause: one was naturally-occurring and the other the result of direct human intervention. International organizations such as the WHO and UN still maintain this distinction, though only vaguely. The U.S. government, in the meantime, has long since dispensed with such niceties, and as a result has radically streamlined the connections between the military, medicine, and the economics of drug development. A White House press release outlining the President's 2003 proposed budget discusses how, "in his 2003 Budget, the President has proposed $1.6 billion to assist State and local health care systems in improving their ability to manage both contagious and non- contagious biological attacks…" Similarly, a 2003 press release describes Project BioShield as a "comprehensive effort to develop and make available modern, effective drugs and vaccines to protect against attack by biological and chemical weapons or other dangerous pathogens." The implication of the word "or"—biological weapons or other pathogens—signals a new, inclusive stage in modern biopolitics. Regardless of the specific context, be it disease or terrorist, the aim is to develop a complete military-medical system for "alert and response" to biological threats. Context and cause are less important than the common denominator of biological effect. It matters little whether the context is terrorism, unsafe foods, compromised Federal regulation of new drugs, or new virus strains transported by air travel.

What matters is that what is at stake, what is always at stake, is the integrity of "life itself." One of the ways that sovereignty maintains its political power is continually to identify a biological threat. Giorgio Agamben points to the "state of exception" created around what he calls "bare life." Bare life, life itself, the health of the population, the health of the nation – these are the terms of

[1] John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica: RAND, 2001), p. 15.

modern biopolitics. By grounding political sovereignty in biology, threats against the biological body politic, in the form of threats against the health of the population, can be leveraged as ammunition for building a stronger sovereign power. This U.S. program of military, medical, and pharmaceutical governance ushers in a politics of biological security. Biological security has as its aim the protection of the population, defined as a biological (and genetic) entity, from any possible biological threat, be it conventional war or death itself. What this also means is that the biological threat--the inverse of biological security--is a permanent threat, even an existential threat. It is a biological angst over "death itself" (the biopolitical inverse of "life itself"). This requires a paradigm in which "the population" can be regarded as simultaneously biological and political. As Foucault notes, "at the end of the eighteenth century, it was not epidemics that were the issue, but something else – what might broadly be called endemics, or in other words, the form, nature, extension, duration, and intensity of the illnesses prevalent in a population…Death was now something permanent, something that slips into life, perpetually gnaws at it, diminishes it and weakens it."[2] It is clear that, in this context, there is no end to biological security, its job is never finished, and by definition, can never be finished. If there is one site in which the state of emergency becomes the norm, it is this site of non-distinction between war and disease, terrorism and endemic.

GOOD VIRUSES (SimSARS I)

In August 2003 the computer worms Blaster and Sobig-F started infesting the Internet. Blaster reportedly infected over 400,000 machines, while the Sobig.F worm was infecting an average of 1 in 17 emails at its height. As network-based worms, they operate almost undetected. Sobig-F exploited weaknesses in Microsoft's email program to replicate and distribute more copies of itself via email, while Blaster exploited a weakness in Window's Remote Procedure Call (RPC) interface. One response was to develop an automated "vaccine" which would, like the worms themselves, circulate autonomously through the networks, detecting flaws and vulnerabilities, and automatically fix them. The anti-Blaster "vaccine virus" was dubbed Welchia (alternate names include Nachi). The idea of an automated "good virus" is not necessarily a comforting thought. With over 77,000 viruses catalogued to date, and with approximately 200 active at any given moment, there is a secret war being waged behind the tranquility of the screen. As the network paradigm gains momentum--in biology, in communications, in international politics--we may be seeing a set of new, network-based strategies being developed on all levels. In some instances this will be a welcome change.

For instance, it could offer a more complex understandings of the biological workings of disease, as with the SARS outbreak earlier that year. During the 2003 epidemic, SARS did not simply infect biological networks, it also infected transportation networks, communications networks, and cultural networks. It also infected the discourse around the war on terrorism. Though it was a "naturally-occurring" outbreak, it was hard to completely separate the anxieties over SARS from bioterrorism, following as it did the 2001 Anthrax attacks in the U.S. In fact the pairing of emerging infectious disease and bioterrorism is something that is programmatically supported by the U.S. government. Project Bioshield aims to support the development of next-generation drugs, which includes both drugs for diseases such as cancer or AIDS, as well as experimental vaccines for "first responders." On December 1, 2003 – World AIDS Day – officials from the U.S. Department of Health and Human Services likened their efforts to the military agenda in Iraq. Just as troops in Iraq were "saving people from tyranny," so were U.S. health agencies "saving people from disease." The disease-as-war metaphor is not new, but takes on a new guise in the era of networks. If, as we are told, we are fighting "a new kind of war" based on networks, then are we also fighting a new kind of medical, biopolitical war?

Now consider the "good virus" model applied to SARS-like events: An epidemic is identified, and due to its networked nature, it is decided that it must be controlled via network means. An engineered microbe containing a vaccine to the epidemic agent is then released (via aerosol drones) into infected "hot zones" and the microbial network war allowed to run its course. Paradoxically, the good virus can only be successful in administering the vaccine if its rate of infection surpasses the bad virus. This nexus of disease, medicine delivery, and military logistics is what we can expect in future evolutions of warfare.

MEDICAL SURVEILLANCE (SimSARS II)

The aphoristic quality of the 2003 SARS epidemic serves to remind us of the intensive nature of networks. Consider current developments in the practice of medical surveillance. The World Health Organization (WHO), working with the Centers for Disease Control and Prevention (CDC), was able to establish a communications and data transmission network which greatly facilitated their decisions on travel advisories, quarantines, and the confirmation of SARS cases based on patient data. An information network was used to combat a biological network. The WHO's "Global Outbreak Alert and Response Network" has as one of its primary aims, the insurance that "outbreaks of potential international importance are rapidly verified and information is quickly shared within the Network." In addition, the CDC has had a number of network-based programs underway which address this network-response challenge. (The Enhanced Surveillance Project and the National Electronic Disease

[2] Michel Foucault, *Society Must be Defended,* (New York: Picador, 2003), pp. 243-244.

Surveillance System are two examples.) These efforts aim to utilize information networks as key communication tools in times of crisis—be they artificial or natural—and to that extent are meeting the same challenge given to the original designers of the Internet itself. For pioneering network engineers like Paul Baran the crisis was the cold war nuclear threat. For the CDC it is current biological threats, or rather, the threat of biology.

The mere existence of medical surveillance is not problematic in itself. Certainly, were it not for the WHO's efforts, the SARS epidemic may have been worse. The key issue lies in the relationship between disease, code, and war. Military battles are becoming increasingly virtual, with a panoply of computer-based and information-driven weaponry. And the idea of disease-as-war has a long history. However, it is foreseeable that the issue of what constitutes "health data" may become a point of some controversy. Concerns over public health will be the Trojan horse for a new era of increased medical surveillance and with it a new militarization of medicine. The institutions of medical surveillance will be almost indistinguishable from national security initiatives and will have shared goals and techniques. While the WHO utilized medical data from patients infected with SARS around the world, it is foreseeable that health data may soon be required in advance from both infected and non-infected organisms. We are already witnessing this in the areas of genetic screening, genetic counseling, and DNA fingerprinting. Imagine a video game simulation like the popular SimCity in which the player develops, builds, and manages a city. But imagine that, instead of managing a whole city, the goal is to manage the medical health of the city's inhabitants; instead of being the "mayor" of SimCity, the player is an official CDC "virus hunter." The goal of the game is to watch for potential disease outbreaks, and also manage the health of the population on a regular basis (including hospital funding, emergency services, research centers). This would help illustrate the future of the network model of public health, itself already fully digitized, online, and multiplayer.

In the informatic mode, disease, like disorder, is always virtual. It creates a virtual state of permanent emergency wherein infection is always kept just out of reach. But the state of permanent emergency can only be propped up by means of better and better medical surveillance systems.

RHETORICS OF FREEDOM

While tactically valuable in the fight against proprietary software, open source is ultimately flawed as a political program. Open source focuses on code in isolation. It fetishizes all the wrong things: language, originality, source, the past, status. To focus on inert, isolated code is to ignore code in its context, in its social relation, in its real experience, or actual dynamic relations with other code and other machines. Debugging never happens though reading the source code, only through running the program. Better than open source would be open runtime which would prize all the opposites: open articulation, open iterability, open practice, open becoming.

But this is also misleading and based in a rhetoric around the relative openness and closedness of a technological system. The rhetoric goes something like this: technological systems can either be closed or open. Closed systems are generally created by either commercial or state interests—courts regulate technology, companies control their proprietary technologies in the market place, and so on. Open systems, on the other hand, are generally associated with the public and with freedom and political transparency. Geert Lovink contrasts "closed systems based on profit through control and scarcity" with "open, innovative standards situated in the public domain."[3] Later, in his elucidation of Castells, he writes of the opposite, a "freedom hardwired into code."[4] This gets to the heart of the freedom rhetoric. If it's hardwired is it still freedom? Instead of guaranteeing freedom, the act of "hardwiring" suggests a limitation on freedom. And in fact that is precisely the case on the Internet where strict universal standards of communication have been rolled out more widely and more quickly than in any other medium throughout history. Lessig and many others rely heavily on this rhetoric of freedom.

We suggest that this opposition between closed and open is flawed. It unwittingly perpetuates one of today's most insidious political myths, that the state and capital are the two sole instigators of control. Instead of the open/closed opposition we suggest the pairing physical/social. The so-called open logics of control, those associated with (non proprietary) computer code or with the Internet protocols, operate primarily using a physical model of control. For example, protocols interact with each other by physically altering and amending lower protocological objects (IP prefixes its header onto a TCP data object, which prefixes its header onto an HTTP object, and so on). But on the other hand, the so-called closed logics of state and commercial control operate primarily using a social model of control. For, example, Microsoft's commercial prowess is renewed via the social activity of market exchange. Or, using another example, Digital Rights Management licenses establish a social relationship between producers and consumers, a social relationship backed up by specific legal realities (DMCA). Viewed in this way, we find it self evident that physical control (i.e. protocol) is equally powerful if not more so than social control. Thus, we hope to show that if the topic at hand is one of control, then the monikers of "open" and "closed" simply further confuse the issue. Instead we would like to speak in terms of "alternatives of control" whereby the controlling logic of both "open" and "closed" systems is brought out into the light of day.

---

[3] Geert Lovink, *My First Recession* (Rotterdam: V2, 2003), p. 14.

[4] Ibid., p. 47.

FEEDBACK VS. INTERACTION I

In the twentieth century there came to pass an evolution in the nature of two-way communication within mass media. This evolution is typified by two models: feedback and interaction. The first model consists of what Beniger calls the mass feedback technologies:

> Market research (the idea first appeared as "commercial research" in 1911), including questionnaire surveys of magazine readership, the Audit Bureau of Circulation (1914), house-to-house interviewing (1916), attitudinal and opinion surveys (a U.S. bibliography lists nearly three thousand by 1928), a Census of Distribution (1929), large-scale statistical sampling theory (1930), indices of retail sales (1933), A. C. Nielsen's audimeter monitoring of broadcast audiences (1935), and statistical-sample surveys like the Gallup Poll (1936).[5]

These technologies establish two-way communications, however, like the media they hope to analyze, the communication loop here is not symmetrical. Information flows in one direction, from the viewing public to the institutions of monitoring.

Contrast this with the entirely different technique of two-way communication called interaction. As a technology, interaction does not simply mean symmetrical communication between two parties. Instead we use interaction to mean an entire system of communicative peers, what Paul Baran called a "distributed network" of communication. We can offer here a list of interactive communications technologies to complement Beniger's list of feedback technologies above:

- Paul Baran's description of distributed communications (1964)
- Recombinant DNA and the practice of gene-splicing (1973)
- the ARPANET's mandatory rollover to the TCP/IP protocol suite (1983)
- Emerging infectious diseases (1980-2000)
- The Gnutella search protocol (2000)

Thus, interaction happens in an informatic medium whenever there exists a broad network of communicative pairs or multiples, and in which each communicative peer is able physically to effect the other. It doesn't happen in mass media like cinema or television because the audience is structurally unable to achieve a symmetrical relationship of communication with the apparatus (no matter how loudly one yells back at the screen). Interaction happens in the technology of gene-splicing because both sides are able physically to change the system: the scientist changes the physical system by inserting a genetic sequence, while DNA is the informatic code that teleonomically governs the development of physical life. Interaction happens in the Internet protocols for the same reason: protocols interact with each other by physically altering and prepending lesser protocological globs.

FEEDBACK VS. INTERACTION II

As models for two-way communication, feedback and interaction also correspond to two different models of control. Feedback corresponds to the cybernetic model of control, where, despite communication occurring bidirectionally between two parties, one party is always the controlling party and the other the controlled party. A thermostat controls temperature, not the other way around. Mass media like television and radio follow this model. Interaction, on the other hand, corresponds to a networked model of control, where decision-making proceeds multilaterally and simultaneously.

Many today say that new media technologies are ushering in a new era of enhanced freedom and that technologies of control are waning. We say, on the contrary, that double the communication leads to double the control. Since interactive technologies such as the Internet are based on multidirectional rather than unidirectional command and control, we expect to see an exponential increase in the potential for exploitation and control through such techniques as monitoring, surveillance, biometrics, and gene therapy. At lease the unidirectional media of the past were ignoring half the loop. At least television didn't know if the home audience was watching or not. Today's media have closed the loop. They physically require the maintained, constant, continuous interaction of users. This is the political tragedy of interactivity. We are "treading water in the pool of liquid power," as Critical Art Ensemble once put it.[6]

We long not for the reestablishment of lost traditions of solidification and naturalization as seen in patriarchy or conservatism. We long for the opposite vision: the past as less repressive from the perspective of informatic media. Television was a huge megaphone. The Internet is a high bandwidth security camera. We are nostalgic, then, for a time when organisms didn't need to produce data about themselves, for a time when one didn't need to talk back.

PROTOCOLS

The principle of political control we suggest is most helpful for thinking about biological and informatic networks is "protocol," a word derived from computer science but

[5] James Beniger, *The Control Revolution* (Cambridge: Harvard University Press, 1989), p. 20.

[6] Critical Art Ensemble, *The Electronic Disturbance* (New York: Autonomedia, 1994), p. 12.

which resonates in the life sciences as well. Protocol abounds in techno-culture. It is a totalizing control apparatus that guides both the technical and political formation of computer networks, biological systems and other media. Put simply, protocols are all the conventional rules and standards that govern relationships within networks. Quite often these relationships come in the form of communication between two or more computers, but "relationships within networks" can also refer to purely biological processes as in the systemic phenomenon of gene expression. Thus by "networks" we want to refer to any system of interrelationality, whether biological or informatic, organic or inorganic, technical or natural--with the ultimate goal of undoing the polar restrictiveness of these pairings.

In computer networks, science professionals have, over the years, drafted hundreds of protocols to govern email, web pages, and so on, plus many other standards for technologies rarely seen by human eyes. The first protocols for computer networks were written in 1969 by Steve Crocker and others. If networks are the structures that connect people, then protocols are the rules that make sure the connections actually work. From the large technological discourse of white papers, memos, and manuals, we can derive some of the basic qualities of the apparatus of organization which we here call protocol:

- protocol facilitates relationships between interconnected, but autonomous, entities;
- protocol's virtues include robustness, contingency, interoperability, flexibility, and heterogeneity;
- a goal of protocol is to accommodate everything, no matter what source or destination, no matter what originary definition or identity;
- while protocol is universal, it is always achieved through negotiation (meaning that in the future protocol can and will be different);
- protocol is a system for maintaining organization and control in networks.

In many current political discussions, networks are seen as the new paradigm of social and political organization. The reason is that networks exhibit a set of properties that distinguishes them from more centralized power structures. These properties are often taken to be merely abstract, formal aspects of the network--which is itself characterized as a kind of meta-structure. We see this in "pop science" books discussing complexity and network science, as well as in the political discourse of "netwars" and so forth. What we end up with is a metaphysics of networks. The network, then, appears as a universal signifier of political resistance, be it in Chiapas, Seattle, Geneva, or online. What we question is not the network concept itself, for, as a number of network examples show, they can indeed be effective modes of political struggle. What we do question is the undue and exclusive reliance on the metaphysics of the network, as if this ahistorical concept legitimizes itself merely by existing.

POLITICAL ANIMALS

Aristotle's famous formulation of "man as a political animal" takes on new meanings in light of contemporary studies of biological self-organization. For Aristotle, the human being was first a living being, with the additional capacity for political being. In this sense, biology becomes the presupposition for politics, just as the human being's animal being serves as the basis for its political being. But not all animals are alike. Deleuze and Guattari distinguishe three types of animals: domestic pets (Freudian, anthropomorphized Wolf-Man), animals in nature (the isolated species, the lone wolf), and packs (multiplicities). It is this last type of animal--the pack--which provides the most direct counter-point to Aristotle's formulation, and which leads us to pose a question: If the human being is a political animal, are there also animal politics? Ethnologists and entymologists would think so. The ant colony and insect swarm has long been used in science fiction and horror as the metaphor for the opposite of Western, liberal democracies. Even the language used in biology still retains the remnants of sovereignty: the queen bee, the drone. What, then, do we make of theories of biocomplexity and swarm intelligence, which suggest that there is no "queen" but only a set of localized interactions which self-organize into a whole swarm or colony? Is the "multitude" a type of animal multiplicity? Such probes seem to suggest that Aristotle based his formulation on the wrong kinds of animals. "You can't be one wolf," of course. "You're always eight or nine, six or seven."[7]

THE GHOST IN THE NETWORK

In discussing the difference between the living and the nonliving, Aristotle points to the phenomena of self-organized animation and motility as the key aspects of a living thing. For Aristotle the "form-giving Soul" enables inanimate matter to become a living organism. If life is animation, then animation is driven by a final cause. But the cause is internal to the organism, not imposed from without as with machines. Network science takes up this idea on the mathematical plane, so that geometry is the soul of the network. Network science proposes that heterogeneous network phenomena can be understood through the geometry of graph theory, the mathematics of dots and lines. An interesting outcome of this is that seemingly incongruous network phenomena can be grouped according to their similar geometries. For instance the networks of

[7] Gilles Deleuze and Félix Guattari, *A Thousand Plateaus* (Minneapolis: University of Minnesota Press, 1987), p. 29.

AIDS, terrorist groups, or the economy can be understood as having in common a particular pattern, a particular set of relations between dots (nodes) and lines (edges). A given topological pattern is what cultivates and sculpts information within networks. To in-form is thus to give shape to matter (via organization or self-organization) through the instantiation of form--a network hylomorphism. But further, the actualized being of the living network is also defined in political terms. "No central node sits in the middle of the spider web, controlling and monitoring every link and node. There is no single node whose removal could break the web. A scale-free network is a web without a spider."[8] Having-no-spider is an observation about predatory hierarchy, or the supposed lack thereof, and is therefore a deeply political observation. In order to make this unnerving jump--from math (graph theory), to technology (the Internet), to politics ("a web without a spider")--politics needs to be seen as following the necessary and "natural" laws of mathematics; that is, networks need to be understood as "an unavoidable consequence of their evolution."[9] In network science, the "unavoidable consequence" of networks often resembles something like neoliberal democracy, but a democracy which naturally emerges according to the "power law" of decentralized networks. Like so, their fates are twisted together.

ACKNOWLEDGMENTS

An earlier version of this article appeared in Joke Brouwer et al., *Feelings Are Always Local* (V2/NAI Publishers), the catalog for the 2004 Dutch Electronic Arts Festival (DEAF).

[8] Albert-László Barabási, *Linked* (Cambridge: Perseus Publishing, 2002), p. 221.

[9] Ibid.