Chapter Three

Networks vs. Hierarchies: The Endgame

I. The Transition from Hierarchies to Networks

To the extent that hierarchies and networks are the characteristic social formations of two successive social systems, the process of transition—like those from the Western Roman Empire to feudalism, and from feudalism to capitalism—itself becomes a subject for study.

It's fairly common to observe that peer-to-peer organization is the nucleus, or dominant mode of production, in a new post-capitalist social formation. That's the premise of the Marxist Oekonux email discussion list: that open-source, commons-oriented peer production is the kernel of a post-scarcity communist society.

The control of information is the central axis of struggle over the control of production; giant corporations control of the global economy, more than anything, depends on enclosure of information. And, as Alistair Davidson argues, the free culture or hacker communities—which base their struggle against corporate power on the struggle for freedom of information—is the nucleus of the future resistance.

> Despite blanket media coverage of Wikileaks and Julian Assange, there has been little discussion of the fact that Assange is merely one leader within a large and complicated social movement. The better analyses have found it interesting that the Swedish Pirate Party are aiding Wikileaks; some note links to the German Chaos Computer Club. But only “geeks” and “hackers” (technology workers) are aware that all of these organisations are members of the same movement.
>
> This social movement, which has been termed the “free culture movement”, has a thirty year history. It incorporates elements reminiscent of earlier workers’ movements: elements of class struggle, political agitation, and radical economics. The movement’s cadre, mainly technology workers, have been locked in conflict with the ruling class over the political and economic nature of information itself.[1]

This new conflict within capitalism—“between the path of greatest production (infinite copying) and the existing source of profits (artificial scarcity)”—was the latest example of Marx's conflict between old and new modes of production.[2]

Stallman's free software movement illustrates what peer production means as a new mode of production: "information workers... owned their means of production and had access to the means of distribution—by the 1980s, all they needed to bypass capital entirely was a computer and a phone line.”[3]

Davidson sets aside the facile debate over whether the Internet was created by the state or the market, and quotes Steven Johnson that it is actually the first large-scale artifact of peer production:

> So was the Internet created by Big Government or Big Capital? The answer is: Neither.

[1] Alistair Davidson, “Wikileaks, Karl Marx and You,” *Moh Kohn*, January 7, 2011 <http://mohkohn.wordpress.com/2011/01/ 07/wikileaks-karl-marx-and-you/>.

[2] *Ibid.*

[3] *Ibid.*

> Peer networks break from the conventions of states and corporations in several crucial respects. They lack the traditional economic incentives of the private sector: almost all of the key technology standards are not owned by any one individual or organization, and a vast majority of contributors to open-source projects do not receive direct compensation for their work. (The Harvard legal scholar Yochai Benkler has called this phenomenon “commons-based peer production.”) And yet because peer networks are decentralized, they don’t suffer from the sclerosis of government bureaucracies.[4]

Writers like James Livingston and Michel Bauwens have explicitly drawn on previous transitions as models for the hierarchy-network transition. Although our political culture, both Right and Left, envisions a post-capitalist transition through the lens of the French and Russian revolutions—abrupt, insurrectionary, and equated largely to the seizure of the state—there's no reason to assume it will be. It could just as easily be a decades-long, relatively gradual process like the decay of the Western Roman Empire and of feudalism. Livingston writes:

> What happens when we stop looking for socialism in all the wrong places?
>
> Start here. When we think about the transition from feudalism to capitalism, we take the long view – we scan the four centuries from 1400 to 1800, looking for signs of fundamental but incremental change. To be sure, we assume that the great bourgeois revolutions of the seventeenth, eighteenth, and nineteenth centuries were both symptoms and causes of this transition.... Still, we know these early modern movements can’t be compared to the communist parties that created state socialism in twentieth-century Russia, China, and Cuba, because in these more recent instances, self-conscious revolutionaries organized workers and peasants to overthrow capitalism and create socialism....
>
> In short, capitalism was the *unintended consequence* of bourgeois revolutions, whereas socialism has been the avowed purpose, or at least a crucial component, of every revolution since 1911....
>
> ….We don’t measure the transition from feudalism to capitalism only by assessing the social origins and political-economic effects of bourgeois revolutions – we’d have to be daft to do so. Instead we ask when, how, where, and why social relations were transformed, over many years, so that a new mode of production and new modes of consciousness, emerged to challenge (if not supplant) the old. Or rather..., we ask *when* capitalism became the hegemonic mode in a mongrel social formation that contained fragments of a residual feudalism and harbingers of a precocious socialism. We don’t think that capitalism was created overnight by revolutionary parties....
>
> Why, then, would we look for evidence of socialism only where a state seized by radicals of the Left inaugurates a dictatorship of the proletariat? Or, to lower the rhetorical volume and evidentiary stakes, why would we expect to find socialism only where avowed socialists or labor parties contend for state power? We should instead assume that socialism, like capitalism, is a cross-class cultural construction, to which even the bourgeoisie has already made significant contributions – just as the proletariat has long made significant contributions to the cross-class construction we know as capitalism. What follows?...
>
> We typically assume that socialism is something signified by state command of civil society, rather than the other way around. Why? Why do we assume, in other words, that markets and socialism don’t mix, that private enterprise and public goods – commutative and distributive justice – are always at odds? And why do we think, accordingly, that socialism must repudiate liberalism and its attendant, modern individualism, rather than think, with Eduard Bernstein and Sidney Hook, that socialism is their rightful heir?
>
> Let’s uproot our assumptions, in keeping with our radical calling. Let’s look for the evidence of socialism in the same places we’ve always looked for the evidence of capitalism: in changing social relations of production *as well as* legislative acts and political actions, in the marketplace of ideas *as well as* porkbellies, in everyday life and popular culture *as well as* learned assessments of the American Dream, in uncoordinated efforts to free the distribution of information and music – the basic industries

[4] Johnson, “We Built That,” quoted in Alistair Davidson, “Peer Production: A New Economic Dawn?” *Moh Kohn*, September 25, 2012 <http://mohkohn.wordpress.com/2012/09/25/peer_production/>.

> of a postindustrial society – from the "business model" quotes of the newspapers and record companies *as well as* social movements animated by anticapitalist ideas....[5]

The 500-odd-year-old capitalist system, like previous historic systems,is not a monolithic unity, but a collection of mutually interacting social formations—some in ascendancy, some in decline. It follows that the supplanting of capitalism need not involve a dramatic rupture on the part of a monolithic unity of progressive forces. As Eugene Holland argues,

> the requirement of such a radical systemic break is necessary only when you conceive of a society or mode of production as a total system in the first place.... Construing such elements in terms of dominant, residual, and emergent improves utopian prospects considerably, inasmuch as there would presumably be positive elements to affirm (the "emergent" ones) alongside the negative ones to critique and reject (presumably all the "dominant" ones)....[6]

Ultimately the situation is resolved when the forces of the old order attempt—and fail—to thwart the transition.

> ...our current situation is propitious... because the constituent power of the multitude has matured to such an extent that it is becoming able, through its networks of communication and cooperation, through its production of the common, to sustain an alternative democratic society on its own. Here is where the question of time becomes essential. When does the moment of rupture come?... Revolutionary politics must grasp, in the movement of the multitudes and through the accumulation of common and cooperative decisions, the moment of rupture... that can create a new world.[7]

But however abrupt and dramatic the final rupture may seem, it is only the culmination of a long preexisting process of "building the structure of the new society within the shell of the old."

> Following 1640, 1776, 1789, 1848, 1917, and 1949, we have been fixated on the image of revolution—of punctual, violent, wholesale transformation—as the most desirable (and often the only acceptable) mode of social change. But revolution is not the only mode of social transformation: feudalism, for instance, arose piecemeal following the decline of the Roman Empire, in a process that took centuries to complete.... Immediate and total social transformation of the revolutionary kind is not absolutely necessary for a number of reasons, not the least of which is that capitalism is not a total system to begin with. Alternatives are not only always possible, they in fact already exist. Inasmuch as the secret of so-called primitive accumulation is that it is actually first and foremost a process of dispossession—ongoing as well as primitive—one answer proposed by affirmative nomadology to the question of what is to be done is thus to initiate a slow-motion general strike. Seek out actually existing alternative modes of self-provisioning—they are out there, in Remarkable number and variety—and also develop new ones; walk away from dependence on capital and the State, one step, one stratum, at a time, while at the same time making sure to have and continually develop alternative practices and institutions to sustain the movement. To effectively replace capitalism and the State, a slow-motion general strike must indeed become-general or reach critical mass or bifurcation point eventually, but it doesn't have to be all encompassing right from the beginning or produce wholesale social change all at once: it can start off small and/or scattered and become-general over time (in much the same way that capitalism starts small and gradually becomes-necessary, in Althusser's view).
>
> Hegemonic thinking (i.e., thinking that social change is always and only a matter of hegemony), [Richard] Day argues, leads to the double impasse of "revolution or reform": given its totalizing view of society, one must either seek the total and utter demolition of that society through revolution or settle for piecemeal reforms that ultimately have no decisive effect on it. But society is not a totality: it is a

[5] James Livingston, "How the Left Has Won," *Jacobin*, August 2012 <http://jacobinmag.com/2012/08/how-the-left-has-won/>.

[6] Holland, *Nomad Citizenship*, p. 169.

[7] Michael Hardt and Antonio Negri, *Multitude: War and Democracy in the Age of Empire* (New York: Penguin, 2004), p. 357.

> contingent assemblage, or assemblage of assemblages. Nomad citizenship thus proposes, in Day's terms, a variety of "small-scale experiments in the construction of alternative modes of social, political and economic organization [as] a way to avoid both waiting forever for the Revolution to come and perpetuating existing structures through reformist demands." For Day, finally, as for affirmative nomadology, what is Important is to create alternatives to abject dependency on capital and the State....[8]
>
> ...[T]he key difference between every ordinary strike and the general strike is that while the former makes demands on capitalist employers, the latter simply steps away from capital altogether and—if it is to succeed—moves in the direction of other form(s) of self-provisioning, enabling the emergence of other form(s) of social life—for example, nomad citizenship and free-market communism.
>
> ...[T]he slow-motion general strike is, in an Important sense, neither reformist nor revolutionary. It does not employ violence in direct confrontation with the capitalist State and is therefore unlikely to provoke State violence in return, yet neither does it rely on and thereby reinforce the existing practices and institutions of capital and the State....
>
> ...Vital to the success of a slow-motion general strike is its sustainability: the unrelenting process of dispossession of capital known as *primitive accumulation* must actually be reversed....[9]

John Holloway argues similarly that the post-capitalist transition will be an "interstitial process" like that from feudalism to capitalism.[10]

The post-capitalist class formation will be one in which commons governance, horizontal networks and p2p organization will replace the corporate-state nexus as the core, with markets and administration persisting in reduced, peripheral form and characterized by their relationship to networks. As Michel Bauwens argues:

> emerging peer production has a core of non-market mechanisms, with markets operating around the commons where the knowledge, code or design is deposited; moreover, I believe that the mutual coordination and stigmergy that is characteristic of immaterial production projects, will expand to material production through open supply chains and open book management, further diminishing the relative part of market dynamics.[11]

Commons-based peer production, as an alternative to both the capitalist corporation and the state, enables

> the direct social production of use value, through new life practices that are largely outside the control of capital, and with means of production which have been socialized to a very significant degree. These new processes are post-capitalist rather than capitalist, in the sense that they no longer need any specific role of capital for their reproduction.[12]

David Ronfeldt, in the context of his TIMN (Tribes, Institutions, Markets and Networks) framework, describes it as "coexistent layering."[13] Elsewhere, writing of Bauwens' conceptual schema, Ronfeldt says that the ascendancy of networks and p2p organization will disproportionately benefit and strengthen civil soci-

[8] Eugene Holland, *Nomad Citizenship: Free-Market Communism and the Slow-Motion General Strike* (Minneapolis: University of Minnesota Press, 2011), pp. 149-150.

[9] *Ibid.*, pp. 155-156.

[10] Jerome Roos, "Talking About a Revolution With John Holloway," *John Holloway*, April 13, 2013 <http://www.johnholloway.com.mx/2013/05/01/talking-about-a-revolution-with-john-holloway/>.

[11] Michel Bauwens, "Do we need p2p to help markets deal with complexity, or does p2p get us beyond markets?" *P2P Foundation Blog*, December 12, 2012 <http://blog.p2pfoundation.net/do-we-need-p2p-to-help-markets-deal-with-complexity-or-does-p2p-get-us-beyond-markets/2012/12/10>. Reproduced from a Facebook debate with John Robb, Franz Nahrada, Fabio Barone and Chris Cook.

[12] Bauwens, "Interview on Peer to Peer Politics with Cosma Orsi," *P2P Foundation Blog*, April 10, 2008 <http://blog.p2pfoundation.net/interview-on-peer-to-peer-politics-with-cosma-orsi/2008/04/10>.

[13] David Ronfeldt, "Q's & A's about "TIMN in 20 minutes" (2nd of 7): nature of the forms and their relationships," *Visions From Two Theories*, October 8, 2012 <http://twotheories.blogspot.com/2012/10/qs-as-about-timn-in-20-minutes-2nd-of-7.html>.

ety, and profoundly alter older state and market institutions forced to accommodate themselves to a society in which the network form increasingly shapes the character of all functions.[14]

According to Michael Hardt and Antonio Negri, the relationship between the dominant class is the opposite of that Hobbes described at the dawn of the modern era. The "nascent bourgeoisie"

> was not capable of guaranteeing social order on its own; it required a political power to stand above it.... The multitude, in contrast to the bourgeoisie and all other exclusive, limited class formations, is capable of forming society autonomously....[15]

Another thing to keep in mind is that the large-scale transition may take place as a comparatively sudden phase change, but only after the ground has been prepared by a prolonged Gramscian “war of position” in civil society. As Jay Ufelder puts it, “revolutionary situations [are] an emergent property of complex systems.”

> One of the features of complex systems is the possibility of threshold effects, in which seemingly small perturbations in some of the system’s elements suddenly produce large changes in others. The fragility of the system as a whole may be evident (and therefore partially predictable) from some aspects of its structure, but the timing of the revolutionary moment’s emergence and the specific form it will take will be impossible to anticipate with any precision.
>
> In this version of politics, the emergence of rival organizations is as likely to be a consequence of the system’s failure as a cause of it.[16]

New Wine in Old Bottles.

[Insert intro on pseudomorph, reorganize subsequent material accordingly]

The transition period is characterized by the attempts of hierarchical institutions to coopt the potential of networked organization for their own benefit. As Andy Robinson describes it:

> ...[E]ver since the 70s the system has been trying to find hybrids of network and hierarchy which will harness and capture the power of networks without leading to "chaos" or system-breakdown. We see this across a range of fields: just-in-time production, outsourcing and downsizing, use of local subsidiaries, contracting-out, Revolution in Military Affairs, full spectrum dominance, indirect rule through multinational agencies, the Nixon Doctrine, joined-up governance, the growing importance of groups such as the G8 and G20, business networks, lifelong learning, global cities, and of course the development of new technologies such as the Internet....
>
> In the medium term, the loss of power to networks is probably irreversible, and capital and the state will either go down fighting or create more-or-less stable intermediary forms which allow them to persist for a time. We are already seeing the beginnings of the latter, but the former is more predominant. The way I see the crisis deepening is that large areas will drift outside state and capitalist control, integrated marginally or not at all (this is already happening at sites such as Afghanistan, NWFP, the Andes, Somalia, etc., and in a local way in shanty-towns and autonomous centres). I also expect the deterritorialised areas to spread, as a result of the concentration of resources in global cities, the ecological effects of extraction, the neoliberal closing of mediations which formerly integrated, and the growing stratum of people excluded either because of the small number of jobs available or the growing set of requirements for conformity. Eventually these marginal spaces will become sites of a proliferation of new forms of living....[17]

[14] Ronfeldt, “Updates about missing posts (3rd of 5): Bauwens’ 'partner state' (part 2 of 3) … vis à vis TIMN,” *Visions From Two Theories*, April 3 <http://twotheories.blogspot.com/2014/04/updates-about-missing-posts-3rd-of-5.html>.

[15] Michael Hardt and Antonio Negri, *Multitude: War and Democracy in the Age of Empire* (New York, 2004), xvii-xviii.

[16] Jay Ufelder, “ISO Revolution, Organized Opposition Not Req’d,” *Dart-Throwing Chimp*, September 7, 2012 <http://dartthrowingchimp.wordpress.com/2012/09/07/iso-revolution-organized-opposition-not-reqd/>.

[17] Andy Robinson, “[p2p research] Berardi essay,” P2P Research email list, May 25, 2009 <http://listcultures.org/pipermail/p2presearch_listcultures.org/2009-May/003079.html>.

Hybrid efforts include attempts by corporate business enterprises to incorporate network elements through such fads as the Wikified Firm and Enterprise 2.0, while using artificial property rights to coopt the networks for their own purposes. They also include projects like "network-centric warfare"—an attempt by the American conventional military establishment to coopt the advantages of networked guerrilla organizations like Al Qaeda Iraq.

Unfortunately for them, in both military and business affairs, such attempts usually fail despite the understanding of their designers because their implementation depends on traditional hierarchies that are jealous of threats to their prerogatives. We see the same result in all areas of life, when hierarchies attempt to incorporate network elements. No matter how well the theorists understand the need to become more network-like, the people actually running the hierarchies are simply unable to keep their hands off.

In the business case, there's an intense Darwinian selection process going on. A small minority of corporations may become network-like enough to survive. But if they find themselves still alive at the end of the transition, they will likely have become so network-like as to be p2p organizations for all intents and purposes, regardless of what legacy name appears on their letterhead. The great majority of corporate hierarchies which fail to transform themselves into networks—which will likely be the vast majority of large corporations—will die.

There are a thousand and one management theory fads out there about flattening hierarchies, self-management, empowerment, and all the rest of it. To give some idea of how hollow it is Bill Gates himself, back in 2004, celebrated the use of blogs as an internal collaborative tool within the corporation.[18] But because the theories are put into practice by bosses, in every case they wind up looking like warmed-over Taylorism.

The problem is that, even if it's necessary to incorporate network methods into a corporate hierarchy, it's not sufficient. According to Harold Jarche, enterprise social tools are necessary to

> enable faster feedback loops inside the organization in order to deal with connected customers, suppliers, partners, and competitors. It takes a networked organization, staffed by people with networked mindsets, to thrive in a networked economy.

But even so, the simulated networked organization inside the corporation isn't as agile as a genuine self-organized network.

> Enterprise knowledge sharing will never be as good as what networked individuals can do. Individuals who own their knowledge networks will invest more in them. I think this means that innovation outside of organizations will continue to evolve faster than inside.[19]

Euan Simple describes how the failure of corporate management to grasp what Enterprise 2.0 is about will sabotage efforts to implement it.

- They'll think it's about technology.
- They're not prepared to deal with the friction generated from allowing their staff to connect.
- They'll assimilate it into business as usual.
- They'll try to do it in a way that 'maximises business effectiveness' without realising that it calls for a radical shift in what's seen as effective.
- They'll grind down their early adopters until they give up.
- They'll get fleeced by the IT industry for over-engineered, under-delivering solutions, thinking that Enterprise 2.0 failed to live up to its promise and move on to the next fad....

[18] "Gates Backs Blogs for Businesses," *BBC News*, May 21, 2004 <http://news.bbc.co.uk/2/hi/technology/3734981.stm>.

[19] Harold Jarche, "The Knowledge-Sharing Paradox," *Life in Perpetual Beta*, March 24, 2013 <http://www.jarche.com/2013/03/the-knowledge-sharing-paradox/>.

- It is individuals, not companies who do Enterprise 2.0.[20]

In the military case, official military doctrines for fourth-generation warfare like the U.S. DOD's "network-centric warfare" are aimed at copying the resilience and flexibility of networked adversaries like Al Qaeda. This means, according to John Robb, taking advantage of the possibilities new communications technology offers to "enable decentralized operation due to better informed people on the ground."[21]

Network-centric warfare dates to a 1998 article by Vice Admiral Arthur Cebrowski and John Garstka, and was described not long afterward as

> an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[22]

The DOD's "Transformation Planning Guidance" in April 2003 called for transforming US military forces into

> Information age military forces [that] will be less platform-centric and more network-centric. They will be able to distribute forces more widely by increasing information sharing via a secure network that provides actionable information at all levels of command. This, in turn, will create conditions for increased speed of command and opportunities for self-coordination across the battlespace.[23]

But no matter how sensible (or even brilliant) the doctrines churned out by 4GW experts in the academies, as applied by the military bureaucracy they mean using the technology instead "to enable more complicated and hierarchical approval processes—more sign offs/approvals, more required processes, and higher level oversight."

> Risk mitigation trumps initiative every time. Careers are more important than victory. Risk evaluation moves upward in the hierarchy. Evaluation of risk takes time, particularly with the paucity of information that can be accessed at positions removed from the conflict.[24]

According to Thomas Hammes, the DOD guidance notwithstanding the actual process of information distribution within the military bureaucracy was still far different in 2004.

> Our advanced information systems are still tied to an outdated, hierarchical organization that slows the dissemination of information. Although specific high-priority commands receive near real-time intelligence, most commanders must submit their intelligence requirements up the chain of command. Each level validates, consolidates, and prioritizes the requests, which are then fed through the centralized staff system to task the assets that will actually collect against the requests. The information is collected, passed to another section for analysis, then put in the form of a usable product, and finally disseminated through the same cumbersome system. Thus, the premier benefit of the Information Age--immediate access to current intelligence--is nullified by the way we route it through our vertical bureaucracy.

[20] Alan Moore, *No Straight Lines: Making Sense of Our Non-Linear World* (Cambridge, England: Bloodstone Books, 2011), p. 90.

[21] John Robb, "Fighting an Automated Bureaucracy," *Global Guerrillas*, December 8, 2009 <http://globalguerrillas.typepad.com/globalguerrillas/2009/12/journal-fighting-an-automated-bureaucracy.html>.

[22] "The Road to Riches," The Economist, Millennium special edition, January 1, 1000-December 31, 1999; quoted in Thomas Hammes, *The Sling and the Stone: On War in the 21st Century* (Saint Paul, Minn.: Zenith Press, 2004), p. 7.

[23] Quoted in Hammes, pp. 8-9.

[24] Robb, "Fighting an Automated Bureaucracy."

> Not only does our bureaucracy delay the distribution of the intelligence products we develop, it actively discourages subordinate units from tapping into the information themselves, via the Internet. The result is a limiting of the variety and timeliness of the information available to our decision makers, from the strategic to the tactical levels.[25]

And it still hadn't changed much in 2009. Afghan War veteran Jonathan Vaccaro, in a *NYT* op-ed, describes the bureaucratic nightmare in detail:

> ...Our answer to Afghans seeking help was: "I can't come today or tomorrow, but maybe next week. I have several bosses that I need to ask for permission."...
>
> In my experience, decisions move through the process of risk mitigation like molasses. When the Taliban arrive in a village, I discovered, it takes 96 hours for an Army commander to obtain necessary approvals to act. In the first half of 2009, the Army Special Forces company I was with repeatedly tried to interdict Taliban. By our informal count, however, we (and the Afghan commandos we worked with) were stopped on 70 percent of our attempts because we could not achieve the requisite 11 approvals in time.
>
> For some units, ground movement to dislodge the Taliban requires a colonel's oversight. In eastern Afghanistan, traveling in anything other than a 20-ton mine-resistant ambush-protected vehicle requires a written justification, a risk assessment and approval from a colonel, a lieutenant colonel and sometimes a major. These vehicles are so large that they can drive to fewer than half the villages in Afghanistan. They sink into wet roads, crush dry ones and require wide berth on mountain roads intended for donkeys. The Taliban walk to these villages or drive pickup trucks.
>
> The red tape isn't just on the battlefield. Combat commanders are required to submit reports in PowerPoint with proper fonts, line widths and colors so that the filing system is not derailed....
>
> Communication with the population also undergoes thorough oversight. When a suicide bomber detonates, the Afghan streets are abuzz with Taliban propaganda about the glories of the war against America. Meanwhile, our messages have to inch through a press release approval pipeline, emerging 24 to 48 hours after the event, like a debutante too late for the ball.[26]

The internal opacity and paralysis of the military's information culture only became worse after the leaks by Manning and Snowden.

The information culture of Al Qaeda, in contrast, is classically stigmergic and permissionless, and characterized by individual super-empowerment based on freely available open platforms:

> Potential enemies are not hampered by an entrenched bureaucracy. They are free to exploit the full range of commercially available information technology. They can use the rapidly expanding worldwide information system to collect information, store it on web sites, collaborate on analysis, and direct attacks on our interests....
>
> ...Remember that much of the commercial technology available today is an outgrowth of the military systems designed specifically to collect and defend against conventional forces. Even small cells can exploit the information revolution to collect against our forces. A group trying to track U.S. forces can watch CNN or a dozen other news agencies for live footage of the movement of our forces from home bases--and often even in theater. They can tap into a wide variety of commercial satellite imaging services--many with resolution of less than one meter. These photos can be used to track our ships, identifying changes in our ports, as well as arrival and assembly areas....
>
> In addition they can get worldwide weather reports. They can conduct online research in port usage, shipping insurance rates (to indicate perception of threat by business), gauge market reaction to current events, and even watch our leaders express their positions to members of the media. Anyone with a computer, a modem, and a credit card is limited only by his own imagination and intelligence in developing information from the political level to the tactical....

[25] Hammes, *The Sling and the Stone*, pp. 192-193.

[26] Jonathan Vaccaro, "The Next Surge—Counterbureaucracy," *New York Times*, December 7, 2009 <http://www.nytimes.com/2009/12/08/opinion/08vaccaro.html>.

> Even more important for using 4GW techniques, today's terrorists are organized as networks rather than as hierarchies. This means that each entity can use the network simultaneously, searching for and receiving the information he is interested in without having to work through a bureaucracy. Ask yourself which you would rather have as a tactical commander: a one-meter resolution image from a commercial source hours after you request it or a high-resolution image from one of our national systems days after you request it. Even more important, the insurgent knows what he can and cannot get. The U.S. commander has to submit his request and wait to see if it can be filled--further delaying his decision cycle....
>
> ...[A]n adept terrorist simply uses the existing networks created by the information-based economy....[27]

The management fad of "disruptive innovation" in recent years is a good illustration of the problems facing hierarchies that try to change themselves internally to adapt to a networked world. It should really be no surprise that established corporations that hire a Chief Disruption Officer and give Disruption badges and coffee mugs to everybody at their management retreat would totally fuck it up. Corporations always fail when they try to incorporate good ideas into the framework of a managerial hierarchy. They do so because they're putting new wine into new bottles, and because the kinds of policies that make for agility and resilience are directly at odds with the privileges and power of the managerial hierarchy.

But more than that, managerial hierarchies are unable to anticipate disruptive innovation because disruptive innovation is a black swan. Nobody can anticipate a black swan. You can only be decentralized enough, with enough empowerment at the network's end-points, to react to it when it happens. Hierarchies, on the other hand, are all about standard operating procedures to deal with an artificially limited range of variation, and fighting the last war. Hierarchies only work in a stable external environment, with the stability usually resulting from society-wide controls imposed from above.

Attempts to simulate networked forms within a hierarchical structure are usually futile compared to building the real thing outside them for the same reason that lobbying is futile compared to direct action. Initiatives like network-centric warfare and Enterprise 2.0 require enormous efforts to change the policies and internal culture of hierarchical institutions, and to persuade entrenched bureaucracies to do things differently against their very real material interests.

For example, Thomas Hammes's agenda for dealing with Fourth Generation Warfare requires "a major shift in culture within the government." It will also require large-scale bureaucratic restructuring towards an organization built around horizontal collaboration and sharing rather than Weberian command and control. These things "will likely take a generation to accomplish."[28]

On the other hand a stigmergic organization like Al Qaeda is permissionless.

So the point is, any established corporation that doesn't try to structure itself to survive in an environment of disruptive innovation will certainly go belly-up. But almost every corporation that tries to do so will fail anyway. Attempts to simulate networks within a hierarchy—Enterprise 2.0, the Wikified Firm, the U.S. military's Fourth Generation Warfare doctrine—will usually be supplanted by the real thing.

Nevertheless, even when such attempts fail and states and corporations simply collapse, efforts at fomenting network culture within them may have positive results. Tthe most important outcome will be the horizontal functional connections (including with state personnel working within the belly of the beast) that persist after the state itself decays.

Interstate Conflict as a Catalyst. During the overall transition from networks to hierarchies as the dominant form of social organization, we can expect the first signs of a tipping point to create a positive feedback process by which the system in decline fractures internally and hastens its own demise—the

[27] Hammes, *The Sling and the Stone,* pp. 195-198.

[28] Hammes, *The Sling and the Stone,* p. 228.

cliches “be eaten last” and “sell us the rope to hang them with” come to mind here. In particular, the supplantation of hierarchies by networks will be hastened by conflict in the international state system.

Our era is characterized by two considerably overlapping contradictions or fracture points. First, we’re in the early stages of historic transition from a social organization dominated by large, centralized, hierarchical institutions like corporations and nation-states, to a world of small, self-governing units connected together horizontally through networks. But second, the old hierarchical forces of corporations and states constitute a global system of power with the United States — the world’s Sole Remaining Superpower — as its enforcer. And in classic geopolitical terms, an expansionist hegemonic state tends to provoke a counter-hegemonic coalition of states seeking to restrain it. When these two intersecting contradictions reinforce each other, it throws in a chaotic element that may accelerate the process of change significantly.

There are many states which, as states, are clearly committed to maintaining the old system of domination internally — yet they desire to expand their independence at the expense of the United States or exert more power of their own over natural resources and markets. Even though states in general tend to rally in defense of hierarchies against networks, individual states may aid networked insurgencies against their competitors in order to get a leg up in the interstate competition.

To the extent that the war on network organizations is identified with one hegemonic state or group of states in particular, the tendency of other states to coalesce into an anti-hegemonic alliance will create divide the forces of hierarchy and create breathing room for networks. And likewise, to the extent that the hegemonic state's promotion of the hegemony of hierarchies is part of its larger policy of suppressing the emergence of viable state competitors in the international arena, other states may see furthering networked resistance movements as a weapon against the dominance of the hegemonic state.

Tom Friedman, in an admirable moment of frankness, once said “For globalism to work, American can’t be afraid to act like the almighty superpower that it is. The hidden hand of the market will never work without a hidden fist. … And the hidden fist that keeps the world safe for Silicon Valley’s technologies to flourish is called the U.S. Army, Air Force, Navy and Marine Corps.”

As imposing as the present global corporate order may seem, we would do well to remember how vulnerable it really is. It’s only as strong as its weakest link.

The Washington Consensus has pursued a maximalist position in enforcing digital copyright claims against file-sharing sites, carrying out reprisals against Wikileaks to the full extent of its powers, etc. Therefore states which resist the hegemony of the United States, or attempt to defy the Washington Consensus, are at least temporarily objective allies.

That's true in particular of any nations that emerge as free information havens in defying the maximalist copyright accords promoted by the US, or in hosting information (like Wikileaks) banned within the DRM Curtain.

To the extent that states defying Washington's hegemony attempt to nullify its advantage in force by resorting to “weapons of the weak” like asymmetric warfare and the kinds of cheap Assassin's Mace weapons we considered in the previous chapter, their geopolitical competition with the American bloc may overlap with and reinforce the networked resistance's emphasis of agility over brute force in all kinds of interesting ways.

Large-scale military power is less likely to result in victory than in the past. Even though warfare is increasingly asymmetrical, it's "increasingly being won by the militarily weaker side." A Harvard study found that asymmetric wars from 1800 and 1849 resulted in victory for the weaker side in 12% of cases. In those from 1950 and 1998, the weaker side won 55% of the time. One reason for this is changes in military technology that result in "the increasing ability of the weaker party to inflict casualties on its opponent at lower cost to itself." For example, in Iraq IEDs were responsible for a majority of casualties—this despite the Pentagon spending $17 billion on radio frequency jammers.[29]

Area denial technology and asymmetric warfare technologies are reversing the long-term shift that resulted from gunpowder and ushered in the Westphalian nation-state.

Weapons that deny access to superior force or degrade the performance of advanced offensive weapons systems are frequently cheaper, by several orders of magnitude, than the weapons they're deployed against. The so-called “Assassin's Mace” technologies we considered earlier are relevant here. Such means include the use of mines at maritime chokepoints and anti-ship missiles like the Sunburn that can in theory take out aircraft carriers.

The Obama administration's recent new Strategic Guidance document announced, as a top priority, overcoming adversary states' attempt to nullify the United States' strategic advantage through comparatively cheap area denial weapons.

> President Obama’s new military strategy has focused fresh attention on an increasingly important threat: the use of inexpensive weapons like mines and cyberattacks that aim not to defeat the American military in battle but to keep it at a distance.
>
> The president and his national security team predict that the security challenges of the coming decade will be defined by this threat, just as the last one was defined by terrorism and insurgency.
>
> A growing number of nations whose forces are overmatched by the United States are fielding these weapons, which can slow, disrupt and perhaps even halt an American offensive. Modern war plans can become mired in a bog of air defenses, mines, missiles, electronic jamming and computer-network attacks meant to degrade American advantages in technology and hardware....
>
> China and Iran were identified as the countries that were leading the pursuit of “asymmetric means” to counter American military force, according to the new strategy document, which cautioned that these relatively inexpensive measures were spreading to terrorist and guerrilla cells.
>
> At his announcement at the Pentagon last week, Mr. Obama said the country should invest in “the ability to operate in environments where adversaries try to deny us access.”...
>
> “Iran’s navy — especially the naval arm of Iran’s Revolutionary Guards — has invested in vessels and armaments that are well suited to asymmetric warfare, rather than the sort of ship-to-ship conflict that Iran would surely lose,” Michael Singh, managing director of the Washington Institute for Near East Policy, wrote in a recent essay for Foreign Policy.
>
> With Chinese and Russian help, Mr. Singh added, Iran is also fielding sophisticated mines, midget submarines and mobile antiship cruise missiles.
>
> Nathan Freier, a senior fellow at the Center for Strategic and International Studies, said, “Iran’s capabilities are best suited for imposing high costs on those who might need to force their way through the Strait of Hormuz, and on those in the region whom the Iranians perceive as being complicit in enabling foreign access.”
>
> The potential challenge from China is even more significant, according to analysts. China has a fleet of diesel-electric attack submarines, which can operate quietly and effectively in waters near China’s shore to threaten foreign warships. China also fields short-, medium- and long-range missiles that could put warships at risk, and has layers of radar and surface-to-air missiles along its coast.
>
> Finding, identifying and striking an American warship is a complex military operation. But the thicket of Chinese defenses could oblige an American aircraft carrier and its strike group to operate hundreds of miles farther out to sea, decreasing the number of attack sorties its aircraft could mount in a day and diminishing their effectiveness.
>
> Perhaps most worrisome is China’s focus on electronic warfare and computer-network attacks, which might blunt the accuracy of advanced American munitions guided by satellite.[30]

[29] Moises Naim, *The End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge Isn't What it Used to Be* (New York: Basic Books, 2013), p. 5

[30] Thom Shanker, “Pentagon Tries to Counter Low-Cost but Potent Weapons,” *New York Times*, January 9, 2012

Large powers are also forced to operate in a much more hostile environment of public awareness, given on-the-ground social media coverage of casualties and networked distribution of alternative news that renders the old press pools obsolete.[31] Israel learned this to its great chagrin in its July 2014 attack on Gaza—the first such Israeli aggression fought in the full light of social media coverage.

The Snowden Affair. The immediate public relations fallout to the security community from Snowden's leaks was only the beginning—but it was substantial in its own right.

Because (as we shall see below) the NSA had no way of tracking what documents Snowden had, it was forced to play defense. It only found out what had been leaked when the documents were actually published, in a slow death by a thousand cuts. As a result the Obama administration and the NSA left themselves wide open for a rope-a-dope strategy, attempting to control damage from each new leaked document with a new round of official happy talk—only to have the happy talk exposed as deliberate lies by the next leak. For example, President Obama, NSA chief Keith Alexander and strident Congressional NSA defenders Mike Rogers all strenuously denied, in a series of August press conferences, that any abuses of NSA surveillance had taken place. This was immediately followed by a *Washington Post* bombshell article on the NSA's abuse of the rules to spy on thousands of Americans every year.[32]

News of the leaks catalyzed a sizable constellation of backlashes against the U.S. Security State and the system of power it upholds.

First of all, it exemplified—and dramatized—a generational shift in thinking among those who had grown up in the digital era. The under-35 generation has fundamentally different attitudes toward institutional authority and loyalty than its parents and grandparents did.

> Gen Y will stare at you blankly if you talk about loyalty to their employer; the old feudal arrangement ("we'll give you a job for life and look after you as long as you look out for the Organization") is something their grandparents maybe ranted about, but it's about as real as the divine right of kings. Employers are alien hive-mind colony intelligences who will fuck you over for the bottom line on the quarterly balance sheet. They'll give you a laptop and tell you to hot-desk or work at home so that they can save money on office floorspace and furniture. They'll dangle the offer of a permanent job over your head but keep you on a zero-hours contract for as long as is convenient. This is the world they grew up in: this is the world that defines their expectations.[33]

The Security State is utterly dependent on what MacKenzie Wark calls the “hacker class” of Snowden's generation—a generation permeated with a distrust of hierarchy and authority and a belief in transparency and information freedom. The NSA is finding it as impossible to deal with the mores of this generation in its own ranks as the music industry has found it to deal with them in the case of the file-sharing movement.

> Keeping secrets is an act of loyalty as much as anything else, and that sort of loyalty is becoming harder to find in the younger generations. If the NSA and other intelligence bodies are going to survive in their present form, they are going to have to figure out how to reduce the number of secrets.
>
> [T]he old way of keeping intelligence secrets was to make it part of a life-long culture. The intelligence world would recruit people early in their careers and give them jobs for life. It was a private club, one filled with code words and secret knowledge.

<http://www.nytimes.com/2012/01/10/world/pentagon-tries-to-counter-low-cost-but-potent-weapons.html>.

[31] Naim, *op. cit.*, p. 111.

[32] Barton Gellman, “NSA broke privacy rules thousands of times per year, audit finds,” *Washington Post*, August 15, 2013 <http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html>.

[33] Charlie Stross, “Snowden leaks: the real take-home,” *Charlie's Diary*, August 16, 2013 <http://www.antipope.org/charlie/blog-static/2013/08/snowden-leaks-the-real-take-ho.html>.

> ...An intelligence career meant that you had access to a new world, one to which "normal" people on the outside were completely oblivious. Membership of the private club meant people were loyal to their organisations, which were in turn loyal back to them.
>
> Those days are gone... Many jobs in intelligence are now outsourced, and there is no job-for-life culture in the corporate world any more. Workforces are flexible, jobs are interchangeable and people are expendable....
>
> Many will also believe in openness, especially the hacker types the NSA needs to recruit. They believe that information wants to be free, and that security comes from public knowledge and debate.....[34]

And the Security State is powerless to stop new Snowdens from emerging within its midst. The NSA, for example, has a thousand sysadmins whose document viewing and downloading practices the agency is unable to track.[35] Despite official happy talk about an "internal audit process," the NSA still has no idea what documents Snowden took.[36] Which, in turn, has of course heightened the paranoia within the NSA leadership, who are waiting for the next shoe—and the next one, and the next—to drop.

> "They think he copied so much stuff — that almost everything that place does, he has," said one former government official, referring to the NSA, where Snowden worked as a contractor for Booz Allen Hamilton while in the NSA's Hawaii facility. "Everyone's nervous about what the next thing will be, what will be exposed."[37]

The generational shift in thinking, brought into higher relief than ever before by the Snowden affair (which itself came on the heels of the Manning and Schwartz stories), has provoked near-unprecedented panic among the generation operating the old centers of power.

> In 1974, it was easier for the ruling class to sacrifice Nixon and to cut a few heads with him. Parallels to the current situation are troubling. Today's ruling class is afraid, in a state of panic, and does not act rationally any more. It seeks to make examples at all costs, to repair each leak hoping it is only a few isolated cases.[38]
>
> I think there's a lot of fear in traditional institutions.... Nobody understands why one of their boys would do this really weird thing. What has the Internet done to these people? What is it doing to their own children? See, that's the thing. If you're part of traditional power right now, this thing that's spreading over the earth, that's changing everything.... If you were the MPAA a few years ago, or the RIAA, this Internet changed everything it touched into this weird thing, and it was like the Borg, or the zombie apocalypse. And if you wonder why they fight so hard, why they chase the Snowdens and try to shut down The Pirate Bay so much more than traditional criminals, it's because it looks so much like the zombie, and possibly media apocalypse—and we already have their children.[39]

[34] Bruce Schneier, "Government Secrecy and the Generation Gap," *Schneier on Security*, September 9, 2013 <https://www.schneier.com/blog/archives/2013/09/government_secr_1.html>.

[35] Mike Masnick, "1,000 Sys Admins Can Copy Any NSA Document Without Anyone Knowing About It; Think Only Snowden Did?" *Techdirt*, August 26, 2013 <https://www.techdirt.com/articles/20130826/12223124315/1000-sys-admins-can-copy-any-nsa-document-without-anyone-knowing-about-it-think-only-snowden-did.shtml>.

[36] Mike Masnick, "Ed Snowden Covered His Tracks Well; How Many Other NSA Staffers Did The Same?" *Techdirt*, August 26, 2013 <https://www.techdirt.com/articles/20130824/21483724305/ed-snowden-covered-his-tracks-well-how-many-other-nsa-staffers-did-same.shtml>; Masnick, "US Still Can't Figure Out What Snowden Took; What Happened To Those Perfect 'Audits'?" *Techdirt*, August 21, 2013 <https://www.techdirt.com/articles/20130820/15441924258/us-still-cant-figure-out-what-snowden-took-what-happened-to-those-perfect-audits.shtml>.

[37] Ellen Nakashima and Greg Miller, "U.S. worried about security of files Snowden is thought to have," *Washington Post*, June 24, 2013 <http://www.washingtonpost.com/world/national-security/us-officials-worried-about-security-of-files-snowden-is-thought-to-have/2013/06/24/1e036964-dd09-11e2-85de-c03ca84cb4ef_story.html?Post%20generic=%3Ftid%3Dsm_twitter_washingtonpost>.

[38] Rick Falkvinge, "The First Global Civil War," *Falkvinge on Infopolicy*, August 28, 2013 <http://falkvinge.net/2013/08/28/the-first-global-civil-war/>.

[39] Quinn Norton keynote address to NetHui2013 convention, Wellington, New Zealand, July 8-10, 2013 <https://www.youtube.com/watch?v=qgXRbJJv7FA#t=228>.

Besides undermining internal security, the general shift in loyalties has made it more difficult for the surveillance state to recruit the new blood necessary to sustain itself in the future. Demand for hackers in the expanding surveillance state—the NSA and the Army's Cyber Command, for example—is outstripping the supply. “They will choose where they work based on salary, lifestyle and the lack of an interfering bureaucracy and that makes it particularly hard to get them into government."[40]

> The U.S. government's efforts to recruit talented hackers could suffer from the recent revelations about its vast domestic surveillance programs, as many private researchers express disillusionment with the National Security Agency....[41]

The Snowden leaks also catalyzed a large-scale trend for the Web's infrastructure to increase its independence of U.S. control. One of the near-to-medium-term casualties of the leaks is likely to be the overwhelming dependence of the global Web on servers in the United States. The Snowden revelations about PRISM sparked immediate buzz about a shift to servers outside the United States that would not automatically roll over to demands from the U.S. Security State.

> One of the reasons electronic surveillance tools such as PRISM work so well is because much of the world's Internet traffic goes through U.S. servers. The American companies that own and operate that equipment can be subpoenaed and the data handed over to the government. Voila — intelligence secured!
>
> But that works only so long as the traffic keeps going where intelligence agencies want it to go. There are signs now that the gravy train of easy data is coming to an end. Foreign companies who once considered hosting their information on U.S. servers are beginning to change their minds. And they're not the only ones. Governments are growing more wary, too....
>
> But thanks to the NSA leaks and the government’s reluctance to fully disclose its activities, criminals are about to have more ways to evade online detection than ever. Investigators’ jobs will get far more difficult if their suspects’ communications suddenly vanish from U.S. servers and reappear in an encrypted format in a country that won’t cooperate with American demands.[42]

Much of the shift is likely to take the form of generational attrition; not so much a dramatic exodus of existing web-hosting customers to servers outside the U.S., which can be an intensive logistical process, but the refusal of a new generation of customers to use U.S. servers in the first place.[43] But even in the short term, there's speculation that offshoring could cost American web-hosting companies up to $35 billion.[44]

As one would expect, news of the extent of U.S. spying on private communications gave new impetus to the mainstreaming of encryption. The Snowden leaks included dismaying information about the extent to which the NSA had already compromised encryption systems widely in use. It was, for example, able to decrypt the TOR router included in versions of the Firefox browser for Windows issued through June 2013. The good news was that this achievement was more limited than it sounded. The TOR onion router itself was not compromised, nor were versions of TOR bundled with Firefox for Linux, nor was TOR incorporated into versions of the Firefox bundle for Windows issued after June.

[40] Peter Apps and Brenda Goh, “Cyber warrior shortage hits anti-hacker fightback,” *Reuters UK*, October 13, 2013 <http://uk.reuters.com/article/2013/10/13/uk-security-internet-idUKBRE99C03A20131013>.

[41] Joseph Menn, “NSA revelations could hurt collaboration with 'betrayed' hackers,” Reuters, August 3, 2013 <http://www.reuters.com/article/2013/08/03/net-us-usa-security-hacking-ethics-idUSBRE9720A020130803>.

[42] Brian Fung, “PRISM works because a ton of data moves through U.S. servers. That’s also why it could fail,” *Washington Post*, August 20. 2013 <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/20/prism-works-because-a-ton-of-data-moves-through-u-s-servers-thats-also-why-it-could-fail/>.

[43] Mike Masnick, “No, There Hasn't Been A Big Shift Away From US Datacenters... Yet,” *Techdirt*, August 23, 2013 <https://www.techdirt.com/articles/20130815/10310724188/no-there-hasnt-been-big-shift-away-us-datacenters-yet.shtml>.

[44] “NSA Internet Spying Sparks Race To Create Offshore Havens For Data Privacy,” *Slashdot*, September 30, 2013 <http://yro.slashdot.org/story/13/09/30/1146236/nsa-internet-spying-sparks-race-to-create-offshore-havens-for-data-privacy>.

And the government's ability to decrypt even communications in the vulnerable categories was limited by its information-processing capabilities.

> But the documents suggest that the fundamental security of the Tor service remains intact. One top-secret presentation, titled 'Tor Stinks', states: "We will never be able to de-anonymize all Tor users all the time." It continues: "With manual analysis we can de-anonymize a very small fraction of Tor users," and says the agency has had "no success de-anonymizing a user in response" to a specific request.[45]

Meanwhile, two prominent encrypted email services—Lavabit and Open Circle—shut down in response to Obama administration demands for user information.[46] This ominous trend spurred announcements of a variety of new encrypted email services in the works.

The Internet's governance institutions responded to news of PRISM by taking steps to free themselves of disproportionate American influence.

> All of the major internet organisations have pledged, at a summit in Uruguay, to free themselves of the influence of the US government.
>
> The directors of ICANN, the Internet Engineering Task Force, the Internet Architecture Board, the World Wide Web Consortium, the Internet Society and all five of the regional Internet address registries have vowed to break their associations with the US government....
>
> That's a distinct change from the current situation, where the US department of commerce has oversight of ICANN.[47]

U.S. control over ICANN had already come under heightened international scrutiny after the U.S. Justice Department used domain names seizures to punish alleged violations of copyright law.

> Even before the Snowden leaks... governments like China, India and Russia have distrusted ICANN. They have demanded control of the net's naming system to be turned over to an organization such as the International Telecommunications Union, an affiliate of the United Nations....
>
> What's more, who controls the internet's infrastructure became an issue last year after the United States began seizing hundreds of domains across the globe for allegedly breaching federal copyright and trademark laws.[48]

The NSA leaks also catalyzed pushback against the U.S. in more traditional diplomatic venues. In October 2013, the European Parliament voted to halt financial data-sharing with the U.S.[49] And revelations that the NSA may have been listening in on German Chancellor Angela Merkel's phone threatened the TAFTA/TIPP trade agreement between the U.S. and EU.[50]

Finally, the NSA story has made the American public a lot more resistant to surveillance in principle, making it more difficult for local police departments to implement policies for increased use of surveillance

[45] James Ball, Bruce Schneier and Glenn Greenwald, "NSA and GCHQ target Tor network that protects anonymity of web users," *The Guardian*, October 4, 2013 <http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption>.

[46] Joe Mullin, "After Lavabit shutdown, another encrypted e-mail service closes," *Ars Technica*, August 9, 2013 <http://arstechnica.com/tech-policy/2013/08/in-wake-of-lavabit-shutdown-another-secure-e-mail-service-goes-offline/>.

[47] Duncan Geere, "The US is losing control of the internet," *Wired UK*, October 12, 2013 <http://www.wired.co.uk/news/archive/2013-10/12/us-internet-control>.

[48] David Kravets, "NSA Leaks Prompt Rethinking of U.S. Control Over the Internet's Infrastructure," *Wired*, October 14, 2013 <http://www.wired.com/threatlevel/2013/10/global-net-infrastructure/>.

[49] Rick Falkvinge, "In Mass Surveillance Fallout, European Parliament Votes to Suspend Financial Data Sharing With U.S.," *Falkvinge on Infopolicy*, October 25, 2013 <http://falkvinge.net/2013/10/25/in-mass-surveillance-fallout-european-parliament-votes-to-suspend-financial-data-sharing-with-united-states/>.

[50] Mike Masnick, "How NSA Spying On Angela Merkel May Scuttle TAFTA/TTIP Trade Agreement," *Techdirt*, October 28, 2013 <https://www.techdirt.com/articles/20131028/00350825030/how-nsa-spying-angela-merkel-may-scuttle-taftattip-trade-agreement.shtml>.

cameras, drones and the like.[51] The backlash when the Snowden leaks exposed telecom and social media collaboration with "the authorities" has also made the latter more leery of cooperating with the security state.[52]

As if all this were not enough, Glenn Greenwald's magazine *The Intercept* has published new leaks suggesting there have been a *second* and *third* leaker. And since, as we saw above, the NSA seems to be really awful at detecting leakers internally or identifying what information has been compromised, we can probably expect a lot more.[53]

II. The Question of Repression

I've encountered plenty of people who are, on the whole, pessimistic about the likely use of hunter-killer drones and other control technologies to root out the counter-economy, when the corporate state sees itself as in a desperate enough position to throw off the pretense of democracy and resort to undisguised large-scale repression. In its most dystopian form, the idea is a repressive onslaught of surveillance systems, hunter-killer drones, crowd-control technologies like microwaves/sonic blasts, and psychopharmacological engineering of the enforcement troops to stamp out the alternative economy and enforce a system of global corporate neo-serfdom under the rule of multibillionaires living inside militarized luxury enclaves.

John Robb describes the way assorted robotic technologies might be used for such purposes. Drones are already being used increasingly for internal surveillance functions by domestic law enforcement, with the actual arrests still being carried out by human boots on the ground.[54]

> ...[H]ow do a very, very small group of neo-feudal plutocrats control a global population (of economic losers) in the modern context?...
>
> Long term? Bots. Software bots. Drones. My good friend Daniel Suarez did a great job of demonstrating how this works in his books Daemon and Freedom.
>
> In short, bots will increasingly allow a VERY small group of people (in our case, a small group of plutocrats that act as the world's economic central planners) to amplify their power/dominance in a the physical world to a degree never seen before.
>
> Software bots automate information dominance. They can do everything from checking purchasing habits to energy use (via smart meters) to social media use o look for "terrorist" signatures. They can dominate markets as we are seeing high frequency trading. These software bots can also automate interactions with human beings from the simple phone spam/customer service phone tree to interfaces like Siri.
>
> Hardware bots include everything from flying drones to crawling rats to kill, maim, or incapacitate individuals and/or groups.... Expect to see them operating in swarms/clouds, conducting highly autonomous decision making (including the decision to kill), and serving in hunter killer roles.
>
> The combination of the two bot systems, software and hardware, provides the means to automate control of vast populations. A perfect, privatized solution for an extremely small group of plutocrats (many of whom are pathogenic).
>
> OUR job is to avoid this future. Build resilient communities that can provide independence and defend themselves. Provide an alternative for those unwilling to become economic losers.[55]

[51] J.D. Tuccille, "NSA Revelations Monkeywrench Police Surveillance State Schemes," *Reason Hit&Run*, October 21, 2013 <http://blog.p2pfoundation.net/producia-building-a-new-economy/2012/02/23>.

[52] Bruce Schneier, "A Fraying of the Public/Private Surveillance Partnership," *Schneier on Security*, November 14, 2013 <https://www.schneier.com/blog/archives/2013/11/a_fraying_of_th.html>.

[53] Schneier, "The US Intelligence Community has a *Third* Leaker," *Schneier on Security*, August 7, 2014 <https://www.schneier.com/blog/archives/2014/08/the_us_intellig.html>.

[54] John Robb, "Drones in the US of A," *Global Guerrillas*, December 11, 2011 <http://globalguerrillas.typepad.com/globalguerrillas/2011/12/drones-in-the-us-of-a.html>.

[55] John Robb, "Q: How Will Plutocrats Dominate a World? A: Bots," *Global Guerrillas*, November 16, 2011

Vinay Gupta, in a recent exchange with me on Twitter, recently argued that the passage of the NDAA (with its provisions for indefinite detention without trial) and the shutdown of Megaupload without due process of law signaled the emergence of the U.S. as a full-blown fascist state. And he suggested the possibility that, as governments implode in the face of networked resistance movements in countries like Spain and Greece, free information havens emerge in places like Iceland, and one domino after another in the global South begins to secede from the neoliberal order, the United States will become embroiled in a desperate World War of counterinsurgency, using air strikes, blockades, cyberwar, black ops, hunter-killer drones, and crowd-control technologies to suppress the emerging free order. “Hacker labs in extradition-resistant areas being hit by special forces is where this goes...”[56] The street fighting between riot cops and Occupy protesters was just a dress rehearsal, as Spain was for WWII.

So are we headed for a likely future in which Skynet and the Terminator HK's are controlled, not by an artificial intelligence, but by Dick Cheney?

I don't think so.

We already saw in the last chapter that networked, stigmergic movements are more agile than authoritarian hierarchies, and able to get inside the state's OODA loop in developing technologies of circumvention faster than the state can develop technologies of control. We've seen that authoritarian hierarchies respond to attack by becoming more authoritarian and hierarchical, while networks respond by becoming more agile and resilient.

Unencrypted drones, to start with that technology, are extremely vulnerable to hacking of their guidance and communications systems. In addition, though, there's the old-fashioned “kinetic option” of shooting them down. Predator and Reaper drones—which carry out the majority of kills in Pakistan—fly at only about 100mph. This means they're highly vulnerable to most jet interceptors currently in service around the world, as well as surface-to-air missiles. And not even Sentinel drones, whose speed tops out at almost Mach 1, are entirely invulnerable.[57]

Finally, drones may be vulnerable to passive resistance, such as altering infrared profiles or creating ambient noise to disrupt their sensors.

Our earlier discussion of Assassin's Mace weapons is relevant here. The resistance's agility in technical development mean it is able to develop mashups of existing technology faster than the corporate state was able to develop the original technologies. It can develop means of circumvention faster than the state can deal with them.

And Al Qaeda seems at least to be working on a wide range of cheap countermeasures—of varying or unknown levels of effectiveness—to American drones.

> 1 -- It is possible to know the intention and the mission of the drone by using the Russian-made “sky grabber” device to infiltrate the drone’s waves and the frequencies. The device is available in the market for $2,595 and the one who operates it should be a computer know-how.
>
> 2 – Using devices that broadcast frequencies or pack of frequencies to disconnect the contacts and confuse the frequencies used to control the drone. The Mujahideen have had successful experiments using the Russian-made “Racal.”
>
> 3 – Spreading the reflective pieces of glass on a car or on the roof of the building.
>
> 4 – Placing a group of skilled snipers to hunt the drone, especially the reconnaissance
>
> ones because they fly low, about six kilometers or less.

<http://globalguerrillas.typepad.com/globalguerrillas/2011/11/q-how-will-plutocrats-dominate-a-world-a-bots.html>.

[56] Vinay Gupta (@leashless), 2:44 PM, March 6, 12 <https://twitter.com/leashless/status/177162811661754369>.

[57] Brian Palmer, “Is It Hard to Kill a Drone?” *Slate*, June 6, 2012 <http://www.slate.com/articles/news_and_politics/explainer/2012/06/cia_drone_program_is_it_hard_to_shoot_one_down_.html>.

> 5 – Jamming of and confusing of electronic communication using the ordinary water-lifting dynamo fitted with a 30-meter copper pole.
>
> 6 – Jamming of and confusing of electronic communication using old equipment and keeping them 24-hour running because of their strong frequencies and it is possible using simple ideas of deception of equipment to attract the electronic waves devices similar to that used by the Yugoslav army when they used the microwave (oven) in attracting and confusing the NATO missiles fitted with electromagnetic searching devices.
> 7 – Using general confusion methods and not to use permanent headquarters.
> 8 – Discovering the presence of a drone through well-placed reconnaissance networks and
> to warn all the formations to halt any movement in the area.
> 9 – To hide from being directly or indirectly spotted, especially at night.
> 10 – To hide under thick trees because they are the best cover against the planes.
> 11 – To stay in places unlit by the sun such as the shadows of the buildings or the trees.
> 12 – Maintain complete silence of all wireless contacts.
> 13 – Disembark of vehicles and keep away from them especially when being chased or during combat.
> 14 – To deceive the drone by entering places of multiple entrances and exits.
> 15 – Using underground shelters because the missiles fired by these planes are usually of the fragmented anti-personnel and not anti-buildings type.
> 16 – To avoid gathering in open areas and in urgent cases, use building of multiple doors or exits.
> 17 – Forming anti-spies groups to look for spies and agents.
> 18 – Formation of fake gatherings such as using dolls and statutes to be placed outside false ditches to mislead the enemy.
> 19 – When discovering that a drone is after a car, leave the car immediately and everyone should go in different direction because the planes are unable to get after everyone.
> 20 – Using natural barricades like forests and caves when there is an urgent need for training or gathering.
>
> 21 – In frequently targeted areas, use smoke as cover by burning tires.
>
> 22 – As for the leaders or those sought after, they should not use communications equipment because the enemy usually keeps a voice tag through which they can identify the speaking person and then locate him.[58]

In the American domestic market an Oregon startup, Domestic Drones Countermeasures LLC, claims to be preparing to offer a package of countermeasures against law enforcement drones.

> Founded in February, DDC was created by the same people behind defense contractor Aplus Mobile, which makes ruggedized computers for other defense contractors. Using knowledge gained from its military contracting work, DDC says it has developed countermeasures that are "highly effective and undefeatable by most current domestic drone technologies."
>
> How does the technology work? The press release was maddeningly vague ("Multiple layer systems ensure success by impeding typical drone sensors, infrared and camera capability and their effectiveness") so we reached out to the company over email. Here's what DDC's Amy Ciesielka has to say: "We simply do not allow the [drone] cameras to observe with any clarity."
>
> More to the point, DDC's system has some sort of software that's programmed to conspire against camera- and infrared-equipped drones. One report described the products as "land-based boxes."...
>
> Not knowing more about what form these countermeasures will take, it is hard to speculate on the broader implications here. But when commercial drones start to crowd our skies, the market for consumers who want to win back some privacy will only grow. You can bet DDC won't be the only one selling anti-drone wares to the masses. [59]

[58] "The Al-Qaida Papers—Drones." This document is one of several found by The Associated Press in buildings recently occupied by al-Qaida fighters in Timbuktu, Mali <http://hosted.ap.org/specials/interactives/_international/_pdfs/al-qaida-papers-drones.pdf>.

[59] Kelsey D. Atherton, "Company to Make Antidrone Tech Available to the Masses," Popsci.com, March 20, 2013 <http://www.popsci.com/technology/article/2013-03/company-to-make-antidrone-tech-available-to-the-masses>.

Any consideration of the repressive use of drones must also take into account the possible spread of such technology to the resistance. The development of technologies like drones seems to be governed by a sort of analogue to Moore's Law: drone tech developed today at an R&D cost of billions will likely be available off the shelf five years later at a tiny fraction of the cost, thanks to open-source hardware hackers.

As John Robb writes, the cost of drone technology is plummeting:

> The cost and size of drones will shrink. Nearly everyone will have access to drone tech (autopilots already cost less than $30). Further, the software to enable drones to employ swarm behavior will improve. So, don't think in terms of a single drone. Think in terms of a single person controlling hundreds and thousands.[60]

As evidence, he cites the DIY Drone community.[61] Most importantly, drone hobbyists have shown *armed* drones (a six-rotor helicopter drone with mounted paintball guns, shooting at fixed targets on the ground) to be entirely feasible.[62] One YouTube video shows a helicopter drone armed with a paintball gun, shooting up targets on the ground.[63] An open-source drone autopilot system, based on the Lisa/S chip, weights about a sixteenth as much as its predecessor, and is compatible with any type of drone.[64]

The dynamic of international state rivalry adds another twist to the proliferation of cheap drone technology, as comparatively high-tech economic and military powers like China export drones to countries threatened by the United States.

> Cheap drones made in China could end up arming potential U.S. foes such as North Korea, Iran and terrorist organizations.
>
> China already makes drones that don't quite match up to U.S. military drones, but for a fraction of the cost. The Chinese military envisions such unmanned autonomous vehicles (UAVs) scouting out battlefield targets, guiding missile and artillery strikes, and swarming potential adversaries, such as U.S. carrier battle groups.
>
> "In whatever future conflict scenario we're in five or 10 years from now, the proliferation of UAVs is going to complicate things for the U.S. military," said Ian Easton, a research fellow at the Project 2049 Institute.
>
> China has built a huge military-industrial complex to support its growing drone fleet, which consisted of about 280 military drones as of mid-2011, according to a report released by the Project 2049 Institute on March 11. Chinese manufacturers supplying the military and state agencies also have begun seeking foreign buyers in a global drone market that aerospace and defense market research firm Teal Group estimates to be worth $89 billion over the next 10 years.
>
> Retired Chinese generals have stated on Chinese state television station CCTV that Chinese drone technology lags American technology by about five years, Easton said. However, Chinese manufacturers are touting their plans to build drones five or even 10 times cheaper than comparable U.S. drones, whose hardware alone costs $5 million to $10 million.[65]

The greater speed of innovation by networks, in particular, is just one example of the broader phenomenon of an agile resistance movement staying inside its enemy's OODA loop. Consider Tor developers' cre-

[60] John Robb, "The Future of Drone Warfare," *Global Guerrillas*, December 21, 2011 <http://globalguerrillas.typepad.com/ globalguerrillas/2011/12/drone-bonjwas.html>.

[61] <http://diydrones.com/>.

[62] J.D. Tuccille, "Forget DIY Drones, How About DIY *Armed* Drones?" *Reason Hit & Run Blog*, December 13, 2012 <http://reason.com/blog/2012/12/13/forget-diy-drones-how-about-diy-armed-dr>.

[63] Annalee Newitz, "This video of a drone with a gun will freak you the hell out," *io9*, June 14, 2013 <http://io9.com/this-video-of-a-drone-with-a-gun-will-freak-you-the-hel-513442074>.

[64] Michel Bauwens, "Project of the Day: the Lisa S Open Source Drone Autopilot System," P2P Foundation Blog, December 22, 2013 <http://blog.p2pfoundation.net/project-of-the-day-the-lisa-s-open-source-drone-autopilot-system/2013/12/22>.

[65] Jeremy Hsu, "Cheap Drones Made in China Could Arm U.S. Foes," *Mashable*, April 3, 2013 <http://mashable.com/ 2013/04/03/china-drones-us-foes/>.

ation of a same-day hack to the Iranian regime's attempt to block its routers. Consider the development of a Firefox workaround extension for SOPA before the bill even came up for a vote. Consider the FBI's seizure of the MegaUpload domain name after many months of preparation—to which Anonymous responded in a matter of hours with the largest DDOS attack in history and a doxing of MPAA chief Chris Dodd. The flexibility and rapid innovations in Occupy Wall Street tactics, in response to police repression—for example the use of light infantry tactics to exploit superior mobility against the plodding riot cops, is yet another example. Generally speaking, the resistance is able to stay a step ahead of the corporate state and keep it permanently off-balance.

Technologies of imperial control like drones may wind up being more useful to the Resistance than to the Empire.

The asymmetry between the state and the Resistance results from the former's relative target density. It also results from the nature of its infrastructure systems and the proliferation of key nodes that can be struck randomly and produce damage at great distances. John Robb writes:

> Standoff attacks. Like many historical swarming attacks, global guerrillas will have significant standoff firepower potential—the ability to attack from a distance. However, this firepower isn't a traditional weapon, rather, its the global guerrilla's ability to use attacks on infrastructure to impact downstream systems miles (perhaps hundreds of miles) distant. Attacks will be rotated among infrastructures in a modern variant of horse archer tactics.[66]

The American state's insurgent enemies today, according to Bruce Schneier, have access to technologies the Soviets could never have dreamed of.

> Defending against these sorts of adversaries doesn't require military-grade encryption only where it counts; it requires commercial-grade encryption everywhere possible.
>
> This sort of solution would require the NSA to develop a whole new level of lightweight commercial-grade security systems for military applications — not just office-data "Sensitive but Unclassified" or "For Official Use Only" classifications. It would require the NSA to allow keys to be handed to uncleared UAV operators, and perhaps read over insecure phone lines and stored in people's back pockets. It would require the sort of ad hoc key management systems you find in internet protocols, or in DRM systems. It wouldn't be anywhere near perfect, but it would be more commensurate with the actual threats.[67]

In other words, it would require a very high and broad-based level of trust in the lowest-level functionaries of the intelligence apparatus—quite dangerous, given the possibility (discussed below) of demoralization and defection within the apparatus in the event of a full-scale war of terror by the American state against its domestic population.

Robb himself acknowledged the possibility that "small groups [might] put together systems like this [autonomous drones] on the cheap." Nevertheless, his primary fear is the ability of such drones " to automate repression, particularly if combined with software bots that sift/sort/monitor all of your data 24x7x365 (already going on)."[68] He described, in a subsequent post, the implications for both foreign and domestic counterinsurgency warfare:

> Gunboat diplomacy was the essence of military power projection for centuries. Want to coerce a country? Sail a aircraft carrier battle group into their national waters.

[66] John Robb, "GLOBAL GUERRILLA SWARMING," *Global Guerrillas*, May 18, 2004 <http://globalguerrillas.typepad.com/globalguerrillas/2004/05/global_guerrill.html>.

[67] Bruce Schnerier, "Intercepting Predator Video," *Schmeier on Security*, December 24, 2009 <http://www.schneier.com/blog/archives/2009/12/intercepting_pr.html>.

[68] John Robb, "The Future of Warfare," *Global Guerrillas*, January 27, 2012 <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/the-future-of-warfare.html>.

> However, carrier battlegroups are hideously expensive, increasingly vulnerable to low cost attack, and less lethal than they appear (most of the weapons systems are used for self-defense).
>
> What are nation-states replacing them with? Drones. You can already see it in action across the world as drone staging areas are replacing traditional military bases/entanglements. Further, drones already account for the vast majority of people killed by US forces.
>
> Of course, the reason for this is clear. Drones are relatively cheap, don't require many people to deploy/operate, don't put personnel directly at risk, can be easily outsourced, can be micromanaged from Washington, and are very effective at blowing things up.
>
> The final benefit of Drone Diplomacy: drones make it possible to apply coercion at the individual or small group level in a way that a blunt instrument like a carrier battle group can't.
>
> **What does this mean?**
>
> It allows truly scalable global coercion: the automation of comply or die.
>
> Call up the target on his/her personal cell (it could even be automated as a robo-call to get real scalability—wouldn't that suck, to get killed completely through bot based automation).
>
> Ask the person on the other end to do something or to stop doing something.
>
> If they don't do what you ask, they die soon thereafter due to drone strike (unless they go into deep hiding and disconnect from the global system)....
>
> All the money is on cyber intel (to generate targets based on "signatures") and drones to kill them. When domestic unrest occurs in the US due to economic decline, these systems will be ready for domestic application.[69]

Robb argues that the only real defenses against drones are to harden targets and thereby raise the average cost of attacks relative to target value, or to develop a counter-offensive drone capability. Drones, like nukes, shift the advantage almost entirely to the offensive. The only real response is to deter them by having "drones of your own."[70]

Given Robb's references to the availability of drone technologies on the cheap, combined with the usefulness of drones for targeting key individuals, it's dismaying that he failed to connect the dots. Some of his readers, however, were quick to do so:

> Why only nation states?
>
> What is it in dronetech that cannot be open sourced and turned against the oppression?...
>
> Most governments can already whack pretty much any subject they care to. But the reverse is not true. With widely available enough drones, some symmetry might again be restored....
>
> —Stuki[71]
>
> What are the weaknesses of drone support crews, drone manufacturers and their employees?
>
> —Craig[72]
>
> ...you could characterize drones as elements in a network and attack/subvert/co-opt critical nodes in that network just the same as you could do when attacking anything else. (And who knows what those may be?)
>
> —Mercutio[73]

[69] John Robb, “Drone Diplomacy: Comply or Die,” *Global Guerrillas*, January 30, 2012 <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/drone-diplomacy-comply-or-die.html>.

[70] John Robb, “Is There a Defense Against Drones?” *Global Guerrillas*, January 31, 2012 <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/is-there-a-defense-against-drones.html>.

[71] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/drone-diplomacy-comply-or-die.html#comment-6a00d83451576d69e201630069ae46970d>.

[72] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/drone-diplomacy-comply-or-die.html#comment-6a00d83451576d69e20168e668714e970c>.

[73] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/is-there-a-defense-against-drones.html#comment-6a00d83451576d69e20168e66db702970c>.

> You defeat drones by killing its tail, the US has these things all over the world, but operating out in the open to a great extent, would not take much ground work to find out where they are flying from and the operational crew, find their base, and kill them on the ground, and kill there ground crews too.... Kill the guys who send the drones, they are findable and hittable, equalize the kill zones, bullets and bombs travel both ways.
>
> —The Black[74]
>
> It seems to me that one defense would be to "grab the belt," in various ways. I would go after the personnel involved, from leadership and their families to the operators. The air force, and their dependents, have escaped conflict for far too long.
>
> —EN[75]
>
> Attacking the drones themselves is far far more difficult than neutralizing the C&C structure behind them.) As 'The Black' mentioned above find the guys with the joysticks and their chain of command.
>
> —Sam [76]
>
> On the kinetic level, drones work both ways. When an insurgent can cheaply print a few dozen with small explosive warheads and swarm them at an enemy airfield, the playing field is a bit leveled. Paddy Moyne and the rest of the SAS were able to take out hundreds of Axis planes on their African airfields using very small charges. Do I need to expound?
>
> —B[77]
>
> Look at the numbers of contractors that supported the war in Iraq/ are supporting the war in Afghanistan. Contractors quit EASY. Pick a company, and I'm not dog piling, but for example Blackwater/XE. How long would their contractors have worked protecting Dept. of State if a family a month was being murdered stateside?
>
> Fill in the blank. Contractors are mission critical and can quit on a moments notice.
>
> —matt[78]

Robb, writing later against the background of the mid-2013 conflict between the U.S. and Bashir Assad over Syria's alleged use of chemical weapons against civilians, speculated that using drones to target specific individuals responsible for such decisions—rather than conventional attacks—was the wave of the future.

> What can we expect to see? A more direct approach. The targeting of specific individuals in the hierarchy that made the decision to use the banned weapons. An extralegal process that doesn't look much like traditional warfare and much more like how nation states hunt "terrorists."
>
> In the case of Syria, the evidence would be presented and adjudicated in an extralegal process. The portion of the national hierarchy involved in the use of the banned weapon would be deemed a terrorist organization and specific people would be placed onto a target list, prioritized, and then hunted as individuals.
>
> I suspect, as this process matures, targets will be made public (listed on the Internet) and given 60 days to give themselves up). After that, it's a one way ticket. Drones away...crowdsourced manhunts...NSA big data...and an eventual explosive death (with the requisite collatoral damage that nobody seems to care about).[79]

[74] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/is-there-a-defense-against-drones.html#comment-6a00d83451576d69e20167616c8f4f970b>.

[75] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/is-there-a-defense-against-drones.html#comment-6a00d83451576d69e20168e66e82f5970c>.

[76] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/is-there-a-defense-against-drones.html#comment-6a00d83451576d69e20163007b375d970d>.

[77] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/is-there-a-defense-against-drones.html#comment-6a00d83451576d69e20168e675b6ff970c>.

[78] <http://globalguerrillas.typepad.com/globalguerrillas/2012/01/is-there-a-defense-against-drones.html#comment-6a00d83451576d69e20168e68062f4970c>.

[79] John Robb, “How to deal with Countries that Use Chemical Weapons? Make it Personal,” *Global Guerrillas*, September

The problem for nation-states like the US, and for other hierarchical institutions like corporations, is that this strategy can be reversed. When hunter-killer drones are a cheap, off-the-shelf technology that can be manufactured in garage factories by networked resistance movements, the US and major corporations will have to worry about their own key command personnel being targeted in the same way they target alleged terrorists today. A list of potential targets includes--but is by no means limited to--military chains of command all the way to the top, and the senior management of military industry. Drones might also carry out pinpoint destruction of physical support facilities like air traffic control at airbases Western drones are launched from, or the factories where the drones are produced. Robb discusses elsewhere, in a context other than drones, the increasing tendency of networked terror movements like ISIS to isolate and target individual leadership figures like corporate CEOs in order to demoralize organizations and remove them from the fight.

> **once an attack on a senior tech executive happens, future threats will be instantly credible and highly coercive.**
>
> If that occurs, we are going to find out very quickly that the corporation, and particularly tech companies, are particularly bad organizations for warfare. One reason is that they are too centralized. In particular, the institution of the CEO is a grave weakness (a *systempunkt* in global guerrilla lingo). The CEO's centrality to the corporate network makes him/her a single point of failure for the entire organization. Another is that executives in most of the western world are very soft targets. Easy to find (Google and Google maps), easy to isolate, and easy to kill...[80]

And the capability of drones is rising at the same time their cost falls:

> Low cost drones flying at very low levels combine extremely high accuracy and extremely difficult targets. They are, in effect, a poor man's cruise missile. In the 80's, the USSR found that the costs of an air defense system required to defend against US cruise missiles was completely beyond their means. While this is on a much smaller scale, it still radically expands the costs.[81]

The clear implication is that, if drones present a comparable threat to hard targets in the U.S. or American hard military targets abroad, then the USSR may well have not been the last superpower to bankrupt itself trying to build a viable defense against such weapons.

The concept of Assassin's Mace weapons, which we discussed in an earlier section, applies more broadly to the vulnerability of military technologies of imperial control to cheap countermeasures. And it casts serious doubt on the prospects for success of any effort at repression on a global scale. The leading powers in the emerging bloc coalescing against the Sole Remaining Superpower are providing sophisticated technologies to small states that come under fire from the Empire.

A good example is the Russian SS-N-22 Sunburn missile, which the Russians have sold to China and Iran. The missile is claimed by some to be potentially lethal to aircraft carriers. The Chinese are in process of introducing an even more lethal missile, the Dongfeng 21-D, designed explicitly for its carrier-killing capability. The purpose is to neutralize U.S. carrier groups in up to 3000k from the Chinese coast. At the estimated cost of production, about 10,000 of them could be produced for the price of a single aircraft carrier.[82]

> Considering the implications and significant threat of China's new generation of carrier-killing missiles, [U.S. Naval War College Professor Toshi] Yoshihara foresees the possibility that they "could have

2, 2013 <http://globalguerrillas.typepad.com/globalguerrillas/2013/09/how-to-deal-with-countries-that-use-chemical-weapons-make-it-personal.html>.

[80] Robb, "It's Open Season on the Tech Elite," *Global Guerrillas*, March 2, 2015 <http://globalguerrillas.typepad.com/globalguerrillas/2015/03/its-open-season-on-the-tech-elite.html>.

[81] John Robb, “JOURNAL: Iron Dome and Magic Wand vs. the Parthian Shot,” *Global Guerrillas*, March 13, 2012 <http://globalguerrillas.typepad.com/globalguerrillas/2012/03/journal-iron-dome-and-magic-wand-vs-the-parthian-shot.html>.

[82] David Cohen, “China Confirms Carrier-Killer,” *The Diplomat*, July 15, 2011 <http://the-diplomat.com/china-power/2011/07/15/china-confirms-carrier-killer/>.

> an enduring psychological effect on U.S. policymakers. It underscores more broadly that the U.S. Navy no longer rules the waves as it has since the end of World War II. The stark reality is that sea control cannot be taken for granted anymore."[83]

> In a conflict, the U.S. Aegis destroyers and cruisers that accompany aircraft carriers could be used to foil anti-ship missiles with SM-3 interceptor rockets, experts say.
>
> But [Naval strategy consultant Paul] Giarra noted that interceptor capacity on Aegis-equipped ships isn't enough to reliably defend against a volley of well-placed anti-ship ballistic missiles.[84]

Another tipping point on the geopolitical level is the increasing threat of defection from neoliberalism by "failed states" on the European periphery. In Spain the Podemos party has emerged from the M-15 movement with 8% of the vote in EU elections as the number four party in their parliamentary system and winning five seats in the European parliament. Ideologically, it is closer to Subcommandante Marcos and the horizontalism of M-15 and Occupy than to anything on the more conventional Left.[85] Meanwhile the Syriza Party in Greece, similarly an outgrowth of the Syntagma movement, got 26% of the vote in the May 2014 EU Parliament elections. And members of the EU Parliament from Podemos and Syriza are closely associated with the M-15 and Syntagma movements.[86]

Returning to our previous discussions of hierarchy becoming more brittle in response to attack in the war between networks and hierarchies, the vulnerability of the state to the human factor extends much more broadly than the narrow question of superiority in innovation. It extends to questions of internal dissension, loss of morale, and a high rate of defection (not to mention internal leaks, sabotage, etc.) among low-level functionaries demoralized by a perpetual war of terror against their own domestic populations. The danger, for the ruling class, is something like the defection of the Winter Palace guards in the Bolshevik Revolution.

Vinay Gupta argues that fighting a networked resistance movement, in the current technological environment, increasingly puts both repressive states and their general populations in a state of cognitive dissonance. This is an edited version of a Twitter chat I had with him, streamlined into blog post format:

> **GUPTA:** 1> No national government is capable of planning clearly for the horror of resource wars between China, America and Europe/Russia.
>
> 2> Therefore, other narratives are being created to cover these inevitable economic and standard-of-living conflicts: drug war, terrorism.
>
> 3> This is why so much of the war seems to be huge amounts of money and manpower for totally ineffective results: immoral == blinding self.
>
> The implication is that a moral side – even a smaller one – could out-compete the Great Powers because moral ground = intellectual clarity. The strategic advantage of a moral war is the ability to think clearly about the ends required to meet a genuinely justified end….
>
> Now refactor that through national politics: the government is stupid *because* the government is evil. Clarity would reveal it as such. The implication is, frankly, that you cannot be smart unless you're going to be good, excepting the genuinely evil who know that they are....
>
> This is important, even though it seems simple, because it's *a moral asymmetry in warfare* – it's a reason to believe the good guys do win. In a conflict, the side which can bear to define it's goals clearly can then plot a strategy to attain them. It can win. You can't win a war who's purpose you cannot bear to define: the Americans in Iraq defined fighting with their eyes closed: empire narrative.

[83] Terrence Aym, "US Navy Stunned: Deadly new Chinese Missiles can Sink Every US Supercarrier," OpEd News, August 7, 2010 <http://www.opednews.com/articles/US-Navy-stunned-Deadly-ne-by-Terrence-Aym-100807-781.html>.

[84] Erik Slavin, "New Chinese anti-ship missile may complicate relations with U.S.," *Stars and Stripes*, July 19, 2010 <http://www.stripes.com/news/new-chinese-anti-ship-missile-may-complicate-relations-with-u-s-1.111552>.

[85] Cristina Flesher Fominaya, ""Spain is Different": Podemos and 15-M," *London School of Economics and Political Science*, January 4, 2014 <http://blogs.lse.ac.uk/eurocrisispress/2014/06/04/spain-is-different-podemos-and-15-m/>.

[86] Srecko Horvat, "The return of the Left in Europe?" *Social Network Unionism*, June 11, 2014 <https://snuproject.wordpress.com/2014/06/11/the-return-of-the-left-in-europe-by-srecko-horvat/>.

Now, what this represents is an opportunity to develop new fundamental doctrine based on whole-of-society offensive/defensive engagement. There is room here for a new moral philosophy, a doctrine of war that cannot easily be used to empower evil regimes. Seriously….

Here's my question: can soldiers who do not understand their purpose out-compete those who do? Answer: probably not. Poor strategic thinking….

What I'm driving at is a moral limitation which command-and-control evolved to get around: wars for the goals of the ruling European classes. And that stuff is all baked into the military, right down to the bone. But we *know* from Deming that Understanding & Equality = Quality. If you look at a modern military through Deming's eyes, the entire thing is a machine for producing cockups....

In short,a transparent and cooperative battle space is only possible when soldiers individually understand their true purpose and objectives. Because if you feel you're in the wrong, you can't bear to look at the data, and you live in a fantasy world: SNAFU and hierarchy lies.

CARSON: ...Your train of thought suggests fascist regimes can't afford to let their soldiers be smart; they will therefore be defeated by networks. Soldiers fighting for an authoritarian cause have morale trouble from cognitive dissonance, and can't be trusted with initiative. That's the same thing Julian Assange said about hierarchies becoming more brittle and opaque to themselves, in response to attack — wasn't it?

GUPTA: And the side which can bear to face its actions head-on can see the battlespace clearly right down to each individual fighter. The more monitoring and intelligence gear you have, the worse it gets: the intel analysts can't bear to think about what they're seeing. Moral failure means your front lines get shit information: self-deception is a critical strategic failure which your enemies can exploit.

In short: hit them in their cognitive dissonance. Map it as a strategic asset, and whip ass on it as hard as possible.

What I am suggesting here is simple: TECHNOLOGY EMPOWERS MORAL WAR. I think we may find that it cripples immoral war: evidence is current....

Now, imagine the Iraqis and the Afghans had a a vast supply of shoulder-launched anti-aircraft weapons and good quality anti-tank gear. All that stuff is cheap, weapon cost less than 1% of target cost, say. They did this based on RPGs and landmines. Imagine if they'd had kit.

Why? To have effective swarm response, fast, fluid tactics, you need a general consensus on strategy, which comes from political clarity....

Now, let's take this and look at post-economic Greece, Spain and Italy. Italy is city states. Greece and Spain nearly went Anarchist nr WW2. With a moral case for war in those nations, they could be the first testbeds for first world populations fighting for new politics. Shit….

If you just dump the data into a bucket, in a transparent battle space, the moral clarity is what results in coordination at the macro scale. That efficient swarm coordination requires shared goals and common knowledge, and IMMORAL WAR has split goals in the force and secrecy....

CARSON [after the fact]: Same thing goes for the battlefields at Oakland, UC Davis, NYC. For the first time, the public is forced to confront what that "thin blue line" really does. Moral unity between the public and those sainted "first responders" is disrupted.

GUPTA: ...[S]ide with lower cognitive dissonance wins….

Conclusion: a shared, rational moral reason for war is an essential part of winning in a transparent battlespace because it enables thinking. And particularly in urban environments, the pace of war requires decision-making to be done as far forwards as possible, and in teams....

Tech provides coordination, which makes Just Following Orders a less adaptive response than looking at the map and acting. Power shift.

...That's actually the key, right there: the military was constructed to magnify the will of a Sovereign, and when that breaks down, boom. Because a sufficiently transparent society, or battlespace, highlights the conflicts of interest between Sovereigns and Soldiers....

In short, for exactly the same reason Communism was out-competed by Capitalism, Networked societies will out-compete Capitalist ones. It's only the unified moral basis which allows for a networked fighting force to find effective unity: without that,transparency tears apart.

> I keep saying it in different ways: when everybody can see everything, the goal of transparent battlespace, the good guys tend to win. Because what I'm saying here is very simple: the Americans are probably going to be the Bad Guys on the next outing. #NDAA
>
> And I think it's important to understand their failings in Iraq and Afghanistan as being optimistic signs for global Liberty. Learn & repeat.
>
> Conclusion of conclusion: there is a decent chance that Netwar will cripple American offensive capability in unjust wars due to moral loss….
>
> War, by the people, for the people, and of the people must be the inevitable consequence of transparency on the battle field. Because, to win, the left hand must know what the right hand is doing, and the right hand is stuffing money down Dick Cheney's pants.[87]

The effect on hierarchies' internal communications is much like John Boyd described in informational terms earlier in this chapter. In fact Boyd himself referred to a similar effect in moral warfare:

> *Physically* we can *isolate* our adversaries by severing their communications with outside world as well as by severing their internal communications to one another....
>
> *Morally* our adversaries *isolate* themselves when they visibly improve their well-being to the detriment of others... by violating codes of conduct or behavior patterns that they profess to uphold or others expect them to uphold.[88]
>
> Such contradictions within ourselves "destroy our internal harmony" and "paralyze us."[89]

Erica Chenoweth argues that the point of nonviolent civil resistance is not so much to persuade the rulers as 1) to "expose the lie" to the public and thereby undermine the ideological basis for compliance, and 2) demoralize officials within the regime so that they stop enforcing its directives.

> **2. Every oppressive regime has ambivalent insiders**. All regimes are, in the end, totally dependent on the obedience of those who support it—economic, military, media, and civilian elites. When such insiders (Sinna, Plutarch, etc.) stop obeying the regime, and its pillars of support begin to crack, it's the beginning of the end. Insiders, too, are often intimately familiar with the regime's vulnerabilities and are therefore quite well-disposed to challenge it.
>
> **3. Power is essentially psychological**. No regime can repress all of the people all of the time. So many regimes rely on terror to suppress dissent. And by and large, it works—until it doesn't.
>
> **4. It's all about exposing the lie**. The psychological power of terror ends when people simply decide to stop being afraid. Then it's all over. Like in the books when the Districts end up rebelling once they realize that 1) the Capitol is (and always has been) vulnerable to challenge; (2) all information coming out of the Capital is (and always was) lies; and (3) all they have to do (now and ever) is coordinate their uprisings. The people of the districts realized they had the power all the time. As soon as this "cognitive liberation" was achieved, it was all over for the Panem of the Hunger Games.[90]

Horizontal, networked communications technologies enable unprecedented speeds of phase transition in public consciousness. Doug McAdam coined the term "Cognitive Liberation" for "a process in which people suddenly and collectively decide that they are no longer afraid, that their recent fear or apathy was based

[87] Kevin Carson, "Vinay Gupta: The Authoritarian Cause Will Be Defeated by Its Own Cognitive Dissonance," *P2P Foundation Blog*, January 17, 2012 <http://blog.p2pfoundation.net/vinay-gupta-the-authoritarian-cause-will-be-defeated-by-its-own-cognitive-dissonance/2012/01/17>.

[88] John Boyd, "The Strategic Game of ? and ?" (June 1987)," p. 47

[89] *Ibid.*, p. 55.

[90] Erica Chenoweth, "Five Lessons from 'The Hunger Games'," *Rational Insurgent*, June 11, 2012 <http://rationalinsurgent.wordpress.com/2012/06/11/five-lessons-from-the-hunger-games/>. She writes elsewhere "Nonviolent resistance does not necessarily succeed because the movement convinces or converts the opponent. It succeeds when the regime's major sources of power -- such as civilian bureaucrats, economic elites, and above all the security forces —stop obeying regime orders." "Think Again: Nonviolent Resistance," *Foreign Policy*, August 24, 2011 <http://www.foreignpolicy.com/articles/2011/08/24/think_again_nonviolent_resistance>.

on lies, and that there is no going back to the old ways of thinking."[91] Once a critical mass of the public decides that change is inevitable, it is. And with networked communications technology, that critical mass may coalesce suddenly and unexpectedly.

Although we've so far discussed the problem of cognitive dissonance largely in terms of cohesion between the rulers and domestic population, or between the rulers and rank-and-file security functionaries who enforce their will, it also applies to internal cohesion within the ruling elite itself. Things are complicated for the U.S. ruling elite (I make the assumption that the U.S., as global military hegemon and core state of the global corporate system, will be the center of any effort at repression), in a scenario of mass repression of the domestic population or aggressive foreign wars against peaceful secessionists from the corporate world order, by the problem of internal divisions.

The situation is further complicated, at the Empire's core, by the contaminating effects of the surrounding American society's culture. I hate to sound like an American exceptionalist. But while it's no doubt easy to find a sufficient number of specialized functionaries in uniform who are willing to waterboard or provide "technical advice" to Pinochet, I doubt there are a sufficient number to provide a stable and internally coherent pool of functionaries to serve the daily needs of such a system. When you look at the sheer numbers of grunts in uniform that are required—police or military—I suspect a majority of them would be so contaminated by the residual effects of Midwestern checkered tablecloths and apple pie, civics book rhetoric about "democracy," etc., as to be quite unreliable in a Winter Palace guards scenario. And that's not even counting the enormous number of cubicle drones required to carry out the administrative functions of the corporate state. So there would probably be a considerable rate of open defiance, and a much higher rate of quiet defection and internal sabotage.

This is all just further illustration of Assange's general observation, noted earlier, about bureaucracies closing in on themselves because they cannot trust their own lower-level functionaries. Hierarchies respond to outside attacks by becoming even more centralized, authoritarian and brittle. And they respond to internal defection, leaks and sabotage by becoming more opaque to themselves, adopting more cumbersome and slow-moving decision-making procedures, and cutting off increasing numbers of decisionmakers from the flow of information required to make intelligent decisions. It's quite likely the bureaucracy governing Skynet would end up looking a lot like that of Neal Stephenson's fictional Feds in *Snow Crash*. Or the fictional example we saw above from *Brazil*, of the Ministry of Works attempting to plug a hole created by the Ministry of Information: "Bloody typical—they went metric again without telling us!"

Another question concerns the possible emergence of new, authoritarian institutions in the power vacuum left by the destruction of the previous ones.

In Murray Bookchin's typology of revolutions, revolutionary movements generate local organs of self-management and self-governance: soviets, workers' factory committees, neighborhood assemblies, and so forth. Orwell's description of Barcelona in the July days of 1936, in *Homage to Catalonia*, is a good illustration. Unfortunately, the next step is usually for a new revolutionary regime to consolidate its power, and either coopt or liquidate the organs of self-governance, and proclaim itself the only legitimate institutional representative of the revolution—now that the situation has been "normalized." It's a common pattern: the Thermidorean Reaction and the Directory in France, the Bolsheviks' liquidation of the Workers Opposition and parties of the libertarian Left and suppression of the Kronstadt Revolt, etc.

> These are not simple consequences of a revolution happening "unprepared", so to speak. Indeed; they happen chiefly when small but well-organised groups are able to gain enough traction to take over the violent enforcement apparatus from the old regime. Those small groups usually have a very well-defined agenda, and they tend to be extremely dogmatic about that agenda.[92]

[91] Chenoweth, "'Cognitive Liberation' in Syria?" *Rational Insurgent*, June 18, 2012 <http://rationalinsurgent.wordpress.com/2012/06/18/cognitive-liberation-in-syria/>.

[92] "Revolutions Deserved," anarchism.is, November 16, 2011 <http://anarchism.is/2011/11/16/revolution.html>.

But the networked revolution prefigured by the Zapatistas, and currently presenting itself in the form of the Arab Spring and Occupy Wall Street, is the first in history in which the technical means which made the revolution possible in the first place also help to make the successor society ungovernable by any would-be "revolutionary regime."

III. The Question of Collapse

The material in the previous section on distributed, modular architectures is relevant to traditional collapse scenarios.

Joseph Tainter argued that the greater the complexity, the more additional complexity is required to deal with it. Increasing complexity is the only way to solve problems -- until you can no longer "afford it."[93]

John Michael Greer's collapse scenario is based largely on Tainter's analysis:

> The central idea of catabolic collapse is that human societies pretty consistently tend to produce more stuff than they can afford to maintain.... As societies expand and start to depend on complex infrastructure to support the daily activities of their inhabitants..., the maintenance needs of the infrastructure and the rest of the society's stuff gradually build up until they reach a level that can't be covered by the resources on hand.
>
> It's what happens next that's crucial to the theory. The only reliable way to solve a crisis that's caused by rising maintenance costs is to cut those costs, and the most effective way of cutting maintenance needs is to tip some fraction of the stuff that would otherwise have to be maintained into the nearest available dumpster. That's rarely popular, and many complex societies resist it as long as they possibly can, but once it happens the usual result is at least a temporary resolution of the crisis. Now of course the normal human response to the end of a crisis is the resumption of business as usual, which in the case of a complex society generally amounts to amassing more stuff. Thus the normal rhythm of history in complex societies cycles back and forth between building up, or anabolism, and breaking down, or catabolism. Societies that have been around a while – China comes to mind – have cycled up and down through this process dozens of times, with periods of prosperity and major infrastructure projects alternating with periods of impoverishment and infrastructure breakdown.
>
> A more dramatic version of the same process happens when a society is meeting its maintenance costs with nonrenewable resources.... Sooner or later you run into the limits of growth; at that point the costs of keeping wealth flowing in from your empire or your oil fields begin a ragged but unstoppable increase, while the return on that investment begins an equally ragged and equally unstoppable decline; the gap between your maintenance needs and available resources spins out of control, until your society no longer has enough resources on hand even to provide for its own survival, and it goes under.
>
> That's catabolic collapse. It's not quite as straightforward as it sounds, because each burst of catabolism on the way down does lower maintenance costs significantly, and can also free up resources for other uses. The usual result is the stairstep sequence of decline that's traced by the history of so many declining civilizations—half a century of crisis and disintegration, say, followed by several decades of relative stability and partial recovery, and then a return to crisis; rinse and repeat, and you've got the process that turned the Forum of imperial Rome into an early medieval sheep pasture.[94]

Greer tacitly assumes that "progress" equates to "increased complexity and capital-intensiveness," and that resource constraints translate into a less advanced way of life. So he shares certain unexamined assumptions with thinkers like Joseph Schumpeter, John Kennneth Galbraith and Alfred Chandler—what might be called the Whig Theory of Industrial History.

> Could an electrical grid of the sort we have today, with its centralized power plants and its vast network of wires bringing power to sockets on every wall, remain a feature of life throughout the indus-

[93] "Interview with Joseph Tainter on the Collapse of Complex Societies," <http://p2pfoundation.net/Interview_with_Joseph_Tainter_on_the_Collapse_of_Complex_Societies>.

[94] John Michael Greer, "The Onset of Catabolic Collapse," *The Archdruid Report*, January 19, 2011 <http://thearchdruidreport.blogspot.com/2011/01/onset-of-catabolic-collapse.html>.

> trial world in an energy-constrained future? If attempts to make sense of that future assume that this will happen as a matter of course, or start with the unexamined assumption that such a grid is the best (or only) possible way to handle scarce energy, and fixate on technical debates about whether and how that can be made to happen, the core issues that need to be examined slip out of sight. The question that has to be asked instead is whether a power grid of the sort we take for granted will be economically viable in such a future – that is, whether such a grid is as necessary as it seems to us today; whether the benefits of having it will cover the costs of maintaining and operating it; and whether the scarce resources it uses could produce a better return if put to work in some other way.[95]

It's not that Greer doesn't recognize the likelihood of shifting to a more distributed, less resource-intensive power system—perhaps a mix of centralized grids in concentrated urban areas and local generating facilities at the point of consumption in rural areas. He specifically refers to it in the same post. It's that he assumes such a system is incompatible with the Internet, and that a scalable Internet using such a power infrastructure is outside the realm of the possible.

Greer's scenario ignores a central reality: the rapid implosion, governed by something analogous to Moore's law, in the amount of "stuff" required to organize basic communication functions. When you break the linear relationship between the cost of "stuff" in an infrastructure and the functions it performs, all bets are off.

Greer and Pollard assume a remarkably static view of technology, in their projections of catabolic collapse of the Internet. Even their pessimistic scenarios assume the basic infrastructure won't start to collapse on a significant scale until the mid-21st century. So their collapse scenarios are only meaningful on the assumption that the Internet's physical infrastructure is organized, thirty or forty years from now, on the same centralized, expensive and capital-intensive model as at present.

This neglects a number of considerations. It neglects the possibility that the present level of capital-intensiveness in our basic infrastructures results not from some inherent technological imperative, but from the state tipping the balance towards one of the least efficient among a number of competing models. It neglects the possibility that the physical infrastructures of the Internet will plummet faster than the resources for maintaining it. It neglects the extent to which the open-source community is already actively developing the technologies of transition to a cheap, distributed infrastructure. And it underestimates the extent to which much lower cost, underutilized infrastructures like railroads and the Internet offer an alternative to the older, capital-intensive infrastructures undergoing catabolic collapse. One major difference between the present situation and the fall of Rome: Rome had no cheaper infrastructures as an obvious, low-hanging fruit alternative to the imperial highways and aqueducts.

Greer's catabolic collapse scenario—as illustrated by the example of the Easter Islanders—also assumes a relatively small amount of slack, at crisis points, in terms of available uncommitted resources that can be used to convert to less resource-intensive ways of doing things.

> On Easter Island, as I think most people know by now, the native culture built a thriving society that got most of its food from deepwater fishing, using dugout canoes made from the once-plentiful trees of the island. As the population expanded, however, the demand for food expanded as well, requiring more canoes, along with many other things made of wood. Eventually the result was deforestation so extreme that all the tree species once found on the island went extinct. Without wood for canoes, deepwater food sources were out of reach, and Easter Island's society imploded in a terrible spiral of war, starvation, and cannibalism.
>
> It's easy to see that nothing would have offered as great an economic advantage to the people of Easter Island as a permanent source of trees for deepwater fishing canoes. It's just as easy to see that once deforestation had gone far enough, nothing on Earth could have provided them with that advantage. Well before the final crisis arrived, the people of Easter Island – even if they had grasped the nature of the trap that had closed around them – would have faced a terrible choice: leave the last few big

[95] John Michael Greer, "The Logic of Abundance," *The Archdruid Report*, March 24, 2010 <http://thearchdruidreport.blogspot.com/2010/03/logic-of-abundance.html>.

> trees standing and starve today, or cut them down to make canoes and starve later on. All the less horrific options had already been foreclosed.[96]

Greer's treatment of the Internet as an enormously costly infrastructure of energy-devouring server farms, doomed to be abandoned by most as an expensive toy for the rich and eventually left to collapse altogether, seems to be a gross exaggeration as well. It turns out that the energy-intensiveness of the Internet is mostly an urban legend, resulting mainly from the work of a couple of right-wing coal industry shills over a decade ago. The Internet, in fact, accounts for a quite modest share of total electricity consumption and has produced net savings from dematerializing many functions.[97]

And although the two have mostly coincided in the past, Tainter's model of society reaching a new equilibrium at a lower level of complexity does not necessarily mean less sophisticated technology. In fact the trend now is toward increased simplicity and resilience through modular architecture.

The old centralized corporate-state infrastructure is indeed undergoing a catabolic collapse scenario described quite well by Tainter's framework of “catabolic collapse.” Consider John Robb's prediction of what will happen to the old electrical power distribution infrastructure:

> - **Nothing new will be built.** We are just realizing we are bankrupt. Our collective wealth has been squandered and stolen, never to be seen again. This means the investment dollars available for improvements and expansion of the electricity grid don’t exist. What does get funded, gets stopped by a justified NIMBY (not-in-my-backyard) movement. So, even if there were a plentiful, sustainable, and inexpensive new supply of centralized electricity production available, it’s very likely it would never reach the customers that would use it.
> - **The grid will fall into disrepair and become intermittently available.** As we become poorer, funding for the maintenance of the national grid will evaporate. As a result, we will see more breakdowns. Further, we will see sources of centralized electricity supply become intermittent, as suppliers go offline due to sagging demand or government attempts to regulate prices in a fragile economy.
> - **The grid will be intentionally broken.** As our economies fall deeper into depression, our political and social systems will follow them into the abyss. Attacks on the grid infrastructure will become more frequent as criminals strip lines of precious metals and domestic guerrillas attack the lines cause disruption. [98]

[96] John Michael Greer, “The Economics of Decline,” *The Archdruid Report*, May 20, 2009 <http://thearchdruidreport.blogspot.com/2009/05/economics-of-decline.html>.

[97] Joe Romm, “Debunking the myth of the internet as energy hog, again: How information technology is good for climate,” ThinkProgress.org, June 21, 2013 <http://thinkprogress.org/climate/2010/06/21/206254/internet-energy-use-myth/>. Romm quotes his friend Jonathan Koomey, who has done most of the work debunking the energy-hog myth:

> Back in 1999, a cleverly written article was published in *Forbes* magazine, claiming that the Internet used 8% of all US electricity, that all computers (including the Internet) used 13% of US electricity, and that this total would grow to half of all electricity use in ten to twenty years....
>
> Joe Romm, Amory Lovins, and I spent a few person years of effort between us demonstrating in the scientific literature that these assertions were all false (for a compilation of that work, go here). The Internet, as defined by the *Forbes* authors, used less than 1% of US electricity in 2000, all computers used about 3%....
>
> ...[W]hile it’s a good idea to make computers energy efficient, it’s even more important to focus on the capabilities information technology (IT) enables for the broader society. Computers use a few percent of all electricity, but they can help us to use the other 95+% of electricity (not to mention natural gas and oil) a whole lot more efficiently.
>
> As an example of this latter point, consider downloading music versus buying it on a CD. A study that is now “in press” at the peer-reviewed *Journal of Industrial Ecology* showed that the worst case for downloads and the best case for physical CDs resulted in 40% lower emissions of greenhouse gases for downloads when you factor in all parts of the product lifecycle. When comparing the best case for downloads to the best case for physical CDs, the emissions reductions are 80%.... In general, moving bits is environmentally preferable to moving atoms, and whether it’s *dematerialization* (replacing materials with information) or *reduced transportation* (from not having to move materials or people, because of electronic data transfers or telepresence) IT is a game changer.

The difference is that, unlike previous collapses (the classic example is the catabolic collapse of the Western Roman Empire) the old infrastructure this time isn't all there is.

For the first time there is an alternative. The old system, indeed, has responded to stresses with increased complexity (i. e., adding more and more parts which require more and more organization). But new network technologies have created unprecedented possibilities for responding to complexity through decentralizing and hardening, modularization, and degovernancing. And what amounts to a new, distributed infrastructure is emerging within the old, dying society.

Tainter's equilibrium at a lower level of simplification can be achieved, not only through a regressive decrease in connectedness, but by adopting more less capital-intensive and more resilient modular architectures.

Conclusion

The implosion of capital outlays associated with the desktop revolution, and the virtual disappearance of transaction costs of coordinating action associated with the network revolution, have (as Tom Coates said above) eliminated the gap between what can be produced in large hierarchical organizations and what can be produced at home in a wide range of industries: software, publishing, music, education, and journalism among them.

The practical significance of this, which we shall develop in the following chapters, is that many of the functions of government can be included in that list. The central theme of this book is the potential for networked organization to constrain the exercise of power by large, hierarchical institutions in a way that once required the countervailing power of other large, hierarchical institutions.

[Draft last modified October 19, 2015]

[98] John Robb, “Is 8 Hours a Day of Electricity in Your Future?” *Resilient Communities*, March 20, 2012 <http://www.resilientcommunities.com/is-8-hours-of-electricity-a-day-in-your-future/>.