# FCJ-018 Living Dead Networks

Eugene Thacker, School of Literature, Communication, and Culture, Georgia Institute of Technology.

## Contagion and Transmission

2 In contemporary popular culture, ideas about contagion are often tied up with ideas about information transmission. The film 28 Days Later, for instance, opens with a harrowing scene in which primates undergo medical experiments by being exposed to large doses of violent media images. Though the link between these images and the 'rage virus' that takes over the British Isles is never explained, the film abstractly puts forth the idea that there is some relation between media image and biological virus. The Japanese horror film Ringu takes this a step further, imaging a videotape, which causes its viewer to suffer a mysterious death. Rumors about the videotape begin circulating and the videotape itself becomes a kind of vector for the contagious and ultimately fatal images. But it is not only in film that such connections between contagion and transmission are expressed. The online, multiplayer video game Resident Evil: Outbreak takes the contagion-transmission link even further in its existence as a network-based game. The game follows the narrative of many of the other Resident Evil games, in which a secret corporate bioweapons program runs amok, releasing its experimental virus into the unsuspecting population of a nearby city. One of the aims of the game is not only to contain the spread of the epidemic (which has the effect of turning its host into a flesh-eating zombie), but also to exterminate those that are already infected. As an online, multiplayer game, Resident Evil: Outbreak is actually played in real-time over the Internet, with other players who take on other roles or characters in the game world. Thus the biological network of the epidemic within the diagesis of the game world is layered onto the informatic network or technical infrastructure, which enables the game to be played. In addition, players in the game must gather various bits of information regarding the status of the epidemic in the infected city (urban regions infected, number of civilians infected, number of kills), making the game a hybrid of typical 'FPS' (first-person shooter) games and a public health computer simulation.

3 What each of these examples does is to raise the issue of the relation between contagion and transmission, or between the assumed materiality of biology, and the assumed immateriality of information. We are accustomed to thinking of contagion as a biological or epidemiological term, which is then metaphorized into non-biological contexts to speak of computer 'viruses,' cultural 'memes,' or 'viral marketing.' Conversely, information is colloquially thought of as an abstract, immaterial entity that may exist in different physical media (DVDs, CDs, or hard drives). Classical information theory, which states that 'the semantic aspects of information are irrelevant to the engineering problem' (Shannon and Weaver, 1965: 31), still influences many of the basic assumptions in the construction and maintenance of information networks today. In short, the concept of contagion presumes a materiality that can then be abstracted into metaphor, while the concept of information assumes an immaterial form or pattern that can then be materialized in a range of physical media.

4 For this reason, it is no surprise that a great number of horror films combine epidemics with the figure of the zombie, or the 'living dead.' Zombies always seem to result from the contagion of biological epidemics, as if the ultimate fear of contagion was not simply death itself, but a death beyond death, a 'living death' in which the biological is exclusively biological, in which the self is nothing but a body. But the figure of the zombie has also gone through many metamorphoses, from the earliest films (e.g. White Zombie) depicting eroticized Haitian voodoo rituals, to the American and Italian splatter horror films of the 1970s (the films of Romero and Fulci), in which zombies are often metaphors for the 'silent majority.' However contemporary genre horror (in film, fiction, games, and comics) adds a twist to the familiar motifs of the zombie film: the role of information in either transmitting, propagating, or even producing contagion. In its own language of genre motifs and campy self-reflexivity, contemporary zombie horror asks an interesting question: how is our understanding of biological epidemics affected by our ambient environment of computer and information networks? That is, how does transmission affect contagion, and vice-versa? Traditionally, zombie films represent the paradox of the living dead as the 'animate corpse' or the state of being nothing but the 'bare life' of a body. The horror of contemporary 'living dead' is not just the fear of being reduced to nothing but body, but, in the 'network society,' perhaps the

horror of the 'living dead' is the fear being reduced to nothing but information – or not being able to distinguish between contagion and transmission. In this sense the paradox of the living dead is also the paradox of 'vital statistics,' a sort of living dead network that exceeds and even supercedes the 'bare life' of the organism.

**A Note on Method**

5 In a sense, emerging technoscientific fields are more avant-garde than the most avant-garde cultural theory. Hybrid DNA chips, neural cells communicating across the Internet, enzyme-based 'wet' computers, in vitro DNA libraries, and computer immune systems are all examples of this vanguard character of contemporary technoscience. Indeed, one of the unique characteristics presented by the artifacts of technoscience is that they seem to demonstrate their contingencies, their modes of knowledge-production, their performative laboratory contexts, and their disciplinary and institutional sites. I speak of such artifacts with a degree of vitalism (and irony) because, in many cases, they demonstrate something in their performance that is in excess of the intentions and discourses that enframe them; they increasingly demand to be considered as fleshy but nonhuman. They are artifacts that not only perform biological labor and produce information, but they are artifacts that also intervene in human decision-making and action.

6 Such artifacts demand a mode of critical engagement that is as uncanny as they are, expressing a sense of the most everyday that is the most unbelievable. Gilles Deleuze suggests one such approach, in his notion of the 'diagram.' In its colloquial sense, a diagram is a graphical mode of representation that is used to conceptualize a process or to produce a model (a workflow diagram, a technical diagram). In this way, a diagram is an analytic tool, a visual artifact pointing to its referent. But a diagram also brings forth relationships between entities in a system that are not apparent in the system itself; it also reveals latent, existing relations, and as such it may cut across traditional distinctions. It is this abstract and concrete character of the diagram that Deleuze emphasizes when he speaks of power relations as being 'diagrammatic.' For Deleuze, 'the diagram is no longer an auditory or visual archive but a map, a cartography' (1999: 34). Furthermore, 'every society has its diagram(s),' its unique topology of the discursive and non-discursive, 'the map of relations between forces that constitute power' (1999: 35, 36).

7 A diagrammatic method revolves around the issue of form. In the work of Michel Foucault, Deleuze identifies a constant interplay between a form that organizes 'matters' (e.g. the prison, the hospital, the school) and a form that canalizes 'functions' (punishing, curing, educating). Now, neither of these aspects of form can be reduced to the other (for instance, 'curing' cannot be reduced to the hospital). But, asks Deleuze, is there a common term that stitches or weaves them together? For Deleuze, the diagram is this topological relation within the forms of power relations, an 'immanent cause that is coextensive with the whole social field' (1999: 37). Foucault is therefore less a 'new historian' and more a 'new cartographer,' drawing out points, relations, and topologies.

8 Deleuze points to three characteristics of the diagram, characteristics that will guide this essay. First, each diagram abstracts a 'spatio-temporal multiplicity,' existing in a way that occupies topologies of all sorts (geographic, economic, biological topologies). Deleuze gives the example of Foucault's history of madness, in the shift from the 'leprosy' diagram of the Middle Ages (which functions by excluding and dividing) to the 'plague' diagram of the early modern era (which functions by including and regulating). A second feature of the diagram is that it is 'continually churning up matter and functions in a way likely to create change' (1999: 35). Diagrams are always about to undergo a phase change, as when Foucault describes hospital reforms in pre-Revolutionary France as a combination of sovereign (state-mandated) and disciplinary (surveillance) diagrams. Finally, Deleuze states that the diagram 'produces a new kind of reality' by drawing out 'unexpected conjugations or improbable continuums' that constitute a particular object of study (1999: 35).

9 The diagram provides a cross-section, a transversal (similar to the transverse cross-sections used on frozen cadavers in digital anatomy). Diagrams cut across separate organs and organ systems, they cut across institutions, governments, social classes, technical paradigms, and cultural forms. The resultant view is very different from the anthropomorphic body politic, though still familiar, if only in a dizzying way. Given that Deleuze is often referenced as the philosopher of becoming, we may be inclined to think of a diagram as that which reveals the 'becoming' of the event. But I would argue instead that a diagram is more like a demonstration, a technical 'demo' of something that is

already in effect. A diagrammatic method would therefore draw out the 'demo' function of each particular context. At its most extreme, a diagrammatic approach is simply a crafted series of juxtapositions. The diagram appears to simply present information, a montage of data and flesh, an artifactual dérive.

**Information Security / Mathematical Epidemiology**

10 Let us begin with the separate fields of information security and mathematical epidemiology. The cultural con-fusion between contagion and transmission mentioned above has its analogue in these two related fields. In information security, biological tropes are used to understand computer 'viruses' and design 'computer immune systems.' In mathematical epidemiology, mathematical, statistical, and probabilistic methods are used to study the dynamics between populations and disease, which is now being extended in the use of computers to simulate and forecast epidemic outbreaks.

11 However, it is not the case that we begin with two separate fields (biology and informatics) which are then fused together via contemporary technoscience, and neither is it the case that a primary unity is subsequently bifurcated into the material (biology) and immaterial (information) domains. Instead what we see is a continual process of differentiations, transdifferentiations, and connections of terms that are at once ontological and thoroughly pragmatic – that is, a diagram.

12 In the case of information security, biological tropes began being applied to accidental or intentionally caused glitches in computer systems in the mid-1960s, with the first intentionally designed computer viruses (e.g. 'Darwin' and 'Cookie Monster'). Many of these vague uses of biologically-inspired terms were crystallized in the work Fred Cohen, whose writings on computer viruses were published in the 1980s, just as personal computing and civilian Internet technologies were gaining momentum. The language of computer 'viruses' and 'infected' computer systems continue to characterize more recent descriptions of Trojan horses, Internet worms, and '5th generation polymorphic' viruses. Currently, information security has expanded its approach to include 'adware,' 'spyware,' and even 'spam' email. Generally speaking, information security concerns itself primarily with ensuring the ongoing systemic integrity of a given computer system or network. This, of course, involves a number of procedures, from identifying what a 'system' or 'network' is (e.g., an individual computer or a local network of computers), to devising techniques for preventing intrusion and infection (e.g. 'firewalls' and 'anti-virus' software). Not surprisingly, the rhetoric of war often accompanies the biologically inspired concepts of information security, which has had the effect of making information security for the average user an everyday battle.

13 However, the basic premise of information security is that specific types of computer behaviors can be understood through the lens of biology. If, as the analogy goes, a piece of software can infiltrate and infect a computer system just as a virus can infiltrate and infect a biological system, then it follows that the best way to prevent such attacks is to construct an 'immune system' for the computer. As one research article states, 'improvements [in computer security] can be achieved by designing computer systems that have some of the important properties illustrated by natural immune systems' (Forrest et al., 1996: 1). Furthermore, just as immunology is predicated on the 'self-nonself' distinction, 'the problem of protecting computer systems from malicious intrusions can similarly be viewed as the problem of distinguishing self from nonself' (Forrest et al., 1996: 3). In addition, designing such computer immune systems require not just the micro-view of immunology, but also a knowledge of the macro-view of epidemiology, or how infectious agents spread throughout a population. The research on 'computer epidemiology' makes just this argument. For instance, Kephart et al. (1993) that a focus on the modes of distribution of computer viruses, including their birth rates, death rates, incident, and threshold, can offer a more effective, global view of how computer viruses affect not just single machines, but entire networks of machines.

14 Most recently, this view has influenced the emerging field of 'network science,' whose scope is not limited to the biological or informational domains, but proposes a synoptic view of networks as both ubiquitous and universal. Albert-László Barabási's work on 'scale-free' networks (in which few nodes are highly connected, a many nodes are minimally-connected) has suggested that traditional methods of tracking down computer viruses are determined to fail in complex networks (Barabási, 2002: 123-42). Instead, Barabási suggests that an approaches that 'discriminate between the nodes, curing mostly the highly connected nodes, can restore a finite epidemic threshold and

potentially eradicate a virus' (Barabási and Dezsno, 2002: 1). In other words, the points of a network that are the most connected are also the most vulnerable to attack or infection. Countering the spread of a computer virus or worm will depend not on targeting individual pieces of software, but on managing the traffic at the most busy nodes or hubs within a network.

15 These are all examples of the way in which biology influences computer science – or, to be more specific, the ways in which concepts and models from immunology and epidemiology influence information security. But the reverse also occurs, and in this regard, epidemiology is an important hinge between computer science and biology. While recent information security research has incorporated the metaphors and concepts of epidemiology, the much lengthier history of epidemiology shows a close relation to mathematical and informatic modes of understanding disease at the macro-level. In 17th century London, the weekly mortality tables compiled by parish clerks provided the basis for the demographic studies of John Graunt, whose mathematical analyses reveal trends in infant mortality and fatal diseases in select urban areas. [1] Another statician, William Petty, characterized such studies as 'political arithmetic' or 'political anatomy.' [2] This mathematical view of death and disease as the macro-level are, as Michel Foucault points out, intimately tied to the intersections of politics and medicine of the time. The controversies surrounding the English Poor Law, the medical reforms of the Hôtel Dieu in Paris, and the development of a system of 'medical police' in Prussia, are all profoundly connected to the growing interest in a quantitative, mathematical view of disease at the macro-level. [3] This 'statistical enthusiasm,' as historian Ian Hacking calls it, was not only concerned with charting the spread or patterns of a population's health, but it was also centrally concerned with the articulation of specific categories into which disease and population types could be set. 'Enumeration demands kinds of things or people to count' (Hacking, 1982: 280).

16 Epidemiology, in its historical context, was not just a matter of counting, however. It required an 'open field' of observation, and an analytical sensibility that could encompass the indeterminate. An epidemic disease was not an autonomous entity that could be enclosed in a box, or categorized in a table; its totality lay precisely in its continual or recurring nature. Throughout the 18th century, epidemiology came to be opposed to the classificatory science of nosology, and it was this time-based, distributed view that led to the recognition of the network effects of disease: 'The analysis of an epidemic does not involve the recognition of the general form of the disease, by placing it in the abstract space of nosology, but the rediscovery, beneath the general signs, of the particular process, which varies according to circumstances from one epidemic to another, and which weaves from the cause to the morbid form a web common to all the sick' (Foucault, 1973: 24). In this sense, the concurrent observations of John Snow and William Budd, both studying the effects of cholera in the 19th century, can be seen as demonstrations of this point. [4] In particular, Snow's famous epidemiological maps of south London reveal a concept that is central to network thinking: the layering, in one space, of different types of networks (e.g. networks of infection, networks of water pumps and sewage channels, and the overall socio-economic topology that described the particular Broad Street neighborhood).

17 What we can highlight in epidemiology is a two-fold network consciousness: an awareness of 'epidemics' as discrete entities displaying network properties, and, inseparable from this, an awareness of the need for network-based techniques for analyzing, mapping, and securing against epidemics. Influenced by the mathematical epidemiology of Norman Bailey, contemporary network science has taken up many of the lessons of epidemiology – as well as information security. As Duncan Watts notes, 'viruses, both human and computer, essentially perform a version of what we have been calling a broadcast search throughout a network,' a mode of propagation in which 'the more contagious a virus is, and the longer it can keep the host in an infectious state, the more efficient it is at searching' (Watts, 2003: 166). Thus, understanding the characteristics that define an epidemic is a first step towards devising strategies for counteracting it. For this reason, it is no surprise that surveillance, or the gathering of information, is a central part of public health and epidemiology. 'The old simple schema of confinement and enclosure – thick walls, a heavy gate that prevents entering or leaving – began to be replaced by the calculation of openings, of filled and empty spaces, passages and transparencies' (Foucault, 1979: 172). It is this shift towards contagion and/or transmission that we are witnessing today.

## Pathogenic Information vs. Informed Pathogens

18 So we have two separate fields, each of which integrates informatics and materiality differently through a network paradigm – this last part is crucial. If information security tells us that certain kinds of computer behavior can be understood through the lens of epidemiology, then it is equally important to note that modern epidemiology tells us that infectious disease can be understood through the lens of mathematics, statistics, and informatics. In one the basic idea is that we can understand particular types of computer behavior through the lens of biology, while in the other the basic idea is that we can understand infectious disease through the paradigm of informatics.

19 This uneven, twofold integration results, however, in two opposing ontological positions. Recall our opening discussion regarding contagion and transmission. While the view of contagion presumes a condition of biological materiality, that can then be abstracted into metaphor (computer 'virus'), when contagion is considered within epidemiology, it also implicitly links contagion with material and biological processes of rate of infection, logistic growth, and epidemic thresholds, encapsulated in the often-referenced SIR (susceptible-infected-removed) model. [5] But these material and biological processes are, in epidemiology, also informational processes that reflect the specific topology of an infectious disease. Mathematical epidemiology, despite its abstruse qualities, must, by definition refer to a real biological-material condition (if for no other reason than this material condition provides the basis for data abstraction).

20 But the same conundrum also holds for the view of transmission, and the field of information security. While the view from classical information theory assumes an immaterial core that can then be instantiated in a range of material, physical media (the assumption behind simple file conversions), transmission is also never separate from its materiality. Indeed, there is a 'materiality of informatics,' in that the classical separation of 'message' from 'channel' is only a heuristic means of assessing the accuracy of information transmission. The reality is that information is never separate from its channel, just as the message is never separate from its medium. Not only does the supposedly immaterial quality of information always require a material substrate (radio towers, fiber optic cable, WiFi transmissions), and not only does information 'matter' in its social effects, but transmission is inseparable from its materiality.

21 Therefore, while the relationship between contagion and transmission is not an exactly symmetrical one, we can derive two distinct positions. While information security views information as being immaterial, epidemiology is predicated on the assumption that information is material. In the former position what we see is pathogenic information – that is, information in the classical, technical sense that has become 'viral' – while the latter position what we see are informed pathogens – that is, biological epidemics that, through epidemiology, become information-dense entities. From this, we can say that information security, as a field, deals with pathogenic information, while mathematical epidemiology deals with informed pathogens.

22 Both, however, are united in their use of the 'network paradigm' to comprehend their objects of study. In both cases, the 'network' serves as the model through which the apparently disparate phenomena of infectious disease and computer processes can be analyzed. However, while the view of pathogenic information (information security, computer 'viruses') assumes information as immaterial, the view of informed pathogens (mathematical epidemiology) presumes a material aspect to information. The question we can now ask, is what sorts of networks result when these apparently opposing views of contagion and transmission are layered on top of each other?

## DSN, not DNS

23 In the past five years or so – and especially in the time since 9/11 – there have been a number of efforts to develop disease alert and response systems that would make use of information networks. The US CDC (Centers for Disease Control and Prevention) began a number of such projects in the 1990s, with acronyms such as LRN (Laboratory Response Network) and NEDSS (National Electronic Disease Surveillance System). [6] The impetus behind such programs was the alarming number of new and emerging infectious diseases being tracked nation-wide by the CDC, and internationally by the WHO (World Health Organization). In addition, the 1980s and 1990s saw a number of instances of biological sabotage (often by religious cults), both within the US and in other countries such as Japan. [7] Such events, combined with evidence suggesting a Soviet offensive bioweapons program in 1979, collectively made 'biodefense' an increasing concern of both public health and national security within the US. [8] It became evident that an information

network like the Internet could be a crucial tool in enabling health officials to foresee potential outbreaks before they have a wide-spread effect on a population.

24 In recent years, two events in particular have given the need for such programs greater urgency. One is the 2001 anthrax attacks that occurred within the US, in which several letters containing a weaponised strain of anthrax in powdered form were sent through the US postal system to media and government offices in New York and Washington, DC. While the anthrax in the letters did not cause a nation-wide or state-wide epidemic, it did cause what one journalist called 'mass disruption,' triggering a state of public alarm through the elaborate media coverage given to the events. Undoubtedly the anthrax attacks were but one important factor behind the 2002 Bioterrorism Act, which, among other things, restricted the access to and research on approximately fifty 'select biological agents' – even within legitimate, university-based biology labs receiving government funding. The other event that has made the need for alert and response systems more urgent was the 2003 SARS epidemic. While SARS barely deserves the title of 'epidemic' in comparison to AIDS and tuberculosis worldwide, the condensed time span in which it spread from China to Canada made it a perfect case study for next-generation alert and response systems. In fact, it was, in part, thanks to the WHO's 'Global Outbreak Alert and Response Network' that the spread of SARS was limited to the cities through which it traveled. [9] Coordinating among hospitals and clinics in infected areas in Beijing, Singapore, Toronto, Hong Kong, and elsewhere, and making use of a central server to upload and download patient data, the WHO was able to issue travel advisories and suggest countermeasures to the spread of SARS. In a sense, the WHO's network provided a proof-of-concept that information networks could be effectively used in countering epidemic outbreaks.

25 This idea – the use of information networks to monitor, prevent, and counter-act epidemics – is called 'biosurveillance' by the US government. The systems that are used are variously referred to as 'syndromic surveillance systems' or 'disease surveillance networks.' For the sake of brevity, and following upon the penchant for acronyms in government agencies, we can broadly refer to them all as disease surveillance networks or simply 'DSN' (not to be confused with 'DNS,' or the 'domain name system' that hierarchically stratifies Internet server addresses). In the wake of 9/11, the US Department of Homeland Security and Department of Health and Human Services has been especially active in promoting the need for a sophisticated, nation-wide DSN. Since the late 1990s, prototype DSNs have been active in multiple cities nationwide. [10] In early 2003, the Homeland Security 'BioWatch' program was tested in a number of American cities, with the cooperation of state and local governments. [11] The BioWatch system routinely took air samples to test for the presence of biological agents, and was connected to a network, through which it would send the data to be processed. This program became the forerunner of the US Biosurveillance program, which received a record-setting $274 million for the development of DSNs alone. The program aims to 'enhance on-going surveillance programs in areas such as human health, hospital preparedness, state and local preparedness, vaccine research and procurement, animal health, food and agriculture safety and environmental monitoring, and integrate those efforts into one comprehensive system' (US Department of Homeland Security, 2004). Proposals and projects surrounding DSNs are, as of this writing, growing at an exponential rate, and include projects underway both from the private sector as well as government-funded, university-based research.

### Networks Fighting Networks

26 The existence and development of DSNs is noteworthy for a number of reasons. Chief among these is the way in which the DSNs integrates – or appears to integrate – the contrary views of contagion and transmission mentioned above (the view of 'pathogenic information' versus 'informed pathogens,' or information security versus mathematical epidemiology). The DSNs bring together the views of contagion and transmission into a single 'artifactual' system. On one view, 'information' is assumed to be immaterial (in that it is a unit of quantitative abstraction), but it operates through a biological process (in that the computer 'virus' has as its aim the infection of hosts and replication of itself). In other words, in the view of information security, biological process is abstracted from biological materiality, and is seen to inhabit the so-called immaterial domains of data and light.

27 This is countered by the other view, in which 'information' has to be material in order for an analysis to be accurate, or for a model to be effective. If there is no correspondence between an

epidemic model and the actual epidemic, then epidemiology and public health have no ground on which to stand. Thus, even mathematical epidemic models are always forced to begin from empirical data. Yet, at the same time, there is ambiguity in this materiality of information. For, in the case of epidemiology, biological or medical information is understood both as a product of knowledge-based systems (e.g. medical records and disease statistics), and as a real 'thing' that spreads throughout a population (e.g. mutations in the RNA 'code' of a virus that enables it to evade medical therapies). In other words, in epidemiology – more specifically in its mathematical guises – informational processes are extracted from the particular media through which and across which information flows. These views intersect in the DSNs. Between the genetic code of a virus, the rate of epidemic growth, its demographic distribution, and the role of medical records, health insurance policies, and sales of pharmaceutical vaccines, there is an ambiguous continuum of informational processes that is informatic and yet thoroughly material.

28 One way of understanding this ambiguity with regards to DSNs is to return to the concept of the network. What is perhaps most striking about DSNs and the very idea of biosurveillance, is the way in which it positions one type of network (a computer network) against another type of network (a biological network). For many epidemiologists, the 2003 SARS epidemic has become a case study in this regard. The WHO's outbreak network – which included network servers and software, as well as conferencing technologies – intentionally positioned itself as a network against the spread of the SARS coronavirus. During the outbreak, a Newsweek article (28 April 2003) summarized this view: 'a 32-year-old Singaporean physician had attended a conference in New York and was on his way home—and he was exhibiting suspicious respiratory symptoms. Reports of cases in Canada and Singapore had recently made their way to Geneva; the predawn call made the situation all the more urgent. WHO officials tracked the man to a Singapore Airlines flight, due in Frankfurt at 9:30 that morning. By the time the plane touched down, quarantine specialists in goggles and jumpsuits were waiting to take the doctor and his two travel companions to an isolation ward.' Such 'preparedness and response' actions involve not just technology, but also negotiations among WHO officials with governments and hospitals, from Toronto to Beijing. All these processes of information exchange and communications constituted part of the WHO's counter-epidemic network.

29 The resultant effect is that of a real-time battle between networks: one, a biological network operating through infection, but abetted by the modern technologies of transportation; the other, an information network operating through communication, and facilitated by the rapid exchange of medical data between institutions. This is a situation of what we can call networks fighting networks, in which one type of network is positioned against another, and the opposing topologies made to confront each other's respective strengths, robustness, and flexibilities. In their analyses of new modes of social organization and conflict, John Arquilla and David Ronfeldt (2001) have pointed to the importance of the network paradigm. What they call 'netwar' reflects the contemporary integration of information technologies and network-based modes of political action, culminating in a Janus-faced dichotomy between pro-democracy activism on the one hand, and international terrorism on the other. As they state, 'governments that want to defend against netwar may have to adopt organizational designs and strategies like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age' (Arquilla and Ronfeldt, 2001: 15). The take-home message is that network forms of organization are highly resistant to top-down, centralized attempts to control and restrain them. Instead, the authors suggest that 'it may take networks to fight networks' (Arquilla and Ronfeldt, 2001: 327). In this case, biosurveillance and DSNs can be seen as initial attempts by governments to re-frame public health within the context of information technologies and national security. [12]

30 However there are a number of significant differences between what Arquilla and Ronfeldt call 'netwar' and the example of biosurveillance and DSNs. The majority of case studies that are considered under the rubric of 'netwar' – case studies which range from the Zapatista resistance, to the anti-WTO protests in Seattle and Geneva, to al-Qaeda – imply human action and decision-making as a core part of the network's organization. In fact, one limit of the netwar approach is that it does not push the analysis far enough, to consider the uncanny, 'nonhuman' characteristics of such networks. In a sense, the interest in the study of network forms of organization is exactly

in their decentralized, or even distributed mode of existing – and for this reason research in biological self-organization often provide a reference point for netwar analysis (e.g. in studies of crowd behavior, flocking, or swarming). Yet, as many studies make clear, the result of netwar analysis is, ultimately, to gain a better instrumental knowledge of the 'how' and 'why' of network forms of organization (that many netwar studies have come out of the RAND think-tank environment is indicative in this regard). In other words, approaches to studying networks seem to be caught between the views of control and emergence with respect to networks as dynamic, living entities. On the one hand, networks are intrinsically of interest because the basic principles of their functioning (e.g. local actions, global patterns) reveal a mode of living organization that is not and cannot be dependent on a top-down, 'centralized' mindset. Yet, for all the idealistic, neoliberal visions of 'open networks' or 'webs without spiders,' there is always an instrumental interest that underlies the study of networks, either to better build them, to make them more secure, or to deploy them in confronting other network adversaries or threats. At the same time that there is an interest in better controlling and managing networks, there is also an interest in their uncontrollable and unmanageable character.

**Indeterminate Control**

31 The challenges put forth in this tension between 'control' and 'emergence' are not just technical problems, but are challenges that raise ontological as well as political questions. From the network perspective, case studies like the 2003 SARS epidemic look very much like a centralized information network counter-acting a decentralized biological network. The WHO's outbreak response network coordinated the exchange of data through network servers and conference calls, and health advisories could then radiate from this central node. By contrast, SARS infection was maximized by moving through the highly-connected nodes of airports and hotels. The strategy of DSNs, then, is to canalize transmission in order to fight the decentralization of contagion. If an epidemic is 'successful' at its goals of replication and spread, then it gradually becomes a distributed network, in which any node of the network may infect any other node. [13]

32 Health officials warned in late 2003 that the SARS virus may very well make occasional re-appearances during the cold and flu season, implying that new and emerging infectious diseases are less one-off events, and more of an ongoing milieu. By definition, if a network topology is decentralized or distributed, it is highly unlikely that the network can be totally shut down or quarantined: there will always be a tangential link, a stray node (a 'line of flight'?) that will ensure the minimal possibility of the network's survival. This logic was, during the Cold War, built into the design of the ARPAnet, and, if we accept the findings of network science, it is also built into the dynamics of epidemics as well. While the idea of totally distributed networks and 'open networks' have become slogans for the peer-to-peer and open source cultures, the hybrid quality of DSNs and biosurveillance (at once material and immaterial, contagion and transmission) reveal the frustratingly oppressive aspects of decentralization. Furthermore, the network organization of epidemics are, as we've noted, much more than a matter of biological infection; epidemic networks of infection are densely layered with networks of transportation, communication, political negotiation, and the economics of health care.

33 In DSNs, the tension between 'control' and 'emergence' points to the 'nonhuman' character of networks. DSNs are nonhuman networks, not because the human element is removed from them and replaced by computers, but precisely because human action and decision-making form constituent parts of the network. This point is worth pausing on. Despite the technophilic quality of many biosurveillance projects, their most interesting network properties come not from the 'automated detection systems,' but from the ways in which a multiplicity of human agencies produces a intentional yet indeterminate aggregate effect. While much time and money is spent on computer systems to model and forecast epidemic spread, such systems are always 'best guesses.' The same is implied in the human involvement – autonomous and conscious – in the epidemics that biosurveillance aims to prevent. As we've noted, the layered quality of networks (infection, transportation, communication) gives each particular epidemic incident a singularity that frustrates any sort of reductive, quantitative modeling. In short, for biosurveillance the challenge for the network management of an epidemic is how to articulate control within emergence. The nearly paradoxical question posed by biosurveillance with regards to epidemics is this: is it possible to construct a network for articulating intention within indeterminacy?

34

Let us rephrase the situation of biosurveillance in plain terms, to make the political issues at stake clearer. An epidemic is underway. An agency – the CDC for example – must develop and deploy a strategy for containing the epidemic. Because epidemics are understood to be network forms of organization, any attempts to contain and eradicate the epidemic must similarly use a network approach. Thus, one network – that of the CDC's NEDSS – must counteract another network – that of the disease. We thus have an instance of 'networks fighting networks.' However the two networks are not simply mirror images of each other. The CDC's network is a centralized network that makes use of information technologies, while the epidemic is a more decentralized combination of biological, technological (e.g. air travel), and other types of networks. To prevent the latter network from becoming more diffuse, the former network becomes more canalized, or rather, more selective. Thus, the main challenge put forth to the first network (the CDC) is how to intervene in, perturb, and shape the topology of the second network (the disease). Meeting this challenge means, then, deciding on the exceptional instances in which intervention and action is warranted. Intervention itself is not so much the issue; rather, it is the decision on intervention that is at stake.

**Network Exception**

35 We can summarize this even further: the challenge of biosurveillance is the challenge of establishing sovereignty within a network. As a political and juridical term, the concept of sovereignty is already defined by paradox. As Giorgio Agamben (1998) notes, the defining feature of modern sovereignty is not that it is the power to execute the law, but that it is the capacity to claim the exception to the rule. 'I, the sovereign, who am outside the law, declare that there is nothing outside the law' (Agamben, 1998: 15). Agamben's dense and thought-provoking analysis suggests that, when sovereignty establishes itself in this way (as the exception to the rule), it necessarily produces its other in the figure of 'homo sacer,' or the 'bare life' that is outside both the political and social orders ('life that can be killed and yet not sacrificed'). Sovereignty's own injunction is to be at once outside and inside the juridical-political order, at once legitimized through law, and yet capable of deciding when the law should be suspended. What is captured in this no-man's-land is 'bare life,' life that is outside of the political order, and yet, by being abandoned in this way, is also inscribed within it. The radicalism of Agamben's proposal is that this logic is common to both the totalitarianism of National Socialist medicine, as well as to the discourse of 'human rights' that emerged in the post-war era. [14] Both the claim to protect the population from hereditary disease, and the claim that human beings, by the fact of being alive, have inalienable rights, draw upon the 'zone of indistinction' between sovereignty and 'bare life.' Whenever 'bare life' or 'life itself' is at stake, the population or body politic is also at stake, legitimizing emergency measures, or the declaration of a 'state of exception.' In this way, sovereignty makes itself known at the very point at which 'bare life' comes under threat, in the state of emergency or state of exception. As both Agamben and Foucault note, this sovereign decision on 'life itself' is also often a decision on 'death itself.' When the state of exception is in effect, then the defense of the 'life itself' of the population depends on a range of exceptional measures or actions taken, actions which often have ambivalent effects.

36 No other 'state of exception' is quite as exceptional as an epidemic – except perhaps war. In fact, the most powerful state of exception is one that is not recognized as such. The sovereign exception obtains its most intense level of legitimation in an environment in which the exception is the rule – that is, a situation in which 'exception' is directly correlated to a 'threat' that is, by definition, indeterminate. In this regard nothing is more exceptional than the inability to distinguish between epidemic and war, between emerging infectious disease and bioterrorism. Although, wars have the benefit of being waged by individual and collective human agents, humans fighting humans. Epidemics ignite public fears with great ease, in part because the 'enemy' is often undetected, and therefore potentially everywhere. But more than this, it is the alien, nonhuman character of epidemics that incite public anxiety – there is no intentionality, no rationale, no aim except to carry out iterations of what we understand to be simple rules (infect, replicate, infect, replicate…). The exceptions of epidemics and war implode in biological warfare, bioterrorism, and in the way that US policy enframes the public health response to infectious disease. In the US, the rubric 'biodefense' – which is increasingly taking on epidemic proportions itself – has come to incorporate within itself what was, at least on an institutional level, the non-

defense concerns of public health. A recent White House press release states that 'the [US] President believes that, by bringing researchers, medical experts, and the biomedical industry together in a new and focused way, our Nation can achieve the same kind of treatment breakthroughs for bioterrorism and other threats that have significantly reduced the threat of heart disease, cancer, and many other serious illnesses' (White House, 2003).

37 The 'biopolitical' analyses of sovereignty by Agamben and Foucault become more complicated with biosurveillance and DSNs. This is because of the way in which biosurveillance ambiguously integrates the informatic and biological views of epidemics, producing an implosion between the immaterial and material, model and object, concept and entity. But the situation regarding sovereignty is also more complicated because of the network properties of DSNs and the epidemics they are designed to combat. In a sense, biosurveillance and DSNs are emblematic of the challenge facing many network forms of organization today – the challenge of the role of sovereignty within networks (or what Negri refers to as the 'political problem of the decision' in the multitude). To posit the need for network strategies to fight network threats is one thing, but it is quite another to place such strategies within governmental and institutional structures that are anything but distributed. The overarching goal of the DSNs becomes suddenly ensnared in the multiple agencies and interests involved in the network. This problem can already be witnessed in current US biodefense policies and practices. While no one will deny that bioterrorism does present a significant threat today, the DSNs that have been deployed and that are currently in development have raised a whole host of ethical and political issues: the confidentiality regarding a patient's medical records, the impact of biosurveillance on public health care systems (most notably health insurance), the question of mandated or voluntary reporting of medical data by physicians, and finally the concern of designing secure information networks dedicated to DSNs – this last issue being particularly interesting, since it posits a scenario in which a computer 'virus' may disable the capacity to stop a biological virus. [15]

38 When networks fight networks, the characteristic political response has been to rely upon the structure of sovereignty to intervene in and define the topology of the networks. The collection of information by Homeland Security officials is predicated on the sovereign 'state of exception,' and this same logic is being carried over into the information networks that underlie the various DSNs that are part of the US biosurveillance endeavor. We have, with DSNs, not just the use of new tools for the same old job, but rather the construction of exceptional topologies, in the sense of an ongoing 'state of exception,' preparedness, and readiness for a threat that is, by definition, immanent to the network itself. As an NEDSS fact sheet notes, 'the long-term vision of NEDSS is that of complementary electronic information systems that automatically gather health data from a variety of sources on a real-time basis; facilitate the monitoring of the health of communities; assist in the ongoing analysis of trends and detection of emerging public health problems; and provide information for setting public health policy' (NEDSS, 2000). The WHO's response to SARS is another exceptional topology, a hybrid of computers, communications, hospitals, health advisories, and what the US calls 'medical countermeasures' such as quarantine and travel restriction.

39 Again, in order to grasp what is at stake ontologically, it is important to resist a simple moral understanding of DSNs, as if the mere fact of surveillance in itself is a 'bad' thing, a sign of the further 'medicalisation' of society. The demonstrated success of the WHO's network makes such condemnations difficult. And yet, without a doubt, biosurveillance programs such as those in the US are in the process of casting the 'medical gaze' further than it has ever been cast before. This is why biosurveillance has to be regarded as a topological problem as well as a political problem. DSNs are caught between the recognition of the need to fight networks with networks, and the insistent need to establish sovereignty within the network. For this reason, we may see the situation of 'networks fighting networks' become the rule rather than the exception. In the condition of a normative state of exception, they may remain continually operative, but relatively invisible in terms of its effects. Until, of course, a threat is identified, at which time the network topology may undergo a sudden, even violent contraction (bioterror alerts, seizure of materials, detention of individuals, Haz-Mat inspections).

**Political Vitalism**

40 This sovereignty of 'exceptional topologies' – the mode of sovereignty specific to networks – is currently having a number of concrete effects in shaping US biosurveillance and biodefense policies. One is that there is no longer any strict division between 'naturally-occurring' infectious diseases and what the CDC calls 'intentional epidemics' (bioterrorism). In a sense, biosurveillance has surpassed even the most avant-garde cultural theory, disregarding the traditional divisions between nature and culture. If their causes are different, from the point of view of 'security,' their effects are the same. (And indeed one of the fearful aspects of bioterrorism is the unknown and indeterminate impact of an artificially-induced, or worse, genetically-engineered epidemic.) If epidemics and bioterrorism are, from the biopolitical perspective of 'security,' the same, then it follows that medical practice and health care systems will increasingly be called upon to participate in the concerns of national security and defense. This is not unique to biosurveillance programs today, however. The history of epidemiology, statistics, and demography reveals a long-standing, implicit collaboration between medicine and government (of which the idea of 'public health' is but one result). [16] Furthermore, military research programs in the US and other Western nations have, at least since World War II (and, arguably, after the first biological sabotage programs in World War I), made biology and medicine part of defense. [17] What is unique about contemporary biosurveillance is the unofficial and vague incorporation of medicine into national security. Such vagueness comes out in the concerns over the degree to which physicians, nurses, and health practitioners may in the future become obligated by law to report specific types of medical information.

41 A blurring of distinctions, then, is one effect of the ambiguousness regarding control versus emergence in biosurveillance. The 'complex' and 'emergent' properties of networks, be they biological or otherwise, serves as the rationale for a technically-sophisticated surveillance system that has, as its long-term goal, the total integration with federal and local healthcare infrastructures. Yet this immanence of biosurveillance has a flip-side, which is the language of 'threat', 'security,' and 'defense,' a language of networks fighting networks that necessitates exceptional measures to intervene in and shape networks. On the one hand, the DSNs will be invisible and immanent, part and parcel of medical practice and public health. On the other hand, that same DSNs may, in times of crisis or a state of emergency, become suddenly contracted and highly centralized. What this masks, of course, is the way in which the DSNs are always in a continual state of emergency. 'Preparedness' simply becomes actualized in 'emergency,' both of which are predicated on the sovereign exception acting within a network.

42 The challenge to epidemiology and public health, then, is to confront the paradoxical claim that 'networks are needed to fight networks.' In other words, the study of epidemics, and the application in biosurveillance and in DSNs, presents us with a situation in which the need for control is also, in some way, the need for an absence of control ('emergence,' 'self-organization,' and so forth). An approach that concentrates on eradicating the 'disease itself' through vaccination will only ever follow the epidemic. Thus, the search for the 'disease itself' will only result in finding the disease everywhere in general, but nowhere in particular. And yet, any attempt to design preventive systems inevitably implies the design of preemptive systems, and the acceptance of the ambiguous politics associated with the doctrine of preemption. In this regard, Agamben's (1998) comment that 'biopolitics necessarily turns into thanatopolitics' takes on a new meaning.

43 DSNs such as those of the WHO, the CDC's NEDSS, and Homeland Security's BioWatch system, are all examples of attempts to use networks to fight networks. In many cases, as we've seen, the strategy is to deploy a centralized information network to counteract the decentralized (or 'becoming-distributed') network of an epidemic. However, what often goes unrecognized is that the effectiveness of the WHO's network may not be due to the technical existence and deployment of information technologies, but to the degree to which the WHO's health advisories were carried out at local levels – that is, 'downstream' from the central node, at the sparsely-connected peripheries of the network. In many cities, including Singapore (where health 'kits' were made available to civilians), the transmission of knowledge about the contagion was key to preventing further epidemic spread. This depended not upon WHO or state officials, but, ultimately, on the more 'horizontal' interactions between local agencies (clinics, physicians, nurses, educators, volunteers). Again, the point is not to seek to idealize the inherently liberal principles of

decentralized or distributed networks, but to notice the following: the situation of 'networks fighting networks' puts forth a challenge to us to rethink traditional notions of 'control', 'decision,' and 'action,' or what these terms may mean in a given network-based context.

44 Can we imagine a situation in which both networks are decentralized, or even distributed? Would this be a desirable thing, or would it signal a greater fatality for our intention to manage and control an epidemic? It is not difficult to imagine a range of possible scenarios based on the current political climate. One is a scenario in which a real-time DSN is established on its own dedicated Internet, on which it runs automatically, without human intervention. This is, in a sense, the biomedical equivalent to the computerized command-and-control weapons systems of the Cold War. Despite the science fictional overtones, the automation of DSNs occupies a significant portion of the research, and at least one automated system – the RODS or Real-time Outbreak and Disease Surveillance system – was implemented at the 2002 Olympic Games in Utah. [18] Another imaginary scenario comes, interestingly enough, from computer science. In 2003, when the 'Blaster' virus made its way through the Internet, an attempt was made to design a software 'vaccine' to Blaster, or a 'good virus.' [19] Dubbed 'Naachi,' this 'good virus' would travel through the Internet, checking computers to see if they were vulnerable to the particular type of attack that the Blaster virus used. If a computer was found to be vulnerable, Naachi would automatically download a patch from the Microsoft website (Blaster only infected PCs running Windows). All this network activity would be happening in the background, with the computer user only half-aware of what was taking place. Unfortunately, due to excessive Internet traffic to and from the Microsoft website, Naachi caused more damage than it prevented, clogging several commercial airline and Navy computer systems. But it is not difficult to imagine the 'good virus' example carried over into biodefense. The prospect is harrowing: from a strictly network perspective, wouldn't the best network counter-offensive be a benign virus, one that would inhabit the very air we breathe, vaccinating us against a potential threat that we did not know existed? And, if the best way to fight networks is with networks, then wouldn't this necessitate a de-emphasis on human-centered action, and an increased emphasis on the 'vital' properties of the network in itself? In such an instance, would it still be possible to distinguish contagion from transmission?

### Author's Biography

Eugene Thacker is Assistant Professor in the School of Literature, Communication, and Culture at Georgia Tech. He has written extensively on the relationships between biology, informatics, and politics, and is the author of two books: Biomedia (University of Minnesota, 2004) and The Global Genome (MIT, 2005).

### Notes

[1] See Rosen, 1993, pp. 251-63.

[back]

[2] See Porter, 1997, 236-37.

[back]

[3] See Foucault, 2000, pp. 134-56.

[back]

[4] See Porter, 1997, pp. 412-14. Also see Snow's pamphlet On the Mode of Communication in Cholera, published during the 1849 outbreak in London.

[back]

[5] The SIR model measures the probability that a disease will become epidemic for a particular population. Individuals within a population are characterized a 'susceptible' (vulnerable to infection), 'infected' (capable of infecting others), or 'recovered' (either through acquired immunity, medical intervention, or possibly death). The threshold of epidemicity is when the overall transition from 'susceptible' to 'infected' is greater than the transition from 'infected' to 'removed.' For a description of the SIR model in epidemiology, see Watts, 2003, pp. 168-74.

[back]

[6] Information about these and other CDC-based surveillance projects can be obtained online at https://www.cdc.gov.

[back]

[7] See Miller et al., 2002, pp. 15-33, 151-54, 160-63.

[back]

[8] See Alibek and Handelman, 1999, and Miller et al., 2002, pp. 135-37.

[back]

[9] For more on the WHO's 'Global Outbreak Alert and Response Network' go to https://www.who.int.

[back]

[10] See the 2000 CDC report "Preventing Emerging Infectious Diseases: A Strategy for the 21st Century," available online at: https://www.cdc.gov/ncidod/emergplan/

[back]

[11] For an example, see Hoffman et al., 2003.

[back]

[12] However networks do not always fight other networks; in many cases the networks can be 'layered' on top of each other to produce an intensification, or a 'network affect.' In the case of the 2001 anthrax attacks in the US, for instance, a minimally-effective biological network was abetted by two 'layers' of information networks: that of the postal system, and that of the mass media. Through this network layering, the actual infection of a small number of individuals had the impact of an epidemic (indeed the threat posed by the anthrax attacks were the primary motive behind the US Bioterrorism Act). In this case, qualitatively different information networks were able to amplify the limited effect of a biological agent. In other words, the layering of different types of networks enabled an overall network amplification to occur.

[back]

[13] Thus, the most 'successful' epidemic is one that is virtual with respect to any actual node on the network.

[back]

[14] See Agamben, 1998, pp. 126-35.

[back]

[15] On these and other issues, see the special issue of JAMIA (Journal of the American Medical Informatics Association), 9.2 (2002), on "The Role of Informatics in Preparedness for Bioterrorism and Disaster."

[back]

[16] See Porter, 1997, pp. 397-427.

[back]

[17] See Harris and Paxman, 1982, and Miller et al. 2002, pp. 38-41.

[back]

[18] See Gesteland et al., 2003.

[back]

[19] For a brief summary, see the article "Attack of the World Wide Worms," Time (1 September 2003): 48-50.

[back]

**References**

Agamben, Giorgio. Homo Sacer: Sovereign Power and Bare Life, trans. Daniel Heller-Roazen (Stanford: Stanford University Press, 1998).

Alibek, Ken and Stephen Handelman. Biohazard (New York: Random House, 1999).

Arquilla, John, and David Ronfeldt, eds. Networks and Netwars: The Future of Terror, Crime, and Militancy (Santa Monica: RAND, 2001).

Barabási, Albert-László. Linked: The New Science of Networks (Cambridge: Perseus, 2002).

Barabási, Albert-László, and Zoltán Dezso. “Halting Viruses in Scale-Free Networks,” Physical Review E 65 (21 May 2002): 1-5.

Deleuze, Gilles. Foucault. Trans. Séan Hand. London: Continuum, 1999 [1986].

Forrest, Stephanie, Steven Hofmeyr, and Anil Somayaji. “Computer Immunology,” Communications of the ACM (21 March 1996).

Foucault, Michel. The Birth of the Clinic: An Archaeology of Medical Perception (New York: Vintage, 1973).

—-. Discipline and Punish: The Birth of the Prison (New York: Vintage, 1979).

—-. Power. The Essential Works of Michel Foucault 1954-1984, ed. James Faubion (New York: New Press, 2000).

Gesteland, P.H. et al. “Implementing Automated Syndromic Surveillance for the 2002 Winter Olympics.” JAMIA (Journal of the American Medical Informatics Association) 10.6 (Nov/Dec 2003): 547-554.

Hacking, Ian. “Bio-power and the Avalanche of Printed Numbers.” Humanities in Society 5 (1982): 279-95.

Harris, Robert, and Jeremy Paxman. A Higher Form of Killing: The Secret History of Biological and Chemical Warfare (New York: Hill & Wang, 1982).

Hoffman, Mark, et al. “Multijurisdictional Approach to Biosurveillance, Kansas City.” Emerging Infectious Disease 9.10 (October 2003): 1281-86.

Kephart, Jeffrey, David Chess, and Steve White. “Computer Viruses and Epidemiology,” IEEE Spectrum 30.5 (May 1993): 20-26.

Miller, Judith, Stephen Engelberg, and William Broad. Germs: Biological Weapons and America’s Secret War (New York: Touchstone, 2002).

NEDSS. “Supporting Public Health Surveillance through the National Electronic Disease Surveillance System (NEDSS),” fact sheet, 2000. Available from: https://www.cdc.gov/od/hissb/docs.htm#nedss.

Porter, Roy. The Greatest Benefit to Mankind: A Medical History of Humanity (New York: Norton, 1997).

Rosen, George. A History of Public Health (Baltimore: Johns Hopkins, 1993 [1958]).

Shannon, Claude, and Warren Weaver. The Mathematical Theory of Communication (Chicago: University of Illinois Press, 1965).

U.S. Department of Homeland Security. “President’s Budget Include $274 Million to Further Improve Nation’s Bio-Surveillance Capabilities,” press release (29 January 2004).

Watts, Duncan. Six Degrees: The Science of a Connected Age (New York: Norton, 2003).

White House, Office of the Press Secretary. “President Details Project BioShield,” press release (3 February 2003).

The Fibreculture Journal (ISSN 1449-1443) — Issue 4, 2005-11-02. This article is published under CC BY-NC-ND. The author retains copyright.

**This PDF is an archival offprint generated from the journal’s text archive** on 2026-11-15. It is not the publisher’s version of record; the published article is at https://four.fibreculturejournal.org/fcj-018-living-dead-networks/. Page numbers here are not the published pagination. Where paragraph numbers appear in the margin they are the journal’s own and are the citable unit.