

Chapter Two

Networks vs. Hierarchies

I. The Systematic Stupidity of Hierarchies

The intrusion of power into human relationships creates irrationality and systematic stupidity. As Robert Anton Wilson argued in “Thirteen Choruses for the Divine Marquis,”

A civilization based on authority-and-submission is a civilization without the means of self-correction. *Effective* communication flows only one way: from master-group to servile-group. Any cyberneticist knows that such a one-way communication channel lacks feedback and cannot behave "intelligently."

The epitome of authority-and-submission is the Army, and the control-and-communication network of the Army has every defect a cyberneticist's nightmare could conjure. Its typical patterns of behavior are immortalized in folklore as SNAFU (situation normal—all fucked-up)... In less extreme, but equally nosologic, form these are the typical conditions of any authoritarian group, be it a corporation, a nation, a family, or a whole civilization.¹

That same theme featured prominently in *The Illuminatus! Trilogy*, which Wilson coauthored with Robert Shea. “...[I]n a rigid hierarchy, nobody questions orders that seem to come from above, and those at the very top are so isolated from the actual work situation that they never see what is going on below.”²

A man with a gun is told only that which people assume will not provoke him to pull the trigger. Since all authority and government are based on force, the master class, with its burden of omniscience, faces the servile class, with its burden of nescience, precisely as a highwayman faces his victim. Communication is possible only between equals. The master class never abstracts enough information from the servile class to know what is actually going on in the world where the actual productivity of society occurs.... The result can only be progressive deterioration among the rulers.³

This inability of those in authority to abstract sufficient information from below, and this perception of superiors by subordinates as “a highwayman,” result in the hoarding of information by those below and their use of it as a source of rents. The power differential, by creating a zero-sum relationship, renders the pyramid opaque to those at its top.

Radical organization theorist Kenneth Boulding, in similar vein, noted “the way in which organizational structure affects the flow of information,”

hence affects the information input into the decision-maker, hence affects his image of the future and his decisions.... There is a great deal of evidence that almost all organizational structures tend to pro-

1 R. A. Wilson, “Thirteen Choruses for the Divine Marquis,” from *Coincidence – A Head Test* (1988) <<http://www.deepleafproductions.com/wilsonlibrary/texts/raw-marquis.html>>.

2 Robert Shea and Robert Anton Wilson, *The Illuminatus! Trilogy* (New York: Dell Publishing, 1975), p. 388.

3 *Ibid.*, p. 498.

duce false images in the decision-maker, and that the larger and more authoritarian the organization, the better the chance that its top decision-makers will be operating in purely imaginary worlds.⁴

In his discussion of *mētis* (i.e. distributed, situational, job-related knowledge), James C. Scott draws a connection between it and mutuality—“as opposed to imperative, hierarchical coordination”—and acknowledges his debt for the insight to anarchist thinkers like Kropotkin and Proudhon.⁵ *Mētis* requires two-way communication between equals, where those in contact with the situation—the people actually doing the work—are in a position of equality.

Interestingly, Wilson had previously noted this connection between mutuality and accurate information in “Thirteen Choruses.” He even included his own allusion to Proudhon:

[Proudhon's] system of voluntary association (anarchy) is based on the simple communication principles that an authoritarian system means one-way communication, or stupidity, and a libertarian system means two-way communication, or rationality.

The essence of authority, as he saw, was Law — that is..., effective communication running one way only. The essence of a libertarian system, as he also saw, was Contract — that is, mutual agreement — that is, effective communication running both ways.

To call a hierarchical organization systematically stupid is just to say that it's incapable of making effective use of the knowledge of its members; it is less than the sum of its parts. Clay Shirky quotes John Seely Brown and Paul Duguid:

“What if HP knew what HP knows?” They had observed that the sum of the individual minds at HP had much more information than the company had access to, even though it was allowed to direct the efforts of those employees.⁶

Because a hierarchical institution is unable to aggregate the intelligence of its members and bring it to bear effectively on the policy-making process, policies have unintended consequences, and different policies operate at cross-purposes with each other in unanticipated ways. And to top it all off, the transaction costs of getting information to management about the real-world consequences of its policies are prohibitive for the same reason that the transaction costs of aggregating the information required for effective policy-making in the first place were prohibitive.

But no worries. Because senior management don't live under the effects of their policy, and subordinates are afraid to tell them what a clusterfuck they created, the CEO will happily inform the CEOs at other organizations of how wonderfully his new “best practice” worked out. And because these “competing” organizations actually exist in an oligopoly market of cost-plus and administered pricing, and share the same pathological institutional cultures, they suffer no real competitive penalty for their bureaucratic irrationality.

A hierarchy is a device for telling naked emperors how great their clothes look. “Thoreau,” a professor of physics who for obvious reasons prefers to blog anonymously, describes it in the context of his interactions with an administrator:

Let's just say that there's something we do that is...sub-optimal. Everyone knows it is sub-optimal...

I observed that what we do is sub-optimal, and we shouldn't expand this, but she was basically pointing out that we routinely generate reports saying that it works. Yes, we do. Those reports involve pigs and lipstick. We all know this. However, she lives in a world that is based on those reports...⁷

4 Kenneth Boulding, “The Economics of Knowledge and the Knowledge of Economics,” *American Economic Review* 56:1/2 (March 1966), p. 8.

5 James Scott, *Seeing Like a State* (New Haven: Yale University Press, 1999), pp. 6-7.

6 Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (Penguin Books, 2008), p. 100.

7 Thoreau, “Going up against the pointy-haired bosses,” *Unqualified Offerings*, February 6, 2013 <<http://highclearing.com/index.php/archives/2013/02/06/15879>>.

When you constantly operate on the assumption that you're going to internalize the effects of your own actions, you have an incentive to anticipate things that could go wrong. And when you make a decision, you continually revise it in response to subsequent experience. Normally functioning human beings—that is, who are in contact with our environments and not insulated from them by hierarchies—are always correcting our own courses of action.

Authority short-circuits this process: it shifts the negative consequences of decisions downward and the benefits upward, so that decision-makers operate based on a distorted cost-benefit calculus; and it blocks negative feedback so that the locus of organizational authority is subject to the functional equivalent of a psychotic break with reality.

When policy *isn't* the result of systematic stupidity, it's an elaborate exercise in plausible deniability, so management can say “But they *knew* about our written policy,” when the inevitable shortcuts to compensate for deliberate understaffing and irrational interference result in a public relations disaster.

The lack of feedback means most organizations are “successful” at achieving goals that are largely artificial—goals defined primarily by the interests of their governing hierarchies, rather than by the ostensible customers or those engaged in directly serving customer needs. On the other hand, organizational structures like networks, which are based on two-way feedback between equals, result in a high rate of “failure.” As Clay Shirky puts it, open source is a threat because it outfails proprietary systems. It can experiment and fail at less cost. Because failure is more costly to a hierarchy, hierarchies are biased “in favor of predictable but substandard outcomes.”⁸

Failure also reflects the empowerment of workers and customers; most products in the corporate economy are only considered “good enough” because customers are powerless.

Chrystia Freeland argues the GOP establishment and its backers were so utterly convinced Obama would lose in 2012, and caught so badly off-guard by the actual outcome of the election, because of the very same kinds of information filtering and group think that prevail in the corporations they represented.

By his own definition, Romney's single strongest qualification to become president was analytically based, managerial excellence. And if the election campaign were the test of that, and even if you were ideologically his fan, you should think it right that he lost. Now, how could it happen? My first thought was it was also the case that all the smartest guys in the room managed to lose a lot of money in 2008 and managed to convince themselves of a set of very mistaken beliefs about where the markets were going to go. It was a lot of the same people on the wrong side of both bets....

...[W]hen you're a rich and powerful guy, it can make it hard to see reality, especially when you're paying your campaign staff great salaries, as Romney was.⁹

To repeat, no matter how intelligent the people staffing a large institution are as individuals, hierarchy makes their intelligence unusable. Given that the institution does not exist as a vehicle for the goals of its members, there's no intrinsic connection between their personal motivation and their roles in the organization, and the information and agency problems of a hierarchy prevent consequences from being fully internalized by actors, individuals simply cannot be trusted with the discretion to act on their own intelligence or common sense. That's the rationale for standardized work-rules, job descriptions, and all the rest of the Weberian model of bureaucratic rationality: because someone, somewhere might use her initiative in ways that produce results that are detrimental to the interests of the organization, you need a set of rules in place that prevent anyone from doing anything at all. Unlike networks, which treat the human brain as an asset, hierarchical rules systems treat it as a risk to be mitigated.

8 *Ibid.*, p. 245.

9 Ezra Klein, “Romney is Wall Street's worst bet since the bet on subprime,” *Washington Post* Wonkblog, November 28, 2013 <<http://www.washingtonpost.com/blogs/wonkblog/wp/2012/11/28/romney-is-wall-streets-worst-bet-since-the-bet-on-subprime/>>.

Job descriptions and union work rules are the other side of the coin to Weberian/Taylorist work rules. Both result from hierarchy. Power, by definition, creates zero-sum relationships. Superiors attempt to externalize effort on subordinates and skim off the benefits of increased productivity for themselves; subordinates, as a result, attempt to minimize the expenditure of effort and do the minimum necessary to avoid getting fired. Both superiors and subordinates filter or hoard information of benefit to the other party, and attempt to maximize the rents from keeping each other ignorant. In this zero-sum relation, where each side can only benefit at the expense of the other, each party seeks mechanisms for limiting abuses by the other.

Paul Goodman illustrated the need to impose constraints on freedom of action, and impede individual initiative in directly adopting the most common-sense and lowest-cost solutions to immediate problems, with the example of replacing a door catch in the New York public school system:

...To remove a door catch that hampers the use of a lavatory requires a long appeal through headquarters, because it is "city property."....

...An old-fashioned type of hardware is specified for all new buildings, that is kept in production only for the New York school system.¹⁰

When the social means are tied up in such complicated organizations, it becomes extraordinarily difficult and sometimes impossible to do a simple thing directly, even though the doing is common sense and would meet with universal approval, as when neither the child, nor the parent, nor the janitor, nor the principal of the school can remove the offending door catch.¹¹

A corporate hierarchy interferes with the judgment of what Friedrich Hayek called "people-on-the-spot," and with the collection of dispersed knowledge of circumstances, in exactly the same way a state does.

Most production jobs involve a fair amount of distributed, job-specific knowledge, and depend on the initiative of workers to improvise, to apply skills in new ways, in the face of events which are either totally unpredictable or cannot be fully anticipated. Rigid hierarchies and rigid work rules only work in a predictable environment. When the environment is unpredictable, the key to success lies with empowerment and autonomy for those in direct contact with the situation.

Hierarchical organizations are—to borrow a wonderful phrase from Martha Feldman and James March—*systematically* stupid.¹² For all the same Hayekian reasons that make a planned economy unsustainable, *no* individual is "smart" enough to manage a large, hierarchical organization. *Nobody*—not Einstein, not John Galt—possesses the qualities to make a bureaucratic hierarchy function rationally. Nobody's that smart, any more than anybody's smart enough to run Gosplan efficiently—that's the whole point. As Matt Yglesias put it,

I think it's noteworthy that the business class, as a set, has a curious and somewhat incoherent view of capitalism and why it's a good thing. Indeed, it's in most respects a backwards view that strongly contrasts with the economic or political science take on why markets work.

The basic business outlook is very focused on the key role of the *executive*. Good, profitable, growing firms are run by brilliant executives. And the ability of the firm to grow and be profitable is evidence of its executives' brilliance. This is part of the reason that CEO salaries need to keep escalating—recruiting the best is integral to success. The leaders of large firms become revered figures.... Their success stems from overall brilliance....

The thing about this is that if this were generally true—if the CEOs of the Fortune 500 were brilliant economic seers—then it would really make a lot of sense to implement socialism. Real socialism. Not

10 Paul Goodman, *People or Personnel*, in *People or Personnel and Like a Conquered Province* (New York: Vintage Books, 1964, 1966), p. 52.

11 *Ibid.* p. 88.

12 Martha S. Feldman and James G. March, "Information in Organizations as Signal and Symbol," *Administrative Science Quarterly* 26 (April 1981); it should be noted, in fairness, that Feldman and March were attempting—unsuccessfully in my opinion—to defend corporations *against* the charge of systematic stupidity.

progressive taxation to finance a mildly redistributive welfare state. But “let’s let Vikram Pandit and Jeff Immelt centrally plan the economy—after all, they’re really brilliant!”

But in the real world, the point of markets isn’t that executives are clever and bureaucrats are dimwitted. The point is that *nobody* is all that brilliant.¹³

No matter how intelligent managers are *as individuals*, a bureaucratic hierarchy insulates those at the top from the reality of what’s going on below, and makes their intelligence less *usable*. Chris Dillow describes it this way:

But why don’t firms improve with practice in the way that individuals’ musical or sporting performance improves? Here are four possible differences:

1. Within firms, there’s no mechanism for translating individuals’ learning, or incremental knowledge, into corporate knowledge. As Hayek said, hierarchies are terrible at using fragmentary, tacit, dispersed knowledge.
2. Job turnover means that job-specific human capital gets lost.
3. Bosses are selected for overconfidence. But overconfidence militates against learning.
4. In companies, the feedback that’s necessary for improvement gets warped by adverse incentives or ego involvement. If I play a phrase or chord badly, my ears tell me to practice it more. But if a company gets some adverse feedback—falling sales, say—no-one has an incentive or desire to say “I screwed up: I’d better improve.” And formal efforts to generate feedback, such as performance reviews, often backfire.

What I’m saying is what every methodological individualist knows: companies are not individuals writ large. The differences between them can mitigate against learning by doing.¹⁴

As an institution becomes larger and experiences increased overhead and bureaucratic ossification, it simultaneously becomes more and more vulnerable to fluctuating conditions in its surrounding environment, and less able to react to them. To survive, therefore, the large institution must control its surrounding environment.

The only real solution to complexity and unpredictability, as security analyst Bruce Schneier argues, is to give discretion to those in direct contact with the situation.

Good security has people in charge. People are resilient. People can improvise. People can be creative. People can develop on-the-spot solutions.... People are the strongest point in a security process. When a security system succeeds in the face of a new or coordinated or devastating attack, it’s usually due to the efforts of people.¹⁵

The problem with authority relations in a hierarchy is that, given the conflict of interest created by the presence of power, those in authority cannot *afford* to allow discretion to those in direct contact with the situation. Systematic stupidity results, of necessity, from a situation in which a bureaucratic hierarchy must develop arbitrary metrics for assessing the skills or work quality of a labor force whose actual work they know nothing about, and whose material interests militate against remedying management’s ignorance.

Most of the constantly rising burden of paperwork exists to give an illusion of transparency and control to a bureaucracy that is out of touch with the actual production process. Every new layer of paperwork is added to address the perceived problem that stuff still isn’t getting done the way management wants, despite the proliferation of paperwork saying everything has been done exactly according to orders. In a hierarchy, managers are forced to regulate a process which is necessarily opaque to them because they are not directly

13 Matthew Yglesias, “Two Views of Capitalism,” *Yglesias*, November 22, 2008 <http://yglesias.thinkprogress.org/2008/11/two_views_of_capitalism/>.

14 Chris Dillow, “Organizational Stupidity,” *Stumbling and Mumbling*, September 23, 2011

<http://stumblingandmumbling.typepad.com/stumbling_and_mumbling/2011/09/organizational-stupidity.html>.

15 Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York: Copernicus Books, 2003), p. 133.

engaged in it. They're forced to carry out the impossible task of developing accurate metrics to evaluate the behavior of subordinates, based on the self-reporting of people with whom they have a fundamental conflict of interest. The paperwork burden that management imposes on workers reflects an attempt to render legible a set of social relationships that by its nature must be opaque and closed to them, because they are outside of it.

Each new form is intended to remedy the heretofore imperfect self-reporting of subordinates. The need for new paperwork is predicated on the assumption that compliance must be verified because those being monitored have a fundamental conflict of interest with those making the policy, and hence cannot be trusted; but at the same time, the paperwork itself relies on their self-reporting as the main source of information. Every time new evidence is presented that this or that task isn't being performed to management's satisfaction, or this or that policy isn't being followed, despite the existing reams of paperwork, management's response is to design yet another—and equally useless—form.

Weberian work rules result of necessity when performance and quality metrics are not tied to direct feedback from the work process itself. They're a metric *of work for* someone who is neither a creator/provider nor an end user. And they are necessary—again—because those at the top cannot afford to allow those at the bottom the discretion to use their own common sense. A bureaucracy can't afford to allow its subordinates such discretion, because someone with the discretion to do things more efficiently will also have the discretion to do something bad. And because the subordinate has a fundamental conflict of interest with the superior, and does not internalize the benefits of applying her intelligence, she can't be trusted to use her intelligence for the benefit of the organization. In such a zero-sum relationship, any discretion can be abused.

The problem is, discretion cannot be entirely removed from any organizational process. James Scott writes that it's impossible, by the nature of things, for everything entailed in the production process to be distilled, formalized or codified into a form that's legible to management.

...[T]he formal order encoded in social-engineering designs inevitably leaves out elements that are essential to their actual functioning. If the [East German] factory were forced to operate only within the confines of the roles and functions specified in the simplified design, it would quickly grind to a halt. Collectivized command economies virtually everywhere have limped along thanks to the often desperate improvisation of an informal economy wholly outside its schemata.

Stated somewhat differently, all socially engineered systems of formal order are in fact subsystems of a larger system on which they are ultimately dependent, not to say parasitic. The subsystem relies on a variety of processes—frequently informal or antecedent—which alone it cannot create or maintain. The more schematic, thin, and simplified the formal order, the less resilient and the more vulnerable it is to disturbances outside its narrow parameters....

It is, I think, a characteristic of large, formal systems of coordination that they are accompanied by what appear to be anomalies but on closer inspection turn out to be integral to that formal order. Much of this might be called “*mētis* to the rescue....” A formal command economy... is contingent on petty trade, bartering, and deals that are typically illegal.... In each case, the nonconforming practice is an indispensable condition for formal order.¹⁶

...In each case, the necessarily thin, schematic model of social organization and production animating the planning was inadequate as a set of instructions for creating a successful social order. By themselves, the simplified rules can never generate a functioning community, city, or economy. Formal order, to be more explicit, is always and to some considerable degree parasitic on informal processes, which the formal scheme does not recognize, without which it could not exist, and which it alone cannot create or maintain.¹⁷

And as I keep trying to hammer home, just the reverse is true of networks and stigmergic organization: their beauty is that they render the intelligence of all their individual members *more* usable. While one-way

16 James Scott, *Seeing Like a State*, pp. 351-352.

17 *Ibid.*, p. 310.

communication creates opacity from above, two-way communication creates horizontal legibility. To quote Michel Bauwens:

The capacity to cooperate is verified in the process of cooperation itself. Thus, projects are open to all comers provided they have the necessary skills to contribute to a project. These skills are verified, and communally validated, in the process of production itself. This is apparent in open publishing projects such as citizen journalism: anyone can post and anyone can verify the veracity of the articles. Reputation systems are used for communal validation. The filtering is a posteriori, not a priori. Anti-credentialism is therefore to be contrasted to traditional peer review, where credentials are an essential prerequisite to participate.

P2P projects are characterized by holoptism. Holoptism is the implied capacity and design of peer to [peer] processes that allows participants free access to all the information about the other participants; not in terms of privacy, but in terms of their existence and contributions (i.e. horizontal information) and access to the aims, metrics and documentation of the project as a whole (i.e. the vertical dimension). This can be contrasted to the panoptism which is characteristic of hierarchical projects: processes are designed to reserve 'total' knowledge for an elite, while participants only have access on a 'need to know' basis. However, with P2P projects, communication is not top-down and based on strictly defined reporting rules, but feedback is systemic, integrated in the protocol of the cooperative system.¹⁸

In a prison—governed by panopticism—the warden can see all the prisoners, but the prisoners can't see each other. The reason is so the prisoners can't coordinate their actions independently of the warden. Holopticism is the exact opposite: the members of a group are horizontally legible to one another, and can coordinate their actions. And “everyone has a sense of the emerging whole, and can adjust their actions for the greatest fit.”¹⁹

The unspoken assumption is that a hierarchy exists for the purposes of the management, and a holoptic association exists for the purposes of its members. The people at the top of a hierarchical pyramid can't trust the people doing the job because their interests are diametrically opposed. It's safe to trust one another in a horizontal organization because a common interest in the task can be inferred from participation.

II. Hierarchies vs. Networks

In a distributed network, it's impossible to prevent communication between nodes by controlling a central node. There are too many alternative nodes through which communication can be routed if any particular node or nodes are closed off. As John Gilmore famously quipped, “the Internet treats censorship as damage and routes around it.”²⁰

The power of distributed networks lies in the fact that in them filters disappear: eliminating or filtering a node or node cluster will not delay access to information. By contrast with the decentralised information system which arose with the invention of the telegraph, in distributed networks it is impossible to “burn bridges” and restrict the information that reaches the final nodes by controlling a few transmitters.²¹

As Ori Brafman and Rod Backstrom describe it, “*when attacked, a decentralized organization tends to become even more open and decentralized.*”²² They use the example of the file-sharing movement. After

18 Michel Bauwens, “The Political Economy of Peer Production,” *Ctheory.net*, December 1, 2005 <<http://www.ctheory.net/articles.aspx?id=499>>.

19 Alan Rosenblith, “Holopticism” (accessed January 22, 2012) <<http://www.slideshare.net/AlanRosenblith/holopticism>>.

20 Philip Elmer-DeWitt, “First Nation in Cyberspace,” *Time*, December 6, 1993 <<http://www.toad.com/gnu/>>.

21 Shirky, *Here Comes Everybody*, p. 43.

22 Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (Portfolio, 2006), p. 21.

Napster was shut down, the movement responded by creating a series of successors—each of which was even more decentralized and presented even less in the way of vulnerable nodes than its predecessor.²³

That's the subject of Francesca Musiani's article on the history of p2p file-sharing architecture, which she argues has been shaped by the offensive-defensive arms race between the forces of state surveillance and those of circumvention.²⁴ The first generation of file-sharing services, typified by Napster, were centralized, one-to-many systems. Subsequent services became increasingly decentralized—although their weak point remained imperfect anonymity. The third stage, Musiani argues, is file-sharing under cover of darknets, with membership by invitation only on a “friend-of-a-friend” basis. Although such organization through conventional, proprietary social networking services like Facebook is still vulnerable to the vagaries of their privacy policy, open-source social networking services like Diaspora are much more promising as avenues for darknet file-sharing.²⁵

“The Pirate Bay,” Rick Falkvinge writes, “has been a trailblazer in *resilience*. After all, a number of bought-and-paid-for or just plain misguided legislatures and courts have tried to eradicate the site, and yet, it still stands untouched.”²⁶ One source of its resilience—as is the case with Wikileaks (see below)—is its lack of dependence on servers that are vulnerable to the laws of any particular country. Like Wikileaks, The Pirate Bay has access to a network of servers in a number of countries; and it responds to shutdown attempts by nimbly switching its Web-hosting to servers in other countries (most recently the servers of the Norwegian and Catalan Pirate Parties as of this writing).²⁷

The ultimate step so far for file-sharing operations has been to bypass site-hosting as a bottleneck altogether and move into the cloud. The Pirate Bay released its software code so that it could be replicated by anyone who wanted to host a Pirate Bay clone.

Earlier this year [2012], after months of legal wrangling, authorities in a number of countries won an injunction against the Pirate Bay, probably the largest and most famous BitTorrent piracy site on the Web. The order blocked people from entering the site.

In retaliation, the Pirate Bay wrapped up the code that runs its entire Web site, and offered it as a free downloadable file for anyone to copy and install on their own servers. People began setting up hundreds of new versions of the site, and the piracy continues unabated.

Thus, whacking one big mole created hundreds of smaller ones.²⁸

And Tribler moves file-sharing in a literal peer-to-peer direction.

The new software called “*Tribler*” is the new weapon in the battle for Internet liberty and does not need a website to track users sharing torrent files.

According to The Raw Story, it is a “*peer-to-peer network protocol that enables computers to share files with thousands of others.*”

For many this could be the solution movie...

While lawmakers are dreaming of a censored web, many believe Tribler will be a true nightmare for them.

23 *Ibid.*, pp. 22-25.

24 Francesca Musiani, “Privacy as Invisibility: Pervasive Surveillance and the Privatisation of Peer-to-Peer Systems,” *tripleC* 9:2 (2011), p. 127.

25 *Ibid.*, pp. 132-138.

26 Rick Falkvinge, “The Pirate Bay is a Trailblazer in Technical Resilience,” *Falkvinge on Infopolicy*, March 23, 2013 <<http://falkvinge.net/2013/03/23/the-pirate-bay-is-a-trailblazer-in-technical-resilience/>>.

27 Falkvinge, “The Hydra Bay: The Pirate Bay Moves to Norwegian, Catalan Pirate Parties,” *Falkvinge on Infopolicy*, February 26, 2013 <<http://falkvinge.net/2013/02/26/the-hydra-bay-the-pirate-bay-moves-to-norwegian-catalan-pirate-parties/>>.

28 Michel Bauwens, “The escalation of the piracy wars when sharing culture moves to the cloud,” *P2P Foundation Blog*, August 23, 2012 <<http://blog.p2pfoundation.net/the-escalation-of-the-piracy-wars-when-sharing-culture-moves-to-the-cloud/2012/08/23>>.

According to the technology blog Torrent Freak, the attempt to disconnect users from the Internet for “illegal” purposes will be foiled by the software that has been in the works for the past five years and will make it nearly “impossible” to stop file sharing.

“The only way to take it down is to take the Internet down,” stated Doctor Pouwelse of Delft University of Technology to the Daily Mail.

Tribler will be entirely decentralized, leaving the control in the hands of the users.

“Individuals can rename files, flag phony downloads or viruses, create ‘channels’ of verified downloads, and act as nodes that distribute lists of peers across the network,” The Raw Story reported.²⁹

More recently, the clumsy attempts of the U.S. government and its allies to suppress Wikileaks through control of strategic nodes (domain name registries, Amazon, PayPal, etc.) have made the same principle abundantly clear. Wikileaks' enemies have strategized against it within the paradigm of a Weberian bureaucratic institution functioning inside a Westphalian nation-state. Will Wilkinson mocked the sheer idiocy of people like Joe Lieberman—and all the clucking chickenhawks in the neocon blogosphere calling for Chelsea Manning or Julian Assange to be waterboarded—in his blog at *The Economist*:

If Mr Assange is murdered tomorrow, if WikiLeaks' servers are cut off for a few hours, or a few days, or forever, nothing fundamental is really changed. With or without WikiLeaks, the technology exists to allow whistleblowers to leak data and documents while maintaining anonymity. With or without WikiLeaks, the personnel, technical know-how, and ideological will exists to enable anonymous leaking and to make this information available to the public....

Yet the debate over WikiLeaks has proceeded as if the matter might conclude with the eradication of these kinds of data dumps—as if this is a temporary glitch in the system that can be fixed.... But I don't think the matter can end this way. Just as technology has made it easier for governments and corporations to snoop ever more invasively into the private lives of individuals, it has also made it easier for individuals, working alone or together, to root through and make off with the secret files of governments and corporations. WikiLeaks is simply an early manifestation of what I predict will be a more-or-less permanent feature of contemporary life, and a more-or-less permanent constraint on strategies of secret-keeping.

Consider what young Bradley Manning is alleged to have accomplished with a USB key on a military network. It was impossible 30 years ago to just waltz out of an office building with hundreds of thousands of sensitive files. The mountain of boxes would have weighed tons. Today, there are millions upon millions of government and corporate employees capable of downloading massive amounts of data onto tiny devices. The only way WikiLeaks-like exposés will stop is if those with the permissions necessary to access and copy sensitive data refuse to do so. But as long as some of those people retain a sense of right and wrong—even if it is only a tiny minority—these leaks and these scandals will continue.³⁰

Mike Masnick, in similar language, expressed his amused contempt for calls from people like Christian Whiton and Marc Thiessen to kill Assange or declare war on Wikileaks and shut it down:

....As was pointed out at the time, this is a statement totally clueless about the nature of Wikileaks, and how distributed it is. If you shut down one node, five more would likely pop up overnight, and they'd be harder to track and harder to shut down. Whiton and Thiessen are reacting to Wikileaks as if it were a threat from an individual or a government. In other words, they're treating it like a threat from decades ago, rather than an open effort to distribute leaked information....

....What the internet allows is for groups to form and do stuff in a totally anonymous and distributed manner, and there really isn't any way to prevent that—whether you agree with the activity or not.³¹

29 “Internet pirates winning the war on SOPA with 'Tribler,’” rt.com, February 9, 2012 <<http://rt.com/usa/internet-war-new-tribler-941/>>.

30 Will Wilkinson, “Missing the Point of Wikileaks,” *Democracy in America (The Economist)*, December 1, 2010 <http://www.economist.com/blogs/democracyinamerica/2010/12/after_secrets>.

31 Mike Masnick, “The Revolution Will Be Distributed: Wikileaks, Anonymous, and How Little the Old Guard Realizes

As *Reason's* Jesse Walker put it,

I remember when the record companies were filled with men and women who thought the key to stopping online filesharing was to shut down a company called Napster. I remember when a teenaged programmer named Shawn Fanning was attracting the sort of press that Julian Assange is getting today. In 2010, the average 14-year-old probably doesn't know who Fanning is. He might not even recognize the name Napster. But he knows how to download music for free.³²

The resilience of Wikileaks against attempts at suppression by the corporate state, in particular, is remarkable. The networked movement to blog and tweet Wikileaks' dotted-line IP addresses around the Web, and to mirror the site by the thousands, should be a source of pride to all friends of information freedom. It reminds me of the DeCSS uprising, in which the “illegal” DeCSS hack for movie DRM was distributed at thousands of blogs and websites worldwide, and sympathizers even showed up for Eric Corley's trial in T-shirts bearing the DeCSS code. And even if the site were entirely shut down it would be feasible to move beyond the current website-based model and simply distribute content worldwide by torrent download.

Similarly, the Egyptian government's so-called shutdown of the Internet during the early 2011 uprising was circumvented by (inter alia) using dialup connections and virtual private networks. As with Wikileaks, social media sites were reportedly still available at their IP addresses. And use of the Tor anonymizer tripled.³³

What's more, another lesson of the shutdown is just how catastrophic the economic consequences are.

A central unknown at this moment is what the economic harm to the country will be. Without internet and voice networks, Egyptians are losing transactions and deals, their stocks and commodities cannot be traded, their goods are halted on frozen transportation networks, and their bank deposits are beyond reach.³⁴

In fact the measure seems so drastic, and the effects so severe, that governments are likely to treat them as a last resort and put them off until it's too late—as was the case in Egypt. Governments are as prone to the Boiled Frog Syndrome as we are.

Attempts to suppress efforts like Wikileaks by interdicting their access to centralized intermediaries like domain name services, web hosts, PayPal, etc., simply serve as a catalyst to create new, decentralized versions of those intermediaries which are less vulnerable to interdiction. There's already been talk about setting up an open-source domain name service by one of the founders of The Pirate Bay. Even before Wikileaks emerged as a major story, services like PayPal had come under criticism from the open source community for their lack of accountability to the user community, and sparked assorted attempts to create an open-source alternative. Attacks on Wikileaks have just increased the momentum behind such movements to reduce the vulnerability of centralized intermediaries.³⁵ The users' power of voice over PayPal is virtually nil, but their power of exit is potentially enormous. Again, the Net is in the process of treating censorship as damage and routing around it.

What's Going On,” *Techdirt*, October 26, 2010 <<http://www.techdirt.com/articles/20101026/01311411586/the-revolution-will-be-distributed-wikileaks-anonymous-and-how-little-the-old-guard-realizes-what-s-going-on.shtml>>.

32 Jesse Walker, “Our Leaky World,” *Reason.com*, December 15, 2010 <<http://reason.com/archives/2010/12/15/our-leaky-world#commentcontainer>>.

33 Klint Finley, “Egypt: Tor use Skyrocketing as Users Route Around Internet Blocks,” *ReadWrite*, January 28, 2011 <<http://www.readwriteweb.com/hack/2011/01/egypt-tor-use-skyrocketing-as.php>>. See also “20 Ways to Circumvent the Egyptian Government's Internet Block,” *Pastebin*, January 29, 2011 <<http://pastebin.com/9jJUku77>>.

34 *Ibid*.

35 Mike Masnick, “How Wikileaks and Operation Payback Have Exposed Infrastructure That Should Be Decentralized But Isn't,” *Techdirt*, December 16, 2010 <<http://www.techdirt.com/articles/20101215/02391012281/how-wikileaks-operation-payback-have-exposed-infrastructure-that-should-be-decentralized-isnt.shtml>>.

Projects to harden the Net against shutdown. Even before the Egyptian government shut down the Internet during the “Twitter Revolution” in early 2011, there was a wide range of projects aimed at increasing the Internet’s resilience in the face of state attempts at shutdown or control. The Egyptian government’s shutdown, combined with talk in the U.S. of an “Internet kill switch,” added a sense of urgency to these projects.

It’s worth bearing in mind, of course, that the resistance movement has been quite creative in circumventing the so-called Net “shutdown” while it was actually going on.

Even shutting down the Internet, which the security services in Syria, Libya, and Egypt all tried at various stages of those uprisings, cannot prevent determined cyber-dissidents from organizing. In Libya, rebels used satellite telephones to upload videos of violence by Qaddafi’s government against protesters. In Egypt, software developers managed to cobble together an alternative Internet—a peer-to-peer network that bypassed the state-controlled one—when the regime began blocking access. And from China to Belarus to Cuba, dissidents have used updated versions of time-tested samizdat methods developed to smuggle prodemocracy writings out from behind the Iron Curtain, downloading videos, images, and text onto tiny USB flash drives and mailing them or smuggling them abroad. Syrians smuggle USB drives across the northern border to Turkey and, thanks to robust connections with relatively free Lebanon, kept a steady flow of images and information streaming into cyberspace even through the darkest moments of the Assad regime’s crackdown. With the U.S. government and other public and private entities funding research into ways of keeping such dissidents just ahead of the censors, the information “arms race” between regimes and their subjects so far appears to give a lopsided advantage to the people.³⁶

Telecomix, a group of European online freedom activists, is a good example. It offered technical support to Egyptian protestors:

Egyptians with dial-up modems get no Internet connection when they call into their local ISP, but calling an international number to reach a modem in another country gives them a connection to the outside world....

The few Egyptians able to access the Internet through Noor, the one functioning ISP, are taking steps to ensure their online activities are not being logged. Shortly before Internet access was cut off, the Tor Project said it saw a big spike in Egyptian visitors looking to download its Web browsing software, which is designed to let people surf the Web anonymously.³⁷

And now many Egyptians are finding ways around the cuts and getting back on the Internet, allowing them to more easily communicate with the outside world and spread information from the inside. One popular method is to use the local phone lines, which remain intact. The trick is to bypass local Egyptian ISPs (Internet Service Providers) by connecting to remote ones hosted in outside countries -- many are hosted here in the United States; Los Angeles seems, for whatever reason, to be a popular site.³⁸

Telecomix has also provided a package for bypassing state Internet surveillance and censorship in Syria, which it put together on a number of mirrored websites, and then circulated links to them by email spam:

It took about one month to design, write, discuss, erase, rewrite, correct and finally package the software. Many people gave their advice either on the design, on the technical content or on how the mes-

36 Michael Moran, “From Shortwaves to Flash Mobs,” *Salon*, April 10, 2012 <http://www.slate.com/articles/news_and_politics/foreigners/2012/04/revolutionary_technology_facebook_twitter_and_wikileaks_pose_a_challenge_to_governments_everywhere_.html>.

37 Nancy Gohring and Robert McMillan, “Without Internet, Egyptians find new ways to get online,” *Computerworld*, January 28, 2011 <http://www.computerworld.com/s/article/9207078/Without_Internet_Egyptians_find_new_ways_to_get_online>.

38 Nicholas Jackson, “Despite Severed Connections, Egyptians Get Back Online,” *The Atlantic*, January 29, 2011 <<http://www.theatlantic.com/technology/archive/2011/01/despite-severed-connections-egyptians-get-back-online/70479/>>.

sage would be welcomed on the Syrian side. One of our Syrian contacts put his heart and guts to provide us a perfectly polished Arabic translation. At this point, the 60MB Telecomix Safety Pack website was ready. It contained security Firefox plugins, a Tor bundle, secure instant messaging software, a link to the Telecomix chat and more. It also emphasized basic guidelines such as avoid revealing personal information over the Internet....

19 mirrors, all using different domain names, managed by 2 load balancers. Not that huge, but hopefully robust enough to both reply to all requests and circumvent a potential blocking against some domain names. Webservers specially installed and configured for this aggressive broadcast. The crossing point between high technical skills, deep emotional involvement and decentralized technological power.

I « pushed the button » on the 5th of September at 1:53am CEST. Then came the anxious monitoring of our respective servers.

Thousands of requests were scrolling on the screen, several megabytes per second were passing through the main mirrors. All servers kept responding bravely to all these requests during the operation time.

Fucking hell yeah. It was working. Cheers, champaign!³⁹

Another project, originally designed for maintaining connectivity in large-scale disasters like Katrina or the Haitian earthquake but also ideal in a case like Mubarak's Internet shutdown, was Tethr: an easily portable, concealable, solar-powered device with a satellite Internet modem and Wifi connectivity.⁴⁰

One open Net project, the Chokepoint Project, states its mission as “To identify chokepoints, understand the issues behind who owns what and has the power to turn off connections or control aspects of internet control like domain names.”⁴¹

During the recent uprising in Egypt, in January 2011, the order was given to “turn off” the Internet, sending shock-waves around the world. Murmurs were heard of US security agencies and American politicians asking for access to a similar kill switch. These actions force us to look at who owns The Internet? This is where the Choke Point Project comes in mapping the nodes of control in service of the multitude of global citizens under who authoritarian regimes can act upon without their consent. We are in favor of exploring approaches to the decentralization of access in favor of guaranteeing connectivity as a counter-weight to the control of the Internet by nation states and corporate influence. A team comprised of web researchers, software developers and data visualization experts aim to gather data from across the web and show the control points, while clearly explaining the issues involved: history of Internet control, current legal situation, choke points, possible strategies for decentralization, reasons for and against kill switches.

We are confident to succeed with this project, through the interconnected network of designers and hackers available through the communities of ContactCon (a major conference focused on an independent Internet which will be held October 20th, 2011 in New York, convened by Douglas Rushkoff) and members of the P2P Foundation community.⁴²

The object of this research is to develop an Internet architecture that is not vulnerable to shutdown. The umbrella term for projects to develop such an architecture is “NextNet.”⁴³ The term was coined by David Rushkoff.⁴⁴

In July 2012 the project reported on its progress to date:

39 KheOps, “When the Internet does not let citizens down,” *Reflets*, September 11, 2011 <<http://reflets.info/opsyria-when-the-internet-does-not-let-citizens-down/>>.

40 “A Simple Box That Can Bring the Internet Anywhere,” *Co.Exist*, November 28, 2012 <<http://www.fastcoexist.com/1680932/a-simple-box-that-can-bring-the-internet-anywhere/>>; Venessa Miemis, “Contact Spotlight Series: Builders of the Next Net,” *Emergent by Design*, June 8, 2011 <<http://emergentbydesign.com/2011/06/18/contact-spotlight-series-builders-of-the-next-net/>>.

41 <<http://chokepointproject.net/>>.

42 “The Project,” *Choke Point Project* <<http://chokepointproject.net/the-project/>>.

43 <<http://p2pfoundation.net/NextNet/>>.

44 David Rushkoff, “The Next Net,” *Reality Sandwich*, February 17, 2011 <http://www.realitysandwich.com/next_net/>.

- Hosting is now set up and data is being processed ready for the forthcoming beta launch of what we are calling the (dis)Connection State Map...
- Ongoing mapping and interface improvements are being added.
- The new website is practically ready to roll and we are starting work on a public wiki as well.
- Strategic partnerships with relevant organisations are coming along and we've had many meetings with interested parties.
- Simon, Ruben & Gustaf were in Rio for RightsCon, the related hackathon and the Freebird "pre-event".
- Data sources have been investigated.
- And we're lucky to have a whole new bunch of very capable people from various disciplines onboard.⁴⁵

Most visions of such a distributed, decentralized Internet architecture involve meshworks of various kinds, in which "there is actually a physical 'many to many' distribution of hardware itself."⁴⁶ As Rushkoff describes the advantages:

Back in 1984, long before the Internet even existed, many of us who wanted to network with our computers used something called FidoNet. It was a super simple way of having a network—albeit an asynchronous one.

One kid... would let his computer be used as a "server." This just meant his parents let him have his own phone line for the modem. The rest of us would call in from our computers (one at a time, of course) upload the stuff we wanted to share and download any email that had arrived for us. Once or twice a night, the server would call some other servers in the network and see if any email had arrived for anyone with an account on his machine. Super simple.

Now FidoNet employed a genuinely distributed architecture.... 25 years of networking later, lessons learned, and battles fought; can you imagine how much better we could do?⁴⁷

The existing Internet architecture still has a considerable hub-and-spoke physical architecture, given its dependence on web-servers and routers. Meshworks overcome this limitation:

Meshies believe that mesh networks will overthrow traditional networking and communications and create entirely new kinds of distributed software. For the purposes of this column, mesh networks (sometimes called mobile ad hoc networks, or MANETs) are local-area networks whose nodes communicate directly with each other through wireless connections. It is the lack of a hub-and-spoke structure that distinguishes a mesh network. Meshes do not need designated routers: instead, nodes serve as routers for each other. Thus, data packets are forwarded from node to node in a process that network technologists term "hopping."

Before dismissing mesh networks as being of interest only to specialists, consider their advantages over existing hub-and-spoke networks. Mesh networks are self-healing: if any node fails, another will take its place. They are anonymous: nodes can come and go as they will. They are pervasive: a mobile node rarely encounters dead spots, because other nodes route around objects that hinder communication.⁴⁸

In a typical Wi-Fi network, there's one router and a relatively small number of devices using it as a gateway to the internet. In a mesh network, every device is also a router. Bring in a new mesh device

45 "What's Cooking in the CPP kitchen (and a request for help)," Chokepoint Project, June 30, 2012 <<http://chokepointproject.net/2012/06/whats-cooking-in-the-cpp-kitchen-and-a-request-for-help/>>.

46 "Michel Bauwens and Sam Rose on the Choke Point Project," *P2P Foundation Wiki* <http://p2pfoundation.net/Michel_Bauwens_and_Sam_Rose_on_the_Choke_Point_Project>.

47 Rushkoff, "The Next Net."

48 Jason Pontin, "From the Editor: Mesh Networking Matters," *Technology Review*, September 2005 <<http://www.technologyreview.com/communications/14740/>>.

and it automatically links to any other mesh devices within radio range. It is an example of what internet architect David Reed calls “cooperative gain” – the more devices, the more bandwidth across the network.⁴⁹

Another benefit of meshworks is that, even if the central fiber-optic network is shut down and there are area limits to the propagation of the network, the local meshwork can support community darknets based entirely on their members' computers and mobile devices. Short of blanketing an entire country with an electromagnetic pulse, there's no way to shut down local meshworks.

The Freenet project is one form of architecture for an encrypted local dark meshwork. It is completely anonymous, since individual nodes' routing functions are encrypted. The downside is that it is not a proxy for the Web; the Freenet includes only material from the World Wide Web which has actually been imported into it and stored on member hard drives.⁵⁰

Nevertheless an urban Freenet, even if completely disconnected from the Web, could provide a robust range of services for a local counter-economy, including: hosting resident websites and community bulleting boards, a community encrypted currency on the model of Greco's credit-clearing networks, local email, sharing of music and other content files (including CAD/CAM files for micromanufacturers), telecommunication and teleconferencing links, assorted collaborative platforms, rating and reputational systems for local commerce, etc. It could also provide similar services for a distributed network like a phyle (about which more in a later chapter).

The Freenet, as a platform, can host member web pages, sites (“freesites”) and social networks visible only to members of the Freenet. It can be used as the darknet or Virtual Private Network platform for any local organization or distributed network. For example the Las Indias cooperative, with which phyle theorist David de Ugarte is affiliated, uses Freenet for its internal functions.

Another meshwork/nextnet project, Commotion Wireless, “aims to build a new type of tool for democratic organizing”:

an open source “device-as-infrastructure” distributed communications platform that integrates users’ existing cell phones, WiFi-enabled computers, and other WiFi-capable personal devices to create a metro-scale peer-to-peer (mesh) communications network.

What it means: Democratic activists around the globe will gain access to a secure and reliable platform to ensure their communications cannot be controlled or cut off by authoritarian regimes.⁵¹

The Commotion Wireless website itself describes the general outlines of the project in much greater detail:

...the developers, technavists, and organizers here propose to build a new type of tool for democratic organizing: an open source “device-as-infrastructure” distributed communications platform that integrates users’ existing cell phones, WiFi-enabled computers, and other WiFi-capable personal devices to create a metro-scale peer-to-peer (mesh) communications network. Leveraging a distributed, mesh wireless infrastructure provides two key enhancements to existing circumvention technologies and supports human rights advocates and civil society organizations working around the globe. First, a distributed infrastructure eliminates the ability of governments to completely disrupt communications by shutting down the commercial or state-owned communications infrastructure. Second, device-as-infrastructure networks enhance communications security among activists by eliminating points for centralized monitoring, by enabling direct peer-to-peer communication, and by aggregating and securing individual communications streams.

49 David Weingerger, “The Grid, Our Cars and the Net: One Idea to Link Them All,” *Wired.com*, May 8, 2009 <<http://www.wired.com/autopia/2009/05/the-grid-our-cars-and-the-internet-one-idea-to-link-them-all/>>.

50 <<http://freenetproject.org/>>.

51 Venessa Miemis, “10 Projects to Liberate the Web,” *Shareable: Science & Tech*, October 4, 2011 <<http://www.shareable.net/blog/10-projects-to-liberate-the-web>>.

For over a decade, developers here have pioneered the development of “device-as-infrastructure” broadband networks.... Specifically, this project proposes the following five-point solution:

- Create a robust and reliable participatory communications medium that is not reliant upon centralized infrastructure for local-to-local (peer-to-peer) and local-to-Internet communications;
- Design ad hoc device-as-infrastructure technologies that can survive major outages (e.g. electricity, Internet connectivity) and are resilient during emergencies, natural disasters, or other hostile environments where conventional telecommunications networks are easily crippled;
- Secure participants’ communication to protect data integrity and anonymity through strong end-to-end encryption and data aggregation;
- Implement communications technologies that integrate low-cost, pre-existing, off-the-shelf devices (e.g. cell phones, laptops, consumer WiFi routers) and maximize use of open source software; and,
- Develop an open, modular, and highly extensible communications platform that is easily upgraded and adapted to the particular needs and goals of different local users.⁵²

More closely related to the specific problems presented by police in Cairo and San Francisco, Stephanie Brancaforte of Avaaz announced a project to “blackout-proof the protests”

—with secure satellite modems and phones, tiny video cameras, and portable radio transmitters, plus expert support teams on the ground—to enable activists to broadcast live video feeds even during internet and phone blackouts and ensure the oxygen of international attention fuels their courageous movements for change.⁵³

The FreedomBox is a small plug-in server with a built-in Tor router, which can plug into an electrical outlet in your home and provide wireless service—as well as providing point-to-point meshwork connection to others with FreedomBoxes, in the event local wireless networks are shut down.⁵⁴ The Freedom Box is part of a larger hardware stack⁵⁵ promoted by the Free Network Foundation.⁵⁶ The stack includes the Freedom Tower—a high-powered mobile wi-fi hotspot with an encrypted router and uninterruptable power supply—which provided communications to Occupy Wall Street.⁵⁷

Venessa Miemis listed sixteen wireless meshwork projects aimed at circumventing state censorship.⁵⁸

Dust is a project that counters government attempts to filter certain kinds of traffic by protocol “fingerprinting,” summarily blocking protocols like SSL, Tor, BitTorrent, and VPNs. Dust reencodes the traffic into a form which cannot be correctly fingerprinted by the filtering system.⁵⁹

In May 2011 the Mozilla Foundation fell afoul of Homeland Security by refusing to comply with a request to remove a new extension from its Firefox browser—MAFIAAfire—which circumvents censorship of the Web by federal law enforcement and the content industries. MAFIAAfire “negates ICE’s domain seizures, by automatically rerouting users to alternate domains.”⁶⁰

52 <<https://tech.chambana.net/projects/commotion>>.

53 Stephanie Brancaforte, “Blackout-proof the protests—it’s happening!” Ahvaaz email newsletter, February 25, 2011.

54 “Learn About the FreedomBox!” Freedom Box Foundation <<http://www.freedomboxfoundation.org/learn/>> Accessed December 14, 2011.

55 <<https://commons.thefnf.org/index.php/FreeNetworkStack>>.

56 <<https://thefnf.org/>>.

57 <<https://commons.thefnf.org/index.php/FreedomTower>>.

58 Venessa Miemis, “16+ Projects & Initiatives Building Ad-Hoc Wireless Mesh Networks,” *Emergent by Design*, February 11, 2011 <<http://emergentbydesign.com/2011/02/11/16-projects-initiatives-building-ad-hoc-wireless-mesh-networks/>>.

59 Bruce Schneier, “Evading Internet Censorship,” *Schneier on Security*, August 28, 2013 <https://www.schneier.com/blog/archives/2013/08/evading_internet.html>.

60 Mike Masnick, “Homeland Security Demands Mozilla Remove Firefox Extension That Redirects Seized Domains,” *Techdirt*, May 5, 2011 <<http://www.techdirt.com/articles/20110505/14444714170/homeland-security-demands-mozilla-remove-firefox-extension-that-redirects-seized-domains.shtml>>.

And Firefox announced a new extension, explicitly directed against SOPA, which functioned much like the earlier MAFIAAfire to circumvent domain name takedowns.⁶¹ More recently, in August 2013, The Pirate Bay released PirateBrowser—an Internet browser for bypassing blocks—which was downloaded 100,000 times in the first three days after its issue.⁶²

III. Networks vs. Hierarchies

But if hierarchies don't do so well at suppressing networked organizations, centralized, hierarchical institutions are finding themselves all too vulnerable to networked resistance.

In the early 1970s, in the aftermath of a vast upheaval in American political culture, Samuel Huntington wrote of a “crisis of democracy”; the American people, he feared, were becoming ungovernable. In *The Crisis of Democracy*, he argued that the system was collapsing from demand overload, because of an excess of democracy. Huntington's analysis is illustrative of elite thinking behind the neoliberal policy agenda of the past thirty years.

For Huntington, America's role as “hegemonic power in a system of world order” depended on a *domestic* system of order; this system of order—variously referred to as corporate liberalism, consensus capitalism, Cold War liberalism, and the welfare-warfare state—assumed a general public willingness to stay out of government affairs.⁶³ And this was only possible because of a domestic structure of political authority in which the country “was governed by the president acting with the support and cooperation of key individuals and groups in the Executive office, the federal bureaucracy, Congress, and the more important businesses, banks, law firms, foundations, and media, which constitute the private establishment.”⁶⁴

America's position as defender of global capitalism required that its government have the ability “to mobilize its citizens for the achievement of social and political goals and to impose discipline and sacrifice upon its citizens in order to achieve these goals.”⁶⁵ Most importantly, this ability required that democracy be largely nominal, and that citizens be willing to leave major substantive decisions about the nature of American society to qualified authorities. It required, in other words, “some measure of apathy and non-involvement on the part of some individuals and groups.”⁶⁶

Unfortunately—from his standpoint—these requirements were being gravely undermined by “a breakdown of traditional means of social control, a delegitimation of political and other means of authority, and an overload of demands on government, exceeding its capacity to respond.”⁶⁷

The phenomena that caused Huntington to recoil in horror in the early 1970s must have seemed positively tame by the late 1990s. The potential for networked resistance created by the Internet exacerbated Huntington's crisis of governability by orders of magnitude.

There is a wide body of literature on the emergence of networked modes of resistance in the 1990s, beginning with the Rand studies on netwar by David Ronfeldt, John Arquilla and other writers. In their 1996 paper “The Advent of Netwar,” Arquilla and Ronfeldt wrote that technological evolution was working to the advantage of networks and the detriment of hierarchies. Although their focus was on the military aspect (what has since been called “Fourth Generation Warfare”), they also mentioned governability concerns in

61 Melanie Pinola, “DeSopa for Firefox Bypasses SOPA DNS Blocking,” *lifehacker*, December 20, 2011 <<http://lifehacker.com/5869665/desopa-for-firefox-bypasses-sopa-dns-blocking>>.

62 J.D. Tuccille, “Surf Forbidden Sites With Pirate Bay's PirateBrowser,” *Reason Hit & Run*, August 13, 2013 <<http://reason.com/blog/2013/08/14/surf-forbidden-sites-with-pirate-bays-pi>>.

63 Samuel P. Huntington, Michael J. Crozier, Joji Watanuki, *The Crisis of Democracy*. Report on the Governability of Democracies to the Trilateral Commission: Triangle Paper 8 (New York: New York University Press, 1975), pp. 105-6.

64 *Ibid.*, p. 92.

65 *Ibid.*, pp. 7-8.

66 *Ibid.*, pp. 113-5.

67 *Ibid.*, pp. 7-8.

civil society much like those Huntington raised earlier. “Intellectual property pirates,” “militant single-issue groups” and “transnational social activists,” in particular, were “developing netwar-like attributes.”

Now... the new information technologies and related organizational innovations increasingly enable civil-society actors to reduce their isolation, build far-flung networks within and across national boundaries, and connect and coordinate for collective action as never before. As this trend deepens and spreads, it will strengthen the power of civil-society actors relative to state and market actors around the globe....

For years, a cutting edge of this trend could be found among left-leaning activist NGOs concerned with human-rights, environmental, peace, and other social issues at local, national, and global levels. Many of these rely on APC affiliates for communications and aim to construct a “global civil society” strong enough to counter the roles of state and market actors. In addition, the trend is spreading across the political spectrum. Activists on the right—from moderately conservative religious groups, to militant antiabortion groups—are also building national and transnational networks based in part on the use of new communications systems.⁶⁸

In “Tribes, Institutions, Markets, Networks” (1996) Ronfeldt focused on the special significance of networks for global civil society.

...[A]ctors in the realm of civil society are likely to be the main beneficiaries. The trend is increasingly significant in this realm, where issue-oriented multiorganizational networks of NGOs—or, as some are called, nonprofit organizations (NPOs), private voluntary organizations (PVOs), and grassroots organizations (GROs)—continue to multiply among activists and interest groups who identify with civil society. Over the long run, this realm seems likely to be strengthened more than any other realm, in relative if not also absolute terms. While examples exist across the political spectrum, the most evolved are found among progressive political advocacy and social activist NGOs—e.g., in regard to environmental, human-rights, and other prominent issues—that depend on using new information technologies like faxes, electronic mail (e-mail), and on-line conferencing systems to consult and coordinate. This nascent, yet rapidly growing phenomenon is spreading across the political spectrum into new corners and issue areas in all countries.

The rise of these networks implies profound changes for the realm of civil society. In the eighteenth and nineteenth centuries, when most social theorists focused on state and market systems, liberal democracy fostered, indeed required, the emergence of this third realm of activity.... However, civil society was also considered to be a weaker realm than the state or the market. And while theorists treated the state and the market as systems, this was generally not the case with civil society....

Now, the innovative NGO-based networks are setting in motion new dynamics that promise to reshape civil society and its relations with other realms at local through global levels. Civil society appears to be the home realm for the network form, the realm that will be strengthened more than any other....

The network form seems particularly well suited to strengthening civil-society actors whose purpose is to address social issues. At its best, this form may thus result in vast collaborative networks of NGOs geared to addressing and helping resolve social equity and accountability issues that traditional tribal, state, and market actors have tended to ignore or are now unsuited to addressing well.

The network form offers its best advantages where the members, as often occurs in civil society, aim to preserve their autonomy and to avoid hierarchical controls, yet have agendas that are interdependent and benefit from consultation and coordination.⁶⁹

Networked global civil society, in the words of James Moore, is becoming a “Second Superpower”:

68 John Arquilla and David Ronfeldt, *The Advent of Netwar* MR-789 (Santa Monica, CA: RAND, 1996) <http://www.rand.org/pubs/monograph_reports/MR789/>.

69 David F. Ronfeldt, *Tribes, Institutions, Markets, Networks* P-7967 (Santa Monica: RAND, 1996) <<http://www.rand.org/pubs/papers/P7967/>>.

As the United States government becomes more belligerent in using its power in the world, many people are longing for a “second superpower” that can keep the US in check. Indeed, many people desire a superpower that speaks for the interests of planetary society, for long-term well-being, and that encourages broad participation in the democratic process. Where can the world find such a second superpower? No nation or group of nations seems able to play this role....

There is an emerging second superpower, but it is not a nation. Instead, it is a new form of international player, constituted by the “will of the people” in a global social movement. ...

While some of the leaders have become highly visible, what is perhaps most interesting about this global movement is that it is not really directed by visible leaders, but, as we will see, by the collective, emergent action of its millions of participants.... What makes these numbers important is the new cyberspace enabled interconnection among the members. This body has a beautiful mind. Web connections enable a kind of near-instantaneous, mass improvisation of activist initiatives....

New forms of communication and commentary are being invented continuously. Slashdot and other news sites present high quality peer-reviewed commentary by involving large numbers of members of the web community in recommending and rating items. Text messaging on mobile phones, or texting, is now the medium of choice for communicating with thousands of demonstrators simultaneously during mass protests. Instant messaging turns out to be one of the most popular methods for staying connected in the developing world, because it requires only a bit of bandwidth, and provides an intimate sense of connection across time and space. The current enthusiasm for blogging is changing the way that people relate to publication, as it allows realtime dialogue about world events as bloggers log in daily to share their insights....

The Internet and other interactive media continue to penetrate more and more deeply all world society, and provide a means for instantaneous personal dialogue and communication across the globe. The collective power of texting, blogging, instant messaging, and email across millions of actors cannot be overestimated. Like a mind constituted of millions of inter-networked neurons, the social movement is capable of astonishingly rapid and sometimes subtle community consciousness and action.

Thus the new superpower demonstrates a new form of “emergent democracy” that differs from the participative democracy of the US government. Where political participation in the United States is exercised mainly through rare exercises of voting, participation in the second superpower movement occurs continuously through participation in a variety of web-enabled initiatives. And where deliberation in the first superpower is done primarily by a few elected or appointed officials, deliberation in the second superpower is done by each individual—making sense of events, communicating with others, and deciding whether and how to join in community actions. Finally, where participation in democracy in the first superpower feels remote to most citizens, the emergent democracy of the second superpower is alive with touching and being touched by each other, as the community works to create wisdom and to take action.

How does the second superpower take action? Not from the top, but from the bottom. That is, it is the strength of the US government that it can centrally collect taxes, and then spend, for example, \$1.2 billion on 1,200 cruise missiles in the first day of the war against Iraq. By contrast, it is the strength of the second superpower that it could mobilize hundreds of small groups of activists to shut down city centers across the United States on that same first day of the war. And that millions of citizens worldwide would take to their streets to rally....

...[T]he continual distributed action of the members of the second superpower can, I believe, be expected to eventually prevail. Distributed mass behavior, expressed in rallying, in voting, in picketing, in exposing corruption, and in purchases from particular companies, all have a profound effect on the nature of future society. More effect, I would argue, than the devastating but unsustainable effect of bombs and other forms of coercion.

Deliberation in the first superpower is relatively formal—dictated by the US constitution and by years of legislation, adjudicating, and precedent. The realpolitik of decision making in the first superpower—as opposed to what is taught in civics class—centers around lobbying and campaign contributions by moneyed special interests—big oil, the military-industrial complex, big agriculture, and big drugs—to mention only a few. In many cases, what are acted upon are issues for which some group is willing to spend lavishly. By contrast, it is difficult in the US government system to champion policy goals that have broad, long-term value for many citizens, such as environment, poverty reduction and

third world development, women's rights, human rights, health care for all. By contrast, these are precisely the issues to which the second superpower tends to address its attention.

Deliberation in the second superpower is evolving rapidly in both cultural and technological terms. It is difficult to know its present state, and impossible to see its future. But one can say certain things. It is stunning how quickly the community can act—especially when compared to government systems. The Internet, in combination with traditional press and television and radio media, creates a kind of “media space” of global dialogue. Ideas arise in the global media space. Some of them catch hold and are disseminated widely....

...The shared, collective mind of the second superpower is made up of many individual human minds—your mind and my mind—together we create the movement. In traditional democracy our minds don't matter much—what matters are the minds of those with power of position, and the minds of those that staff and lobby them. In the emergent democracy of the second superpower, each of our minds matters a lot. For example, any one of us can launch an idea. Any one of us can write a blog, send out an email, create a list. Not every idea will take hold in the big mind of the second superpower—but the one that eventually catches fire is started by an individual. And in the peer-oriented world of the second superpower, many more of us have the opportunity to craft submissions, and take a shot.

The contrast goes deeper. In traditional democracy, sense-making moves from top to bottom. “The President must know more than he is saying” goes the thinking of a loyal but passive member of the first superpower. But this form of democracy was established in the 18th century, when education and information were both scarce resources. Now, in more and more of the world, people are well educated and informed. As such, they prefer to make up their own minds. Top-down sense-making is out of touch with modern people.⁷⁰

In *The Zapatista "Social Netwar" in Mexico*,⁷¹ Arquilla, Ronfeldt et al. expressed some concern over the possibilities of decentralized "netwar" techniques for destabilizing the existing political and economic order. They saw early indications of such a movement in the global political support network for the Zapatistas. Loose, ad hoc coalitions of affinity groups, organizing through the Internet, could throw together large demonstrations at short notice, and "swarm" the government and mainstream media with phone calls, letters, and emails far beyond their capacity to cope.

The information revolution is leading to the rise of network forms of organization, whereby small, previously isolated groups can communicate, link up, and conduct coordinated joint actions as never before. This, in turn, is leading to a new mode of conflict—“netwar”—in which the protagonists depend on using network forms of organization, doctrine, strategy, and technology. Many actors across the spectrum of conflict—from terrorists, guerrillas, and criminals who pose security threats to social activists who do not—are developing netwar designs and capabilities.⁷²

The interesting thing about the Zapatista netwar, according to Ronfeldt and Arquilla, is that to all appearances it started out as a run-of-the-mill Third World army's suppression of a run-of-the-mill local insurgency. Right up until Mexican troops entered Chiapas, there was every indication the uprising would be suppressed quickly according to the standard script, and that the world outside Mexico would “little note nor long remember” it. It looked that way until Subcommandante Marcos and the Zapatistas made their appeal to global civil society and became the center of a networked movement that stirred activists the world over. The Mexican government was blindsided by the global reaction.⁷³ The reaction included not only activist support around the world, but a demonstration of hundreds of thousands in solidarity in Mexico City

70 James F. Moore, “The Second Superpower Rears Its Beautiful Head,” Chapter Two of John Lebkowski and Mitch Ratcliffe, eds., *Extreme Democracy* (Lulu, 2005), pp. 37-41 <<http://www.extremedemocracy.com/>>.

71 John Arquilla, David Ronfeldt, Graham Fuller, and Melissa Fuller. *The Zapatista "Social Netwar" in Mexico* MR-994-A (Santa Monica: Rand, 1998) <http://www.rand.org/pubs/monograph_reports/MR994/index.html>.

72 *Ibid.*, xi.

73 David Ronfeldt and Armando Martinez, “A Comment on the Zapatista Netwar,” in Ronfeldt and Arquilla, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: Rand, 1997), pp. 369-371.

—a fact which no doubt figured in the government's decision to accept a ceasefire.⁷⁴ Since then, Immanuel Wallerstein argues, this political support has been the main factor in the government limiting itself largely to skirmishes and harassment of areas under EZLN control, despite overwhelming military superiority.⁷⁵

Swarming—in particular the swarming of public pressure through letters, phone calls, emails, and public demonstrations, and the paralysis of communications networks by such swarms—is the direct descendant of the “overload of demands” Huntington wrote of in the 1970s. In “Swarming & the Future of Conflict,” Ronfeldt and Arquilla focused on swarming, in particular, as a technique that served the entire spectrum of networked conflict—including “civic-oriented actions.”⁷⁶ Despite the primary concern with swarming as a military phenomenon, they also remarked on networked global civil society—and the Zapatista support network in particular—as examples of peaceful swarming with which states were ill-equipped to deal:

Briefly, we see the Zapatista movement, begun in January 1994 and continuing today, as an effort to mobilize global civil society to exert pressure on the government of Mexico to accede to the demands of the Zapatista guerrilla army (EZLN) for land reform and more equitable treatment under the law. The EZLN has been successful in engaging the interest of hundreds of NGOs, who have repeatedly swarmed their media-oriented “fire” (i.e., sharp messages of reproach) against the government. The NGOs also swarmed in force—at least initially—by sending hundreds of activists into Chiapas to provide presence and additional pressure.⁷⁷

At present, our best understanding of swarming—as an optimal way for myriad, small, dispersed, autonomous but internetworked maneuver units to coordinate and conduct repeated pulsing attacks, by fire or force—is best exemplified in practice by the latest generation of activist NGOs, which assemble into transnational networks and use information operations to assail government actors over policy issues. These NGOs work comfortably within a context of autonomy from each other; they also take advantage of their high connectivity to interact in the fluid, flexible ways called for by swarm theory.

The growing number of cases in which activists have used swarming include, in the security area, the Zapatista movement in Mexico.... The [Zapatista movement] is a seminal case of “social netwar,” in which transnationally networked NGOs helped deter the Mexican government and army from attacking the Zapatistas militarily....

Social swarming is especially on the rise among activists that oppose global trade and investment policies. Internet-based protests helped to prevent approval of the Multilateral Agreement on Investment (MAI) in Europe in 1998. Then, on July 18, 1999—a day that came to be known as J18—furious anticapitalist demonstrations took place in London, as tens of thousands of activists converged on the city, while other activists mounted parallel demonstrations in other countries. J18 was largely organized over the Internet, with no central direction or leadership. Most recently, with J18 as a partial blueprint, several tens of thousands of activists, most of them Americans but many also from Canada and Europe, swarmed into Seattle to shut down a major meeting of the World Trade Organization (WTO) on opening day, November 30, 1999—in an operation known to militant activists and anarchists as N30, whose planning began right after J18. The vigor of these three movements and the effectiveness of the activists’ obstructionism came as a surprise to the authorities.

The violent street demonstrations in Seattle manifested all the conflict formations discussed earlier—the melee, massing, maneuver, and swarming. Moreover, the demonstrations showed that information-age networks (the NGOs) can prevail against hierarchies (the WTO and the Seattle police), at least for a while. The persistence of this “Seattle swarming” model in the April 16, 2000, demonstrations (known as A16) against the International Monetary Fund and the World Bank in Washington, D.C., suggests that it has proven effective enough to continue to be used...

74 Andalusia Knoll and Itandehui Reyes, “From Fire to Autonomy: Zapatistas, 20 Years of Walking Slowly,” *Truthout*, January 25, 2014 <<http://www.truth-out.org/news/item/21427-from-fire-to-autonomy-zapatistas-20-years-of-walking-slowly>>.

75 Immanuel Wallerstein, “The Neo-Zapatistas: Twenty Years After,” *Immanuel Wallerstein*, May 1, 2014 <<http://www.iwallerstein.com/nezapatistas-twenty-years/>>.

76 Arquilla and Ronfeldt, *Swarming & the Future of Conflict* DB-311 (Santa Monica, CA: RAND, 2000), iii <http://www.rand.org/pubs/DOCUMENTED_briefings/DB311/>.

77 *Ibid.*, p. 39.

In these social networks... swarming appears not only in real-life actions but also through measures in cyberspace. Swarms of email sent to government figures are an example. But some “hacktivists” aim to be more disruptive—pursuing “electronic civil disobedience.” One notable recent effort associated with a collectivity called the Electronic Disturbance Theater is actually named SWARM. It seeks to move “digital Zapatismo” beyond the initial emphasis of its creators on their “FloodNet” computer system, which has been used to mount massive “ping” attacks on government and corporate web sites, including as part of J18. The aim of its proponents is to come up with new kinds of “electronic pulse systems” for supporting militant activism. This is clearly meant to enable swarming in cyberspace by myriad people against government, military, and corporate targets.⁷⁸

Swarming, in all its manifestations, involves a new understanding of the strategic principle of mass, in which mass is achieved by a rapid, transitory concentration of forces at the point of attack. The flash mob, when used for activist purposes, is a good example of this. Another, older example of the same phenomenon was the Wobbly practice of unannounced one-day strikes at random intervals.

The new principle of mass is far less vulnerable to preemptive disruption in its preparatory stages. Swarming attacks, which can be organized on comparatively short notice by loose networks, require far less advance planning. More conventional mass demonstrations in the previous era, like the East German uprisings in 1989, were much more visible to authorities during their planning stages. Now the planning and preparatory phase is drastically shortened and virtually invisible to the authorities, with the highly visible public demonstration seeming to appear out of nowhere with little or no warning.⁷⁹

The German *Blitzkrieg* doctrine, by way of analogy, relied on radio-equipped tanks to turn their armored force—fewer, more lightly armored and with lighter guns than that of the French—into a “coordinated group weapon.”⁸⁰ German armored formations, by converging rapidly at the breakthrough point and then rapidly dispersing, or by achieving concentration of fire without spatial concentration, prefigured the flash mobs which—although possessing far less firepower than the state's police—are able to form and disperse before the state can react to them.

Since then, doctrines like the American Airland Battle of the 1980s attempted to attain mass through concentration of fire (coordinated artillery, missile and air strikes) on the *Schwerpunkt*, with the physical concentration of rapidly assembled and dispersed ground forces playing a secondary role. A force with superior agility, despite smaller numbers, can achieve local superiority at will and defeat the enemy in detail.

Netwar, Ronfeldt and Arquilla wrote elsewhere, is characterized by “the networked organizational structure of its practitioners—with many groups actually being leaderless—and the suppleness in their ability to come together quickly in swarming attacks.”⁸¹

The disappearance of time and space limitations, associated with networked communications operating at the speed of light, has strong implications for the growing capability of swarming attacks. Consider the radical compression of the time factor, as described by Sarah Wanenchak:

Now the spread of information is nearly instantaneous. A protest is violently put down in an afternoon; by the evening, one can see solidarity demonstrations in multiple other nations. People act and react more quickly and more fluidly in response to new information, to changing perceptions of opportunity and threat. The heartbeat of collective action has sped up.

78 *Ibid.*, pp. 50-52.

79 Clay Shirky, *Here Comes Everybody*, pp. 168-169.

80 *Ibid.*, pp. 172-173.

81 John Arquilla and David Ronfeldt, “Introduction,” in Arquilla and Ronfeldt, eds., “Networks and Netwars: The Future of Terror, Crime, and Militancy” MR-1382-OSD (Santa Monica: Rand, 2001) <http://www.rand.org/pubs/monograph_reports/MR1382/> ix.

Coordination across large distances is another practical result of the increased speed of information sharing.... [N]ow protesters in multiple different countries call a day of protest, and over 900 cities worldwide take part.⁸²

And as Julian Assange argues, such advances in speed and ubiquity make it possible for the swarming attack to take the form of a full court press, overwhelming multiple governments or agencies at once so that each is too preoccupied dealing with its own swarming attacks to cooperate with the others.

In relation to the Arab Spring, the way I looked at this back in October of 2010 is that the power structures in the Middle East are interdependent, they support each other. If we could release enough information fast enough about many of these powerful individuals and organizations, their ability to support each other would be diminished. They'd have to fight their own local battles – they'd have to turn inward to deal with the domestic political fallout from the information. And therefore they would not have the resources to prop up surrounding countries.⁸³

The rest of this section is, in many ways, a direct continuation of our discussion of stigmergy in the previous chapter. It might be fruitful to reread the fourth section of Chapter One and proceed directly to the material below.

Many open-source thinkers, going back to Eric Raymond in *The Cathedral and the Bazaar*, have pointed out the nature of open-source methods and network organization as force-multipliers.⁸⁴ Open-source design communities pick up the innovations of individual members and quickly distribute them wherever they are needed, with maximum economy. This is a feature of the stigmergic organization that we considered earlier.

This principle is at work in the file-sharing movement, as described by Cory Doctorow. Individual innovations immediately become part of the common pool of intelligence, universally available to all.

Raise your hand if you're thinking something like, “But DRM doesn't have to be proof against smart attackers, only average individuals!...”

...I don't have to be a cracker to break your DRM. I only need to know how to search Google, or Kazaa, or any of the other general-purpose search tools for the cleartext that someone smarter than me has extracted.⁸⁵

It used to be that copy-prevention companies' strategies went like this: “We'll make it easier to buy a copy of this data than to make an unauthorized copy of it. That way, only the *uber*-nerds and the cash-poor/time rich classes will bother to copy instead of buy.” But every time a PC is connected to the Internet and its owner is taught to use search tools like Google (or The Pirate Bay), a third option appears: you can just download a copy from the Internet....⁸⁶

Bruce Schneier describes the stigmergic Bazaar model as automation lowering the marginal cost of sharing innovations.

Automation also allows class breaks to propagate quickly because less expertise is required. The first attacker is the smart one; everyone else can blindly follow his instructions. Take cable TV fraud as an example. None of the cable TV companies would care much if someone built a cable receiver in his basement and illicitly watched cable television. Building that device requires time, skill, and some

82 Sarah Wanenchak, “Everything New is Old Again: Historical Augmented Revolution,” *Cyborgology*, November 29, 2011 <<http://thesocietypages.org/cyborgology/2011/11/29/everything-new-is-old-again-historical-augmented-revolution/>>.

83 Michael Hastings, “Julian Assange: The Rolling Stone Interview,” *Rolling Stone*, February 2, 2012 <<http://www.rollingstone.com/politics/news/julian-assange-the-rolling-stone-interview-20120118?print=true>>.

84 Eric S. Raymond, *The Cathedral and the Bazaar* <<http://catb.org/~esr/writings/homesteading>>.

85 Doctorow, “Microsoft DRM Research Talk,” in *Content: Selected Essays on Technology, Creativity, Copyright, and the Future of the Future* (San Francisco: Tachyon Publications, 2008), pp. 7-8.

86 Doctorow, “It's the Information Economy, Stupid,” in *Ibid.*, p. 60.

money. Few people could do it. Even if someone built a few and sold them, it wouldn't have much impact.

But what if that person figured out a class break against cable television? And what if the class break required someone to push some buttons on a cable box in a certain sequence to get free cable TV? If that person published those instructions on the Internet, it could increase the number of nonpaying customers by millions and significantly affect the company's profitability.⁸⁷

The reduced cost of aggregating or replicating small contributions is a key feature of stigmergy. This is one illustration of a broader advantage of stigmergy: modular design. In Schneier's words, expertise is "[e]ncapsulated and commoditized." "Take a class break [i.e. a hack], automate it, and propagate the break for free, and you've got a recipe for a security disaster."⁸⁸

Open-source insurgency follows this model, with each individual contribution quickly becoming available to all. John Robb writes:

The decentralized, and seemingly chaotic guerrilla war in Iraq demonstrates a pattern that will likely serve as a model for next generation terrorists. This pattern shows a level of learning, activity, and success similar to what we see in the open source software community. I call this pattern the bazaar. The bazaar solves the problem: how do small, potentially antagonistic networks combine to conduct war? Lessons from Eric Raymond's "The Cathedral and the Bazaar" provides a starting point for further analysis. Here are the factors that apply (from the perspective of the guerrillas):

- Release early and often. Try new forms of attacks against different types of targets early and often. Don't wait for a perfect plan.
- Given a large enough pool of co-developers, any difficult problem will be seen as obvious by someone, and solved. Eventually some participant of the bazaar will find a way to disrupt a particularly difficult target. All you need to do is copy the process they used.
- Your co-developers (beta-testers) are your most valuable resource. The other guerrilla networks in the bazaar are your most valuable allies. They will innovate on your plans, swarm on weaknesses you identify, and protect you by creating system noise.⁸⁹

The rapid innovation in Improvised Explosive Devices (IEDs) achieved by open-source warfare networks in Iraq and Afghanistan is a case in point.⁹⁰ Any innovation developed by a particular cell of Al Qaeda Iraq, if successful, is quickly adopted by the entire network.

The key to understanding the agility of networks is the concept of cognitive feedback loops.

Intelligence is a cognitive feedback system that allows us to adjust appropriately to changing conditions....

As a society, we use things like science, journalism, blogs, twitter feeds, and intelligence services to collectively observe what's going on within and around our society. We use pundits, academia, government deliberations, boardroom conferences, online forums and other conversations to reflect on what we've observed and to formulate our responses based on what we think we're learning. We call up relevant pieces of the past using libraries, databases, history, the records of mass media, and our own individual memories. We take action through corporate and government policies and activities and the billions of decisions and activities of variously informed individuals, families, networks, and other social groupings. We then reflect on the results of what "we" have done, not only through the institutions I

87 Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York: Copernicus Books, 2003), p. 95.

88 *Ibid.*, p. 96.

89 John Robb, "THE BAZAAR'S OPEN SOURCE PLATFORM," *Global Guerrillas*, Sept3ember 24, 2004 <http://globalguerrillas.typepad.com/globalguerrillas/2004/09/bazaar_dynamics.html>. Eric Raymond has raised a caveat concerning Robb's application of the Bazaar paradigm [email]

90 Adam Higginbotham, "U.S. Military Learns to Fight Deadliest Weapons," *Wired*, July 28, 2010 <http://www.wired.com/magazine/2010/07/ff_roadside_bombs/all/1>.

mentioned earlier—science, journalism, etc.—but also through the investigations and protests of activists and other political players working through political campaigns and lobbying.

This is our societal collective intelligence—or lack of it—the feedback system through which our society responds to changes in its collective circumstances—changes like climate change....

How well does our society's collective intelligence feedback system—the many ways we collectively learn (or not) from experience—recognize and deal with the feedback systems that generate climate change? What factors help us do this—and which ones hinder us? THIS is what we need to attend to.

Because ultimately, climate change is not the issue. ***Ultimately, the issue is our collective ability to observe, think, feel, decide, act, and reflect on our actions and their results. If we can do that well, we can deal well with every issue we face because—thanks to our own cognitive feedback powers—it doesn't matter where we start. We'll be able to improve and correct our course as we proceed, collectively, into a better future.***⁹¹

For this reason, John Robb argues, a hierarchical military establishment like the U.S. is unlikely to surpass the agility of a networked effort like Al Qaeda Iraq.

First, out-innovating the insurgency will most likely prove unsuccessful. The insurgency uses an open-source community approach (similar to the decentralized development process now prevalent in the software industry) to warfare that is extremely quick and innovative. New technologies and tactics move rapidly from one end of the insurgency to the other, aided by Iraq's relatively advanced communications and transportation grid - demonstrated by the rapid increases in the sophistication of the insurgents' homemade bombs. This implies that the insurgency's innovation cycles are faster than the American military's slower bureaucratic processes (for example: its inability to deliver sufficient body and vehicle armor to our troops in Iraq).⁹²

Stigmergic, networked organizations are far more agile than hierarchical institutions because they require no permission or administrative coordination to act. A traditional hierarchy, in which decisions are mediated administratively or socially, incurs enormous transaction costs getting everyone on the same page before anyone can act.

Networks have the property that Nassim Taleb calls “antifragility.” An antifragile system is one that “regenerates itself continuously by using, rather than suffering from, random events, unpredictable shocks, stressors, and volatility. The antifragile gains from prediction errors, in the long run.”⁹³

The speed and agility of the network, its shortened reaction time, and the rapidity with which it shares information and new techniques, mean that networks are typically inside what strategist John Boyd called the OODA loop of hierarchies.⁹⁴ They react more quickly to changing circumstances than do hierarchies, so they can stay a step ahead of them and keep them constantly off-balance. As a result, networks can go through multiple generations of tactical innovation while hierarchies are still ponderously formulating a response to first-generation practices. Organizations that can process new information and make generational

91 Tom Atlee, “Feedback Dynamics in Climate and Society,” *Random Communications from an Evolutionary Edge*, February 2013 <<http://tom-atlee.posterous.com/feedback-dynamics-in-climate-and-society>>.

92 John Robb, “Open Source War,” *New York Times*, October 15, 2005 <<http://www.nytimes.com/2005/10/15/opinion/15robb.html>>

93 Nassim Taleb, *Antifragile: Things That Gain From Disorder* (New York: Random House, 2012), p. 8.

94 “...in order to win, we should operate at a *faster tempo or rhythm* than our adversaries—or, better yet, get inside adversary's *Observation-Oriented-Decision-Action time cycle or loop*.” John R. Boyd, *Patterns of Conflict* (December 1986), p. 5. The idea is to “Simultaneously compress our time and stretch-out adversary time to generate a *favorable mismatch in time/ability* to shape and adapt to change.” One does this by exploiting operations and weapons that “Generate a rapidly changing environment” and at the same time to “Inhibit an adversary's capacity to adapt to such an environment.” p. 7. By doing this one may “Render adversary powerless by denying him the opportunity to cope with unfolding circumstances.” p. 136.

changes in praxis in response to that information more quickly outperform those that don't. Boyd biographer Grant Hammond writes:

Boyd's answer is that we should be open to possibilities, to opportunities and ready and able to recognize choices and make them. It is all a matter of connections and choices. The more we know, the more we connect—to the environment, to the past, the future, to people, to ideas, and to things. In doing so, we have to make choices, to prioritize, to do trade-off thinking about options and possibilities. We also have to embrace novelty, to synthesize, to create opportunities out of the things around us, to be the architect of our own life in so far as possible. For Boyd, living is thinking and creating through endless OODA Loops of various sizes, speeds, and importance.⁹⁵

Boyd called it the Law of Iteration:

the primary determinant to winning dogfights was not observing, orienting, planning, or acting better. The primary determinant to winning dogfights was observing, orienting, planning, and acting *faster*. In other words, how quickly one could iterate. *Speed of iteration*, Boyd suggested, *beats quality of iteration*.⁹⁶

Generally, OODA loops become shorter as the “distance” decreases, or friction is reduced (in information terms) between the observation and acting portion of the loop—the actor ideally being empowered to directly implement changes in actions based on her own observation of the results of previous action. Anything that erects barriers between the different sub-processes of the OODA loop—like policy-making procedures within a hierarchy—or impedes feedback will slow down information-processing and reaction.

Whatever has been planned, there are always unwanted consequences for a reason that has nothing to do with the quality of the research or with the precision of the plan, but with the very nature of action. It has never been the case that you first know and then act. You first act tentatively and then begin to know a bit more before attempting again.⁹⁷

To synthesize Boyd and Taleb, an antifragile system is characterized by a short OODA loop: a rapid cycle of iterations and immediate adoption of successful variations. The larger the number of nodes contributing their individual experience, and the faster the cycle of iterations, the more likely the network is to benefit. A good example from Taleb is research. Payoffs from research follow a power law distribution: a small number of trials pay off enormously. “Consequently, payoff from research should necessarily be linear to number of trials, not total funds involved in the trials.”⁹⁸ Individual innovations are random and unpredictable, and do not correlate with research expenditure. What matters is the size of the network, the number of iterations, and the lowest possible transaction cost of replicating innovations within the network.

Only successful iterations matter because their successes become the collective property of the entire network. A single network is experiencing—in the sense of benefiting from the experience of—thousands, millions or billions of constant iterations, so that the collective spins off innovations with the speed of replicating yeast, and evolves as fast as a bacteria population developing antibiotic resistance.

A stigmergic network with a short OODA loop that can adopt the benefits of individual nodes' experience evolves in a Lysenkoist manner. In Darwinian evolution, only the most successful individuals live and pass their successful mutations to their own physical offspring. But stigmergic organization means that every individual node that adopts the successful innovation through imitation becomes the “offspring” of the

95 Grant T. Hammond, “The Essential Boyd” October 6, 2006 <<https://fasttransients.files.wordpress.com/2012/03/hammond-theessentialboyd1.pdf>>.

96 Jeff Atwood, “Boyd's Law of Iteration,” *Coding Horror*, February 7, 2007 <<http://www.codinghorror.com/blog/2007/02/boyds-law-of-iteration.html>>.

97 Bruno Latour, quoted at *Infotechia* <<http://infotechia.com/post/37881756675/whatever-has-been-planned-there-are-always>>.

98 Taleb, p. 230.

innovator; the successful mutations generated by individual nodes can immediately be adopted as part of the genetic code of every other node in the network, without the others having to die off. So the network as a whole thrives and grows in response to randomness and volatility—the definition of antifragility.

In the evolutionary model, the network is closer to the species than to the individual animal.

To satisfy the conditions for... immortality, the organisms need to predict the future with perfection—near perfection is not enough. But by letting the organisms go one lifespan at a time, with modifications between successive generations, nature does not need to predict future conditions.... Every random event will bring its own antidote in the form of ecological variation. It is as if nature changed itself at every step and modified its strategy every instant.

Consider this in terms of economic and institutional life. If nature ran the economy, it would not continuously bail out its living members to make them live forever. Nor would it have permanent administrations and forecasting departments that try to outsmart the future....⁹⁹

Compare this to the hierarchical organization, like John Kenneth Galbraith's corporate technostructure in *The New Industrial State*, which survives only by suppressing randomness and volatility in its surrounding environment and making it predictable—in other words, it's fragile.

When you are fragile, you depend on things following the exact planned course, with as little deviation as possible—for deviations are more harmful than helpful. This is why the fragile needs to be very predictive in its approach, and, conversely, predictive systems cause fragility. When you want deviations, and you don't care about the possible dispersion of outcomes that the future can bring, since most will be helpful, you are antifragile.¹⁰⁰

What makes life simple is that the robust and antifragile don't have to have as accurate a comprehension of the world as the fragile—and they do not need forecasting.¹⁰¹

“Optionality”—the freedom from not being locked into a course of action by past investments or a burden of overhead and debt—means “you don't have much need for what is commonly called intelligence, knowledge, insight, skills.... For you don't have to be right that often.” Instead, you can gain from random trial and error and incremental tinkering. In evolution, “nature simply keeps what it likes....”¹⁰² The network benefits from the long-shot contributions of any members, without any downside risk to the network as a whole from individual failures.

In most cases individual success comes from luck or trial and error, not knowledge or predictive capability. The knowledge inheres not in individuals, but in the process or the network as a whole—whether, as Taleb says, it be phrased in the terms of the Muslim skeptic philosopher Al-Ghazali who said knowledge is a property of God), Adam Smith's invisible hand of the market, or modern theorists who talk about self-organizing systems.¹⁰³

Stigmergy means that the network is far—far, far—more than the sum of its individual nodes. Each addition to the size of a network is non-linear.

Collaboration has an explosive upside, what is mathematically called a superadditive function, i.e., one plus one equals more than two, and one plus one plus one equals much, much more than three. That is pure nonlinearity with explosive benefits...¹⁰⁴

99 *Ibid.* p. 68.

100 *Ibid.* p. 71.

101 *Ibid.* p. 135.

102 *Ibid.* pp. 180-181.

103 *Ibid.* p. 233.

104 *Ibid.*

If there is intelligence involved—and I believe there is—the ex post theories constructed by academics may in some sense model it. But the intelligence itself is mainly an emergent phenomenon of the collective.

The ability to take advantage of this kind of stigmergic effect tends to be identified with module-platform architectures that are infinitely granular and possess low overhead. Such architectures position the collective to quickly take advantage of random opportunity, whereas centralized or hierarchical architectures not only make it harder to take advantage of opportunities but also to escape path dependencies from unsuccessful decisions in the past. The central property of top-down decision-making, Taleb says: it is

usually irreversible, so mistakes tend to stick, whereas bottom-up is gradual and incremental, with creation and destruction along the way....

Further, things that grow in a natural way... have a fractal quality to them. Like everything alive, all organisms, like lungs, or trees, grow in some form of self-guided but tame randomness.... These fractals induce a certain wealth of detail based on a small number of rules of repetition of nested patterns.¹⁰⁵

Taleb discusses trial-and-error tinkering and optionality in language that sounds much like Jane Jacobs's argument that technological advancement results mainly from taking advantage of unforeseen spinoffs or off-brand uses of technologies originally developed for other purposes.

Coca-Cola began as a pharmaceutical product. Tiffany & Co.... started life as a stationery store.... Raytheon, which made the first missile guidance system, was a refrigerator maker.... Nokia, who used to be the top mobile phone maker, began as a paper mill.... DuPont, now famous for Teflon... and the durable fabric Kevlar, actually started out as an explosives company.¹⁰⁶

Harold Jarche makes similar points to Taleb's and Boyd's about the need for a faster learning-response cycle and the need enable optionality by individual participants in the networked organization.

As feedback loops get faster with increased connectivity, the ability to learn and “spin on a dime” becomes paramount.... Technology is only a small part of creating more nimble companies. Workers have to be able to recognize patterns in complexity and chaos and be empowered to do something with their observations and insights....

Innovative and contextual methods mean that standard processes do not work for **exception-handling** or identifying new patterns. Self-selection of tools puts workers in control of what they use, like **knowledge artisans** whose distinguishing characteristic is seeking and sharing information to complete tasks. Equipped with, and augmented by, technology, they cooperate through their networks to solve complex problems and test new ideas. This only works in transparent environments.¹⁰⁷

We quoted, earlier, R. A. Wilson's observations on the tendency of hierarchy to suppress accurate feedback to those in authority, so that they're unable to respond properly to information from their environment. Open, networked associations, on the other hand, are agile precisely because, in an organization where individuals possess no authority over each other, there are no barriers to accurate feedback.

The problem, as we saw, is that hierarchies can't afford to be antifragile because they're founded on conflict of interest. Attempting to make an institution more legible to those at the top of the hierarchy, by deskilling labor, will make processes more fragile.

Innovation and progress come through interaction between large numbers of individuals—but horizontally, not in a centrally planned manner. Hierarchy preempts this horizontal relationship and attempts to extract rents from it, thereby rendering the parts—the source of real innovation—impotent.

105 *Ibid.* pp. 324-325.

106 *Ibid.* p. 235.

107 Harold Jarche, “hyper connected pattern-seeking,” *Life in perpetual Beta*, December 11, 2012 <<http://www.jarche.com/2012/12/hyper-connected-pattern-seeking/>>.

Although Deming's motto "Drive out fear" can never be fully realized in a hierarchy, it can be in a self-organized network.

The whole ethos of the network, as illustrated by Eric Raymond's Bazaar, is based on sharing knowledge ("release early and release often") and benefiting from feedback ("many eyeballs make shallow bugs").

A good example is modern science. Alchemists, Clay Shirky argues, failed to benefit from each other's knowledge because they were, as a group,

notably reclusive; they typically worked alone, they were secretive about their methods and their results, and they rarely accompanied claims of insight or success with anything that we'd recognize today as documentation, let alone evidence. Alchemical methods were hoarded rather than shared, passed down from master to apprentice, and when the alchemists did describe their experiments, the descriptions were both incomplete and vague.

This was hardly a recipe for success; even worse, no two people working with alchemical descriptions could reliably even fail in the same way. As a result, alchemical conclusions accumulated only slowly, with no steady improvement in utility. Absent transparent methods and a formal way of rooting out errors, erroneous beliefs were as likely as correct ones to be preserved over generations. In contrast, members of the Invisible College [a number of natural philosophers grouped around Robert Boyle in 1645—direct ancestor of the Royal Society] described their methods, assumptions, and results to one another, so that all might benefit from both successes and failures....

Culture—not tools or insights—animated the Invisible College and transmuted alchemy into chemistry. The members accumulated facts more quickly, and were able to combine existing facts into new experiments and new insights. By insisting on accuracy and transparency, and by sharing their assumptions and working methods with one another, the collegians had access to the group's collective knowledge and constituted a collaborative circle.¹⁰⁸

And the American bureaucratic national security state's clumsy response to terrorism is typical of the way hierarchies react to networks.

According to some estimates, it now takes Iraqi insurgents less than a month to adapt their methods of attack, much faster than coalition troops can respond. "For every move we make, the enemy makes three," U.S. Brigadier General Joe E. Ramirez Jr. told attendees at a May conference on IEDs. "The enemy changes techniques, tactics, and procedures every two to three weeks. Our biggest task is staying current and relevant."

Unfortunately, the traditional weapons acquisition process, which dictates how the United States and other Western militaries define and develop new weapons systems, is simply not designed to operate on such a fleeting timescale. It can take years and sometimes decades—not to mention many millions or billions of dollars—for a new military machine to move from concept to design to testing and out into the field. Worse, the vast majority of the battlefield technologies now wending their way through the acquisition bureaucracy were intended to fight large force-on-force battles among sovereign nations, not the guerrilla warfare that typifies the conflicts in Iraq, Afghanistan, and elsewhere....

This past spring and summer I interviewed dozens of current and former military officers, analysts, weapons developers, and others to try to understand why the coalition forces' technological might has proved so ineffectual. Nearly everyone I spoke with agreed there is a serious mismatch between the West's industrial-age approach to warfare and the insurgents' more fluid and adaptive style....

Terrorist Web sites serve not only to spread propaganda but also to share knowledge among insurgent groups.... That helps explain why the learning cycles among Iraqi insurgents are some 20 times as fast as the Irish Republican Army's were in Northern Ireland in the 1980s, according to military estimates....¹⁰⁹

108 Clay Shirky, *Cognitive Surplus* (New York: The Penguin Press, 2010), pp. 138-139.

109 Robert N. Charette, "Open-Source Warfare," *IEEE Spectrum*, November 2007
<<http://spectrum.ieee.org/telecom/security/opensource-warfare/0>>.

Open-source asymmetric warfare networks, by making ad hoc use of off-the-shelf technology, are able to develop weapons that rival in sophistication the products of years of military R&D. As Cory Doctorow notes, cheap technologies which can be modularized and mixed-and-matched for any purpose are just lying around. “[T]he market for facts has crashed. The Web has reduced the marginal cost of discovering a fact to \$0.00.” He cites Robb’s notion that “[o]pen source insurgencies don’t run on detailed instructional manuals that describe tactics and techniques.” Rather, they just run on “plausible premises.” You just put out the plausible premise—i.e., the suggestion based on your gut intuition, based on current technical possibilities, that something can be done—that IEDs can kill enemy soldiers, and then anyone can find out *how* to do it via the networked marketplace of ideas, with virtually zero transaction costs.

But this doesn’t just work for insurgents — it works for anyone working to effect change or take control of her life. Tell someone that her car has a chip-based controller that can be hacked to improve gas mileage, and you give her the keywords to feed into Google to find out how to do this, where to find the equipment to do it — even the firms that specialize in doing it for you.

In the age of cheap facts, we now inhabit a world where knowing something is possible is practically the same as knowing how to do it.

This means that invention is now a lot more like collage than like discovery.

Doctorow mentions Bruce Sterling’s reaction to the innovations developed by the protagonists of his (Doctorow’s) *Makers*: “There’s hardly any engineering. Almost all of this is mash-up tinkering.” Or as Doctorow puts it, it “assembles rather than invents.”

It’s not that every invention has been invented, but we sure have a lot of basic parts just hanging around, waiting to be configured. Pick up a \$200 FPGA chip-toaster and you can burn your own microchips. Drag and drop some code-objects around and you can generate some software to run on it. None of this will be as efficient or effective as a bespoke solution, but it’s all close enough for rock-n-roll.¹¹⁰

Murray Bookchin anticipated something like this back in the 1970s, writing in *Post-Scarcity Anarchism*:

Suppose, fifty years ago, that someone had proposed a device which would cause an automobile to follow a white line down the middle of the road, automatically and even if the driver fell asleep.... He would have been laughed at, and his idea would have been called preposterous.... But suppose someone called for such a device today, and was willing to pay for it, leaving aside the question of whether it would actually be of any genuine use whatever. Any number of concerns would stand ready to contract and build it. No real invention would be required. There are thousands of young men in the country to whom the design of such a device would be a pleasure. They would simply take off the shelf some photocells, thermionic tubes, servo-mechanisms, relays, and, if urged, they would build what they call a breadboard model, and it would work. The point is that the presence of a host of versatile, reliable, cheap gadgets, and the presence of men who understand all their cheap ways, has rendered the building of automatic devices almost straightforward and routine. It is no longer a question of whether they can be built, it is a question of whether they are worth building.¹¹¹

Among the practical results are the so-called “Assassin’s Mace” weapons, which simply take the same off-the-shelf components used by the state and make better use of them. The term initially appeared in the press in the context of cheap black boxes broadcasting on multiple frequencies and capable of disrupting the expensive American air-to-surface missiles which knock out SAM sites by homing in on radar signals. But it refers, more broadly, to all cases of ephemeralization where a countermeasure can knock out a weapons

110 Cory Doctorow, “Cheap Facts and the Plausible Premise,” *Locus Online*, July 5, 2009 <<http://www.locusmag.com/Perspectives/2009/07/cory-doctorow-cheap-facts-and-plausible.html>>.

111 Murray Bookchin, “Toward a Liberatory Technology,” in *Post-Scarcity Anarchism* (Berkeley, Calif.: The Ramparts Press, 1971), pp. 49-50.

system costing several orders of magnitude more: “asymmetric power... allow[s] cheap things to undo expensive ones.”

The Pentagon defines the Maces as technologies that might afford an inferior military an advantage in a conflict with a superior power. In this view, an Assassin’s Mace is anything which provides a cheap means of countering an expensive weapon. Other examples might include Chinese anti-satellite weapons, which might instantly knock out U.S. space assets, or a conventional ballistic missile, designed to take out a supercarrier and all its aircraft in one hit. It’s an interesting contrast to the perspective of the American arms industry, which can end up spending vast amounts countering low-tech, low-cost threats like mines and IEDs.¹¹²

IV. Systems Disruption

The dynamics of competition between networks and hierarchies lead to what John Robb calls “systems disruption.” Networks, despite much smaller resources than those which hierarchies can field, are able to leverage those resources through focused attacks on key nodes or weak points that achieve incapacitation many times greater than the apparent damage.

Because of their agility and the nature of network organization itself, they are able to route around damage much faster than hierarchies.

But perhaps the most important advantage of networks is the way hierarchies respond to attack. Hierarchies typically respond to network attacks by adopting policies that hasten their own destruction. Brafman and Backstrom stated the general principle, as we saw earlier, that “*when attacked, a decentralized organization tends to become even more open and decentralized.*” On the other hand, “*when attacked, centralized organizations tend to become even more centralized.*”¹¹³ Hierarchies respond to attacks by becoming even more hierarchical: more centralized, more authoritarian, and more brittle. As a result they become even less capable of responding flexibly to future attacks, actively suppressing their own ability to respond effectively.

Al Qaeda has adopted an explicit strategy of “open-source warfare,” using relatively low-cost and low-risk attacks, whose main damage will come not from the attacks but from the U.S. government’s reaction to them. In its slick English language e-zine *Inspire*, aimed at an American readership, it announced:

To bring down America we do not need to strike big. ...[With the] security phobia that is sweeping America, it is more feasible to stage smaller attacks that involve less players and less time to launch.

Robb, in the blog post from which the quote above was excerpted, cited additional material from *Inspire* on the thinking behind the recent parcel bomb attack:

Al Qaeda’s choice of a demonstration was to use parcel bombs (called **Operation Hemorrhage**—a classic name for a systems disruption attack). These low cost parcel bombs, were inserted into the international air mail system to generate a security response by western governments. It worked. The global security response to this new threat was massive....

Part of effective systems disruption is a focus on ROI (return on investment) calculations.¹¹⁴

112 David Hambling, “China Looks to Undermine U.S. Power, With ‘Assassin’s Mace,’” *Wired.com*, July 2, 2009 <<http://www.wired.com/dangerroom/2009/07/china-looks-to-undermine-us-power-with-assassins-mace/>>.

113 *Ibid.*, p. 139.

114 John Robb, “Open Source Jihad,” *Global Guerrillas*, November 21, 2010 <<http://globalguerrillas.typepad.com/globalguerrillas/2010/11/note-on-innovation-in-warfare.html>>.

And Al Qaeda, in its commentary at *Inspire*, made it clear that ROI calculations were very much on its mind:

Two Nokia phones, \$150 each, two HP printers, \$300 each, plus shipping, transportation and other miscellaneous expenses add up to a total bill of \$4,200. That is all what Operation Hemorrhage cost us... On the other hand this supposedly 'foiled plot', as some of our enemies would like to call [it], will without a doubt cost America and other Western countries billions of dollars in new security measures.¹¹⁵

Kevin Drum gives the example of a passenger flight forced to land—accompanied by a fighter jet—because the crew found a camera on board. The camera turned out to be perfectly normal and harmless, of course. And in any case, the fighter was useless—the plane hadn't been hijacked, and there's nothing it could have done about a bomb on board. So a flight was diverted and a fighter brought in, at enormous cost, for absolutely nothing. What's more, as Drum observes, this suggests a more cost-effective form of “terrorism”: “if al-Qaeda were smart, they'd recruit lots of sympathizers who weren't really ready for the whole suicide bomber thing and just have them leave cameras on board airplanes. It would tie up international air travel nicely.”¹¹⁶

And in fact Al Qaeda's deliberate strategy is pretty much to goad the U.S. into doing something stupid—usually a safe gamble. Security analyst Bruce Schneier coined the term “Post-Traumatic Stupidity Syndrome” to describe the way organizations overreact to events after the fact.¹¹⁷

Al Qaeda spokesman Adam Gadahn explicitly stated in a March 2010 video statement, that the U.S. government's response to “failed” attacks, and the resulting economic damage, was their whole point:

Even failed attacks can help the jihadists by "bring[ing] major cities to a halt, cost[ing] the enemy billions, and send[ing] his corporations into bankruptcy." Failed attacks, simply put, can themselves be successes. This is precisely why AQAP devoted an entire issue of *Inspire* to celebrating terror attempts that killed nobody.

All the other supposedly “failed” attacks on air travel have been resounding successes, by this standard. From Richard Reed's “shoe bomb” to the alleged liquid explosives in shampoo bottles, to the so-called “underwear bomber” on Christmas 2009, every single failed attack results in an enormously costly and reactive knee-jerk TSA policy—resulting in increased inefficiencies and slowdowns and ever more unpleasant conditions for travelers—to prevent that specific mode of attack from ever happening again. It doesn't matter whether it works or not. So we have to take off our shoes, leave our shampoo and bottled water at home—and most recently, choose between being ogled and groped. Every such new measure amounts to a new tax on air travel, and results in yet another small but significant group of travelers on the margin deciding it's the last straw. After the TSA required checked baggage to be screened, for example, air travel dropped by 6% between 4th Quarter 2002 and 1st Quarter 2003.¹¹⁸ Air travel on Thanksgiving 2010 was down about a tenth from the figure in 2009, which probably owes something to the public furor over the new body scanners and “enhanced patdowns.”

It's only a matter of time till some Al Qaeda cell is smart enough to allow one its agents to get “caught” with explosives in a bodily orifice, and—if TSA reacts according to pattern—the whole civil aviation system dissolves into chaos.

115 Quoted in Daveed Gartenstein-Ross, “Death by a Thousand Cuts,” *Foreign Policy*, November 23, 2010 <http://www.foreignpolicy.com/articles/2010/11/23/death_by_a_thousand_cuts>.

116 Kevin Drum, “Bomb Scares and Fighter Escorts,” *Mother Jones*, August 1, 2012 <<http://www.motherjones.com/kevin-drum/2012/08/bomb-scares-and-fighter-escorts>>.

117 Bruce Schneier, “This Week's Overreactions,” *Schneier on Security*, December 21, 2012 <http://www.schneier.com/blog/archives/2012/12/this_weeks_over.html>.

118 Nate Silver, “The Hidden Costs of Extra Security,” *Nate Silver's Political Calculus (NYT)*, November 18, 2010 <<http://fivethirtyeight.blogs.nytimes.com/2010/11/18/the-hidden-costs-of-extra-airport-security/>>

Hierarchies degrade their own effectiveness in another way, as well: by becoming less capable of preventing future attacks. 9/11, as Robb pointed out, was a Black Swan event: i.e., it was a one-off occurrence that could not have been predicted with any degree of confidence, and which is unlikely to be repeated. And most subsequent new kinds of attack, like the “shoe bomber” and “underwear bomber,” were of similar nature. Even when there is fairly high quality, actionable intelligence specifically pointing to some imminent threat, like the warning from the underwear bomber's uncle, the system is so flooded with noise that it doesn't notice the signal. Given the very large pool of individuals who are generally sympathetic to Al Qaeda's cause or who fit some generic “terrorist” personality profile, and given the very small number of people who are actively and deliberately involved in planning terror attacks, it's inevitable that genuinely dangerous suspects will be buried 99.9-to-0.1 in a flood of false positives. As Matt Yglesias argues,

Out of the six billion people on the planet only a numerically insignificant fraction are actually dangerous terrorists. Even if you want to restrict your view to one billion Muslims, the math is the same. Consequently, tips, leads and the like are overwhelmingly going to be pointing to innocent people. You end up with a system that's overwhelmed and paralyzed. If there were hundreds of thousands of al-Qaeda operatives trying to board planes every year, we'd catch lots of them. But we're essentially looking for needles in haystacks.¹¹⁹

...the key point about identifying al-Qaeda operatives is that there are extremely few al-Qaeda operatives so (by Bayes' theorem) any method you employ of identifying al-Qaeda operatives is going to mostly reveal false positives....

...If you have a 99.9 percent accurate method of telling whether or not a given British Muslim is a dangerous terrorist, then apply it to all 1.5 million British Muslims, you're going to find 1,500 dangerous terrorists in the UK. But nobody thinks there are anything like 1,500 dangerous terrorists in the UK. I'd be very surprised if there were as many as 15. And if there are 15, that means your 99.9 percent accurate method is going to get you a suspect pool that's overwhelmingly composed of innocent people. The weakness of al-Qaeda's movement, and the very tiny pool of operatives it can draw from, makes it essentially impossible to come up with viable methods for identifying those operatives.¹²⁰

The surveillance state responds to terror attacks by increasing the scope of its data collection in order to anticipate such events in the future. But in hoovering up larger and larger amounts of data, it simply increases the size of the haystack relative to the needle and exacerbates the problem of false positives.

The rising hay-to-needles ratio and the attendant problem of false positives becomes still worse when a growing share of needles remove themselves from the haystack through encryption. The quality of data available to the surveillance state is already skewed fairly heavily by this phenomenon, and every new high-profile story like the Snowden leaks and every successful arrest of a terror cell or crackdown on dissidents will result in further adoption of clandestine communications by groups with reason to fear the state.

The bulk of government surveillance efforts are “aimed at the sort of platforms and communication devices used by the general public—the sort of people who make use of the 'top level' because they actually have nothing to hide.” Leonid Bershidsky argues that

The infrastructure set up by the National Security Agency, however, may only be good for gathering information on the stupidest, lowest-ranking of terrorists. The Prism surveillance program focuses on access to the servers of America's largest Internet companies, which support such popular services as Skype, Gmail and iCloud. These are not the services that truly dangerous elements typically use.¹²¹

119 Matthew Yglesias, “Too Much Information,” *Think Progress*, December 28, 2009 <<http://yglesias.thinkprogress.org/2009/12/too-much-information/>>.

120 Yglesias, “Very Rare Terrorists are Hard to Find,” *Think Progress*, December 31, 2009 <<http://yglesias.thinkprogress.org/2009/12/very-rare-terrorists-are-very-hard-to-find/>>.

121 Tim Cushing, “Shallow Surveillance Efforts Like PRISM Will Only Catch The 'Stupidest, Lowest-Ranking Of Terrorists,’” *Techdirt*, June 25, 2013 <<https://www.techdirt.com/articles/20130624/18343523604/shallow-surveillance-efforts-like-prism-will-only-catch-stupidest-lowest-ranking-terrorists.shtml>>.

It's really common just common sense that those with something to hide—and anyone who has problems with the existing arrangement of corporate and state power has legitimate reason to fear the government—will be most likely to disappear from the surveillance state's radar. As Australian Crypto Party founder Asher Wolf noted, “those who want to break the law have already probably learnt cryptography.”¹²²

All of this together means that attempts to anticipate and prevent terror attacks through the bloated surveillance state, or to prevent attacks through standardized policies like shoe removal and “enhanced pat-downs,” amount to nothing more than an elaborate—but practically worthless—feel-good ritual. It's the placebo effect—or in Bruce Schneier's memorable phrase, “security theater.”

When your system for anticipating attacks upstream is virtually worthless, achieving defense in depth with the “last mile” becomes monumentally important: having people downstream capable of recognizing and thwarting the attempt, and with the freedom to use their own discretion in stopping it, when it is actually made. Since 9/11, all the major failed terror attacks in the U.S. were thwarted by the vigilance and initiative of passengers directly in contact with the situation. The underwear bomber was stopped by passengers who took the initiative to jump out of their seats and take the guy down. And the official response to every failed terror attack has been to further restrict the initiative and discretion of passengers in direct contact with the situation.

But if hierarchies are unable to keep us under adequate surveillance or adequately process the information, they are finding themselves crippled by the effects of *our* gaze. Thomas Knapp describes this asymmetrical relationship:

There are key asymmetries at work which yield huge advantages to the state's opponents.

Yes, states possess powerful surveillance capabilities, but those capabilities are centrally and hierarchically directed, and accessible only through relatively small and somewhat identifiable forces of operators. And they attempt to seek out and surveill what amount to straw-colored needles in a haystack of seven billion humans.

The world's networked resistance movements are those needles. It's much easier for the needle to see and identify the guy with the pitchfork than it is for the guy with the pitchfork to see and identify the needle. There are a lot more needles than there are guys with pitchforks. And the needles have access to their own set of tools — tools which are cheap, easy to use, and available to nearly anyone (including those aforementioned operators!) who might decide, at any time and for any reason, to become a needle.¹²³

Perhaps the best recent example of systems disruption is Wikileaks. A number of commentators have noted that the U.S. government's response to Wikileaks is directly analogous to the TSA's response to Al Qaeda attacks on civil aviation and the RIAA's response to file-sharing. For example Mike Masnick of *Techdirt*, in a juxtaposition of articles that probably wasn't coincidental (even the titles are almost identical), wrote on the same day that “the TSA's security policies are *exactly* what Al Qaeda wants,”¹²⁴ and that both the TSA and Wikileaks stories showed

how a system based on centralization responds to a (very, very different) distributed threat. And, in both cases, the expected (and almost inevitable) response seems to play directly into the plans of those behind the threat....

122 Asher Wolf, “Crypto Parties and How to Protect Your Data,” *World News Australia*, 2012 <<https://www.youtube.com/watch?v=uK6Cx7zxlDc>>.

123 Thomas Knapp, “The New Political Asymmetry: Nowhere to Run, Nowhere to Hide,” *Center for a Stateless Society*, February 8, 2013 <<http://c4ss.org/content/17078>>.

124 Mike Masnick, “How The US Response Turns 'Failed' Terrorist Attacks Into Successes,” *Techdirt*, December 2, 2010 <<http://www.techdirt.com/articles/20101130/03585512056/how-us-response-turns-failed-terrorist-attacks-into-successes.shtml>>.

...It's what happens when a centralized system, based on locking up information and creating artificial barriers, runs smack into a decentralized, open system, built around sharing. For those who are trying to understand why this whole story reminds me of what's happened in the entertainment industry over the past decade, note the similarities. It's why I've been saying for years that the reason I've spent so much time discussing the music industry is because it was an early warning sign of the types of challenges that were going to face almost every centralized industry or organization out there.¹²⁵

Assange's stated goal is to destroy or degrade the effectiveness of hierarchies, not through direct damage from attack, but by their own responses to attack.

The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. This must result in minimization of efficient internal communications mechanisms (an increase in cognitive "**secrecy tax**") and consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaptation.

Hence in a world where leaking is easy, secretive or unjust systems are **nonlinearly** hit relative to open, just systems. Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, mass leaking leaves them **exquisitely vulnerable to those who seek to replace them with more open forms of governance.**¹²⁶

Blogger Aaron Bady describes the double bind into which this imperative puts an authoritarian institution:

The problem this creates for the government conspiracy then becomes the organizational problem it must solve: if the conspiracy must operate in secrecy, how is it to communicate, plan, make decisions, discipline itself, and transform itself to meet new challenges? The answer is: by controlling information flows. After all, if the organization has goals that can be articulated, articulating them openly exposes them to resistance. But at the same time, failing to articulate those goals to itself deprives the organization of its ability to process and advance them. Somewhere in the middle, for the authoritarian conspiracy, is the right balance of authority and conspiracy.

This means that "the more opaque it becomes to itself (as a defense against the outside gaze), the less able it will be to "think" as a system, to communicate with itself."

The leak... is only the catalyst for the desired counter-overreaction; Wikileaks wants to provoke the conspiracy into turning off its own brain in response to the threat. As it tries to plug its own holes and find the leakers, he reasons, its component elements will de-synchronize from and turn against each other, de-link from the central processing network, and come undone.¹²⁷

Consider how the U.S. government's "information security" fetish hampered the efforts of the prosecution in the Chelsea Manning case. Email filters tasked with "preventing anything relating to Wikileaks from appearing on a government computer has tripped up military prosecutors, causing them to miss important emails from the judge and defense involved in the case..."¹²⁸

125 Masnick, "How The Response To Wikileaks Is Exactly What Assange Wants," *Techdirt*, December 2, 2010 <<http://www.techdirt.com/articles/20101202/02243512089/how-response-to-wikileaks-is-exactly-what-assange-wants.shtml>>.

126 Julian Assange, "The Non-Linear Effects of Leaks on Unjust Systems of Governance," December 31, 2006. Reproduced at Cryptome.org <<http://cryptome.org/0002/ja-conspiracies.pdf>>.

127 Aaron Bady, "Julian Assange and the Computer Conspiracy: 'To destroy this invisible government,'" *zunguzungu*, November 29, 2010 <<http://zunguzungu.wordpress.com/2010/11/29/julian-assange-and-the-computer-conspiracy-to-destroy-this-invisible-government/>>.

128 Josh Gerstein, "Blocking WikiLeaks emails trips up Bradley Manning prosecution," *Under the Radar* (Politico.com), March 15, 2012 <<http://www.politico.com/blogs/under-the-radar/2012/03/blocking-wikileaks-emails-trips-up-bradley-manning-117573.html>>.

So public embarrassment resulting from the cable leaks is not the end, but the means to the end. The end is not embarrassment, but the authoritarian state's reaction to such embarrassment:

...Assange is not trying to produce a journalistic scandal which will then provoke red-faced government reforms or something, precisely because no one is all that scandalized by such things any more. Instead, he is trying to strangle the links that make the conspiracy possible, to expose the necessary porousness of the American state's conspiratorial network in hopes that the security state will then try to shrink its computational network in response, thereby making itself dumber and slower and smaller.¹²⁹

The effect, a degrading of synaptic connections within the hierarchical organization, is analogous to the effect of Alzheimer's Disease on the human brain.

It happened after Manning's diplomatic cable dump to Wikileaks; the government tried to

cut off access to the leaked cables and even to outlets that *discussed* the leaked cables. At the Air Force, employees' computers were blocked from accessing more than 25 publications, including *The New York Times*, *Le Monde*, *Der Spiegel*, and, yes, *The Guardian*. No longer able to prevent information from reaching the public, the government instead attempted to prevent it from reaching itself.¹³⁰

It happened again after Edward Snowden's leaks of NSA documents.

The Army admitted Thursday to not only restricting access to The Guardian news website at the Presidio of Monterey, as reported in Thursday's Herald, but Armywide.

Presidio employees said the site had been blocked since The Guardian broke several stories on data collection by the National Security Agency.

Gordon Van Vleet, an Arizona-based spokesman for the Army Network Enterprise Technology Command...wrote it is routine for the Department of Defense to take preventative "network hygiene" measures to mitigate unauthorized disclosures of classified information.¹³¹

"No longer able to prevent information from reaching the public," *Reason* writer Jesse Walker quipped, "the government instead attempted to prevent it from reaching itself."¹³²

The NSA has responded by tightening up internally.

American leaders say they will avoid future Mannings and Snowdens by segmenting access to information so that individual analysts cannot avail themselves of so much, and by giving fewer security clearances, especially to employees of contractors such as Booz Allen Hamilton, where Snowden worked. This will not work. Segmentation of access runs counter to the whole point of the latest intelligence strategy, which is fusion of data from disparate sources. The more Balkanized the data, the less effective the intelligence. And, as Dana Priest and William Arkin make clear in their important book *Top Secret America*, intelligence agencies are collecting so much information that they have to hire vast numbers of new employees, many of whom cannot be adequately vetted. Since 9/11 the National Security Agency's workforce has grown by a third, to 33,000, and the number of private companies it relies on for contractors has tripled to close to 500. The more people know your secrets, the more likely it is they will leak out.¹³³

129 Bady, *op. cit.*

130 Jesse Walker, "Why a Government That Collects Everyone's Private Data Won't Let Its Employees Access Public Information," *Reason Hit & Run*, June 28, 2013 <<http://reason.com/blog/2013/06/28/why-a-government-that-collects-everyones>>.

131 Phillip Molnar, "Restricted web access to The Guardian is Armywide, officials say," *Monterey Herald*, June 27, 2013 <http://www.montereyherald.com/local/ci_23554739/restricted-web-access-guardian-is-army-wide-officials>.

132 "Why a Government That Collects Everyone's Private Data Won't Let Its Employees Access Public Information," *op. cit.*

133 Hugh Gusterton, "Not All Secrets Are Alike," *Bulletin of the Atomic Scientists*, July 23, 2013 <<http://www.thebulletin.org/not-all-secrets-are-alike>>.

John Boyd described the effect of degrading an adversary's internal communications in much the same way:

He who can generate many non-cooperative centers of gravity magnified friction. Why? Many non-cooperative centers of gravity within a system restrict interaction and adaptability of system with its surroundings, thereby leading to a focus inward (i.e., within itself), which in turn generates confusion and disorder, which impedes vigorous or directed activity, hence, by definition, magnifies friction or entropy.

Any command and control system that forces adherents to look inward, leads to dissolution/disintegration (i.e., system becomes unglued).¹³⁴

Noam Scheiber at *The New Republic* argues that Wikileaks "is, in effect, a huge tax on internal coordination. And, as any economist will tell you, the way to get less of something is to tax it. As a practical matter, that means the days of bureaucracies in the tens of thousands of employees are probably numbered."

There are two options for dealing with this. The first, to suppress leaks and tighten up internal control, is probably impossible in the long run. Which leaves the second option:

....to shrink. I have no idea what size organization is optimal for preventing leaks, but, presumably, it should be small enough to avoid wide-scale alienation, which clearly excludes big bureaucracies. Ideally, you'd want to stay small enough to preserve a sense of community, so that people's ties to one another and the leadership act as a powerful check against leaking. My gut says it's next to impossible to accomplish this with more than a few hundred people....

I'd guess that most organizations a generation from now will be pretty small by contemporary standards, with highly convoluted cell-like structures. Large numbers of people within the organization may not even know one another's name, much less what colleagues spend their days doing, or the information they see on a regular basis. There will be redundant layers of security and activity, so that the loss of any one node can't disable the whole network. Which is to say, thanks to Wikileaks, the organizations of the future will look a lot like ... Wikileaks.¹³⁵

Recall our discussion above of the "secrecy tax" which self-censorship and internal authoritarianism imposes on hierarchies. Robb, in *Brave New War*, refers to a "terrorism tax" on a city resulting from

an accumulation of excess costs inflicted on a city's stakeholders by acts of terrorism. These include direct costs inflicted on the city by terrorists (systems sabotage) and indirect costs because of the security, insurance, and policy changes needed to protect against attacks. A terrorism tax above a certain level will force the city to transition to a lower market equilibrium (read: shrink).

In particular, a "terrorism tax" of 6.3 to 7 percent will overcome the labor-pooling and transportation savings advantage of concentrating population sufficiently to compel the city to move to a lower population equilibrium.¹³⁶

Similarly, the excess costs imposed on hierarchies by the imperatives of conflict with hostile networks will act as a tax on them, compelling them to move to a lower size equilibrium. And increased levels of disobedience and disregard of government authority, and increased transaction costs of enforcing the law, will function as a disobedience tax. As a result, simply put, the advantages of hierarchy will be outweighed by the disadvantages at a lower size threshold. Large hierarchical institutions, both state and corporate, will become increasingly hollow, unable to enforce their paper claims to authority.

As Vinay Gupta argues, there's a close parallel between what networked efforts like Wikileaks want to do to large hierarchical institutions and what George Kennan envisioned the U.S. doing to the USSR.

134 John Boyd "Organic Design for Command and Control" (May 1987), pp. 20-21.

135 Noam Scheiber, "Why Wikileaks Will Kill Big Business and Big Government," *The New Republic*, December 27, 2010 <<http://www.tnr.com/article/politics/80481/game-changer>>.

136 Robb, *Brave New War*, p. 109.

And both are closely connected to Boyd's concept of the OODA loop.

The idea: there's an information theoretic model of conflict that runs through Kennan, Ogarkov, Boyd, Marshall, Assange. And that it's dominant.

Kennan writes the Long Telegram, thinks the Soviets will collapse because of crap information processing. Ogarkov sees only battle, agrees.

Assange paraphrased "we've become like the Soviets, which was Kennan's greatest fear, and we can beat our governments the same way."¹³⁷

In addition, as we will see later, hierarchies experience another kind of internal disunity in response to attack: moral.

Hierarchies are entering a very brutal period of natural selection, in which some will be supplanted from outside by networks, and some (those which survive) will become more network-like under outside pressure. The hierarchies which survive will be those which, faced with pressure from systems disruption, adapt (in Eric Raymond's phrase) by decentralizing their functions and hardening their local components. Hierarchies will face pressure to become less authoritarian internally, as they find themselves competing with networks for the loyalty of their workers. The power of exit will reinforce the power of voice.

David Ronfeldt, summarizing Michel Bauwens' view of the phase transition to p2p society, writes:

across history, from ancient to modern times, when a new form of organization has arisen in the context of older, stronger forms — “embedded” amid them — it makes sense for “hybrids” to emerge during phase transitions. Such hybrids combine actors from an era’s “dominant mode” of organization with actors representing an era’s emerging mode, in ways that benefit all partners to the hybrid, but that may also help subvert the old order and generate the new one. For the looming phase transition, this crucial interim role will be played by “netarchical capitalists” — e.g., Google (?) — who are willing to work with P2P commoners. Thus, in this view, phase transitions depend not so much on struggles between elites and masses, as on innovative alliances between break-away segments from the old system and adaptive segments from the emergent one...¹³⁸

So some large-scale infrastructures of the present corporate economy may take on a progressively network-like character, until they eventually so closely resemble networks as to make no real difference.

This natural selection process is inevitable, even without intentionally malicious attacks by networks on hierarchies. Raymond argues that the prevailing bureaucratic, hierarchical institutions of the 20th century were more or less workable, and capable of functioning based on Weberian rules and “best practices,” so long as the complexity of the problems they faced was not insupportable. Even in those days, of course, there were significant efficiency tradeoffs in return for control. In James Scott's terminology, rendering the areas managed by hierarchies “legible” to those at the top entailed a level of abstraction and oversimplification that severely limited the functionality of the leadership's understanding of the world. “The categories that they employ are too coarse, too static, and too stylized to do justice to the world that they purport to describe.”¹³⁹

And the process of rendering the functioning of the managed areas legible, through standard operating procedures and best practices, also entailed disabling or hindering a great deal of the human capital on which an organization depended for optimal functioning. The proper functioning of any organization depends heavily on what Friedrich Hayek called “distributed knowledge,” and what Michael Polanyi called

137 Vinay Gupta (as @leashless) on Twitter, 05:42 PM - 09 Feb 13 <<https://twitter.com/leashless/status/300298599122731008>>; 05:42 PM - 09 Feb 13 <<https://twitter.com/leashless/status/300298759433252865>>; 05:44 PM - 09 Feb 13 <<https://twitter.com/leashless/status/300299104817389569>>.

138 David Ronfeldt, “Bauwens’ “partner state” (part 3 of 3) . . . vis à vis TIMN,” *Visions From Two Theories*, October 19, 2011 <<http://twotheories.blogspot.com/2011/10/bauwens-partner-state-part-3-of-3-vis.html>>.

139 James C. Scott, *Seeing Like a State*, p. 262.

“tacit knowledge.” It is direct, practical knowledge of the work process, which cannot be reduced to a verbal formula and transmitted apart from practical experience of the work. It is also practical knowledge of the social terrain within the organization, and the network of personal relationships it's necessary to navigate in order to get anything done. Scott uses the Greek term *metis*, as opposed to *techne*. Bureaucratic micro-management, interference, and downsizing, between them, decimate the human capital of the organization¹⁴⁰—much like the eradication of social memory in elephant herds where a large enough portion of the elderly matriarchs have been destroyed to disrupt the transmission of social mores.

For all these efficiency losses, from the hierarchy's perspective they are necessary trade-offs for the sake of acquiring and maintaining power. Reality must be abstracted into a simple picture, and specialized knowledge known only to those actually doing the work must be eradicated—not only to make the organization simple enough to be manageable by a finite number of standard rules, but because the information rents entailed in tacit/distributed knowledge render the lower levels less easily milked.

The state, like a demon, is bound by the laws and internal logic of the form it takes. When a segment of the bureaucracy is captured by its own ideological self-justification, or courts by the letter of the law they pretend to enforce, they can be used as a weapon for monkey-wrenching the larger system. Bureaucrats, by following the letter of policy, often engage in de facto “work-to-rule” against the larger system they serve.

The state, like any authoritarian hierarchy, requires standing rules that restrict the freedom of subordinates to pursue the institution's real purpose, because it can't trust those subordinates. The state's legitimizing rhetoric, we know, conceals a real exploitative function. Nevertheless, despite the overall functional role of the state, it needs standard operating procedures to enforce predictable behavior on its subordinates.

And once subordinates are following those rules, the state can't send out dog-whistles telling functionaries what “real” double-super-secret rules they're “really” supposed to follow, or to supplement the countless volumes of rulebooks designed to impose predictability on subordinates with a secret memo saying “Ignore the rulebooks.” So, while enough functionaries may ignore the rules to keep the system functioning after a fashion, others pursue the letter of policy in ways that impair the “real” mission of the state.

Unlike the state and other authoritarian institutions, self-organized networks can pursue their real interests while benefiting from their members' complete contribution of their abilities, without the hindrance of standard operating procedures and bureaucratic rules based on distrust. To put it in terms of St. Paul's theology, networks can pursue their interests single-mindedly without the concupiscence — the war in their members — that weakens hierarchies.

So we can game the system, sabotaging the state with its own rules — what's called “working to rule” in labor disputes.

But today, the complexity of problems faced by society has become so insupportable that hierarchies are simply incapable of even passably coping with it. As Scott points out, the policies of bureaucratic hierarchies have always been made by people who “ignore the radical contingency of the future” and fail to account for the possibility of incomplete knowledge.¹⁴¹ But contingency and incompleteness have increased exponentially in recent years, to levels with which only a stigmergic organization can cope.

Raymond argues that the level of complexity in American society, in the mid-20th century, was such that it could be managed—if not effectively, at least more or less adequately—by the meritocratic managerial classes using Weberian-Taylorist rules to govern large bureaucratic organizations. But if Gosplan and Bob

140 *Ibid.*, pp. 334-337.

141 *Ibid.*, pp. 343-344.

McNamara could manage to stumble along back then, the level of unsupportable complexity in recent decades has outstripped the ability of hierarchical, managerial organizations to manage.¹⁴²

Meanwhile, hierarchies' responses to network attacks are self-destructive in another way besides the "secrecy tax." They undermine their own perceived legitimacy in the eyes of the public. For one thing, they undermine their moral legitimacy by behaving in ways that directly contradict their legitimizing rhetoric. As Martin van Creveld argued, when the strong fight the weak they become weak—in large part because the public can't stomach the knowledge of what goes into their sausage. The public support on which the long-run viability of any system of power depends is eroded by loss of morale.

The reason is that when the strong are seen beating the weak (knocking down doors, roughing up people of interest, and shooting ragtag guerrillas), they are considered to be barbarians. This view, amplified by the media, will eventually eat away at the state's ability to maintain moral cohesion and drastically damage its global image.¹⁴³

We saw this with the public reaction to Abu Ghraib and Guantanamo. And every video of an Israeli bulldozer flattening a Palestinian home with screaming mother and children outside undermines the "beleaguered Israeli David vs. Arab Goliath" mystique on which so much third party support depended. The "David vs. Goliath" paradigm is replaced by one of the Warsaw Ghetto vs. the Nazis, with the Israelis in the role of bad guys.

But more importantly, networked resistance undermines the main source of legitimacy for all authoritarian institutions, which is their "plausible premise"—their ability to deliver the goods in return for loyalty and compliance. Every attack against a hierarchy, to which it demonstrates its inability to respond effectively, undermines its grounds for expecting loyalty. It's one thing to sell one's soul to the Devil in return for a set of perks. But when the Devil is unable to deliver the goods, he's in trouble.

[Draft last modified November 27, 2015]

142 Eric Raymond, "Escalating Complexity and the Collapse of Elite Authority," *Armed and Dangerous*, January 5, 2010 <<http://esr.ibiblio.org/?p=1551>>.

143 John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (Hoboken: John Wiley & Sons, 2007), p. 28.