Conflicting Diagrams

By Alexander R. Galloway

No. 29 – 2003

Abstract

Throughout the years new diagrams have appeared as solutions or threats to existing ones. Bureaucracy and hierarchy are diagrams; networks are too. In recent decades the primary conflict between organizational designs has been between hierarchies and networks, an asymmetrical war exemplified most starkly in the war against terrorism. But what happens when "the powers that be" evolve from centralized hierarchies into networked power? For Alex Galloway in the future we are likely to experience a general shift downward into a new bilateral organizational conflict-networks fighting networks.

> "Netwar is about the Zapatistas more than the Fidelistas, Hamas more than the Palestine Liberation Organization (PLO), the American Christian Patriot movement more than the Ku Klux Klan, and the Asian Triads more than the Costa Nostra."[1]
>
> *--John Arquilla & David Ronfeldt*

Throughout the years new diagrams (also called graphs or organizational designs) have appeared as solutions or threats to existing ones. Bureaucracy is a diagram. Hierarchy is one too, so is peer-to-peer. Designs come and go, useful asset managers at one historical moment, then disappearing, or perhaps fading only to reemerge later as useful again. The Cold War was synonymous with a specific military diagram--bilateral symmetry, mutual assured destruction (MAD), massiveness, might, containment, deterrence, negotiation; the war against drugs has a different diagram--multiplicity, specificity, law and criminality, personal fear, public awareness.

In this diagramatic narrative it is possible to pick sides and describe one diagram as the protagonist and another as the antagonist. Thus the rhizome is thought to be the solution to the tree,[2] the wildcat strike the solution to the boss's control, Toyotism[3] the solution to institutional bureaucracy, and so on. Alternately, terrorism is thought to be the only real threat to state power, the homeless punk-rocker a

threat to sedentary domesticity, the guerrilla a threat to the war machine, the temporary autonomous zone a threat to hegemonic culture, and so on.

This type of conflict is in fact a conflict between different social structures, for the terrorist threatens not only through fear and violence, but specifically through the use of a cellular organizational structure, a distributed network of secretive combatants, rather than a centralized organizational structure employed by the police and other state institutions. Terrorism is a sign that we are in a transitional moment in history. (Could there ever be anything else?) It signals that historical actors are not in a relationship of equilibrium, but instead are grossly mismatched.

It is often observed that, due largely to the original comments of networking pioneer Paul Baran, the Internet was invented to avoid certain vulnerabilities of nuclear attack. In Baran's original vision, the organizational design of the Internet involved a high degree of redundancy, such that destruction of a part of the network would not threaten the viability of the network as a whole. After World War II, strategists called for moving industrial targets outside of urban cores in a direct response to fears of nuclear attack. Peter Galison calls this dispersion the "constant vigilance against the re-creation of new centers."[4] These are the same centers that Baran derided as an "Achilles Heel"[5] and what he longed to purge from the telecommunications network.

"City by city, country by country, the bomb helped drive dispersion,"[6] Galison continues, highlighting the power of the A-bomb to drive the push towards distribution in urban planning. Whereas the destruction of a fleet of Abrams tanks would certainly impinge upon Army battlefield maneuvers, the destruction of a rack of Cisco routers would do little to slow down broader network communications. Internet traffic would simply find a new route, thus circumventing the downed machines.[7]

(In this way, destruction must be performed absolutely, or not at all. "The only way to stop Gnutella," comments WiredPlanet CEO Thomas Hale on the popular file sharing protocol, "is to turn off the Internet."[8] And this is shown above in our examination of protocol's high penalties levied against deviation. One is completely compatible with a protocol, or not at all.)

Thus the Internet can survive attacks not because it is stronger than the opposition, but precisely because it is weaker. The Internet has a different diagram than nuclear attack; it is *in a different shape*. And that new shape happens to be immune to the older.

All the words used to describe the World Trade Center after the attacks of September 11, 2001 revealed its design vulnerabilities vis-ˆ-vis terrorists: it was a tower, a center, an icon, a pillar, a hub. Conversely, terrorists are always described with a different vocabulary: they are cellular, networked, modular, and nimble. Groups like Al-Qaeda specifically promote a modular, distributed structure based on

small autonomous groups. They write that new recruits "should not know one another," and that training sessions should be limited to "7 - 10 individuals." They describe their security strategies as "creative" and "flexible."[9]

This is indicative of two conflicting diagrams.

The first diagram is based on the strategic massing of power and control, while the second diagram is based on the distribution of power into small, autonomous enclaves. "The architecture of the World Trade Center owed more to the centralized layout of Versailles than the dispersed architecture of the Internet," wrote Jon Ippolito after the attacks. "New York's resilience derives from the interconnections it fosters among its vibrant and heterogeneous inhabitants. It is in decentralized structures that promote such communal networks, rather than in reinforced steel, that we will find the architecture of survival."[10] In the past the war against terrorism resembled the war in Viet Nam, or the war against drugs--conflicts between a central power and an elusive network. It did not resemble the Gulf War, or World War II, or other conflicts between states.

"As an environment for military conflict," the *New York Times* reported, "Afghanistan is virtually impervious[11] to American power." (In addition to the stymied US attempt to route Al-Qaeda post-September 11th is the failed Soviet occupation in the years following the 1978 coup, a perfect example of grossly mismatched organizational designs.) Today being "impervious" to American power is no small feat.

The category shift that defines the difference between state power and guerilla force shows that through a new diagram, guerillas, terrorists and the like can gain a foothold against their opposition.

But as Ippolito points out this should be our category shift too, for anti-terror survival strategies will arise not from a renewed massing of power on the American side, but precisely from a distributed (or to use his less precise term, decentralized) diagram. Heterogeneity, distribution, communalism are all features of this new diagramatic solution.

In short, *the current global crisis is one between centralized, hierarchical powers and distributed, horizontal networks*. John Arquilla and David Ronfeldt, two researchers at the RAND Corporation who have written extensively on the hierarchy-network conflict, offer a few propositions for thinking about future policy:

- Hierarchies have a difficult time fighting networks. [...]
- It takes networks to fight networks. [...]
- Whoever masters the network form first and best will gain major advantages.[12]

These comments are incredibly helpful for thinking about tactical media and the roll of today's political actor. It gives subcultures reason to rethink their strategies vis-a-vis the mainstream. It forces us to rethink the techniques of the terrorist. It also raises many questions, including what happens when "the powers that be" actually evolve into networked power (which is already the case in many sectors).

In recent decades the primary conflict between organizational designs has been between hierarchies and networks, an asymmetrical war. However, in the future we are likely to experience a general shift downward into a new bilateral organizational conflict--networks fighting networks.

"Bureaucracy lies at the root of our military weakness," wrote advocates of military reform in the mid eighties. "The bureaucratic model is inherently contradictory to the nature of war, and no military that is a bureaucracy can produce military excellence."[13]

While the change to a new unbureaucratic military is on the drawing board, the future network-centric military--an unsettling notion to say the least--is still a ways away. Nevertheless networks of control have invaded our life in other ways though, in the form of the ubiquitous surveillance, biological informatization and other techniques.

The dilemma, then, is that while hierarchy and centralization are almost certainly politically tainted due to their historical association with fascism and other abuses, networks are both bad and good. Drug cartels, terror groups, black hat hacker crews and other denizens of the underworld all take advantage of networked organizational designs because they offer effective mobility and disguise. But more and more we witness the advent of networked organizational design in corporate management techniques, manufacturing supply chains, advertisement campaigns and other novelties of the ruling class, as well as all the familiar grass-roots activist groups who have long used network structures to their advantage.

In a sense, then, networks have been vilified simply because the terrorists, pirates and anarchists made them notorious, not because of any negative quality of the organizational diagram itself. In fact, positive libratory movements have been capitalizing on network design protocols for decades if not centuries. The section on the rhizome in *A Thousand Plateaus* is one of literature's most poignant adorations of the network diagram.

Thus future evaluation of conflict in and among diagrams should not be reduced to simple condemnation of one form over another, but instead should flow from, as Jameson wrote, the real conditions of life now and how we feel in our bones it ought to be lived.

Notes

1. John Arquilla & David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: RAND, 2001), p. 6. A similar litany from 1996 reads: "netwar is about Hamas more than the PLO, Mexico's Zapatistas more than Cuba's Fidelistas, the Christian Identity Movement more than the Ku Klux Klan, the Asian Triads more than the Sicilian Mafia, and Chicago's Gangsta Disciples more than the Al Capone Gang" (see John Arquilla & David Ronfeldt, *The Advent of Netwar* [Santa Monica: RAND, 1996], p. 5). Arquilla & Ronfeldt coined the term netwar which they define as "an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age" (see Arquilla & Ronfeldt, *Networks and Netwars*, p. 6).

2. This is Deleuze & Guatari's realization in *A Thousand Plateaus*.

3. For an interesting description of Toyotism, see Manuel Castells, *The Rise of the Network Society* (Oxford: Blackwell, 1996), pp. 157-160.

4. Peter Galison, "War against the Center," *Grey Room* 4, Summer 2001, p. 20.

5. Baran writes: "The weakest spot in assuring a second strike capability was in the lack of reliable communications. At the time we didn't know how to build a communication system that could survive even collateral damage by enemy weapons. RAND determined through computer simulations that the AT&T Long Lines telephone system, that carried essentially all the Nation's military communications, would be cut apart by relatively minor physical damage. While essentially all of the links and the nodes of the telephone system would survive, a few critical points of this very highly centralized analog telephone system would be destroyed by collateral damage alone by missiles directed at air bases and collapse like a house of card." See Paul Baran, Electrical Engineer, an oral history conducted in 1999 by David Hochfelder, IEEE History Center, Rutgers University, New Brunswick, NJ, USA.

6. Galison, "War against the Center," p. 25.

7. *New Yorker* writer Peter Boyer reports that DARPA is in fact rethinking this opposition by designing a distributed tank, "a tank whose principle components, such as guns and sensors, are mounted on separate vehicles that would be controlled remotely by a soldier in yet another command vehicle," (see "A Different War," *The New Yorker*, July 1, 2002, p. 61). This is what the military calls Future Combat Systems (FCS), an initiative developed by DARPA for the US Army. It is described as "flexible" and "network-centric." I am grateful to Jason Spingarn-Koff for bring FCS to my attention.

8. Cited in Gene Kan "Gnutella" in Andy Oram, Ed. *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (Sebastopol: O'Reilly, 2001), p. 99.

9. See *The al-Qaeda Documents: Vol. 1* (Alexandria, VA: Tempest, 2002), pp. 50, 62.

10. Jon Ippolito, "Don't Blame the Internet," *Washington Post*, September 29, 2001, p. A27.

11. Wanting instead American invulnerability to Soviet nuclear power, in 1964 Paul Baran writes that "we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n [communication] stations. If n is made sufficiently large, it can be shown that highly survivable system structures can be built--even in the thermonuclear era." See Paul Baran, *On Distributed Communications: 1. Introduction to Distributed Communications Networks* (Santa Monica, CA: RAND, 1964), p. 16. Baran's point here is that destruction of a network is an all or nothing game. One must destroy all nodes, not simply take out a few key hubs. But the opposite is not true. A network needs only to destroy a single hub within a hierarchical power to score a dramatic triumph. Thus, Baran's advice to the American military was to become network-like. And once it did the nuclear threat was no longer a catastrophic threat to communications and mobility (but remains, of course, a catastrophic threat to human life, material resources, and so on).

12. Arquilla & Ronfeldt, *Networks and Netwars*, p. 15, emphasis removed from original. Contrast this line of thinking with that of Secretary of Defense Robert McNamara in the nineteen sixties, whom Senator Gary Hart described as advocating "more *centralized* management in the Pentagon." See Gary Hart & William Lind, *America Can Win* (Bethesda, MD: Adler & Adler, 1986), p. 14. Or contrast it in the current milieu with the Powell Doctrine, named after four-star general and Secretary of State Colin Powell, which states that any American military action should have the following: clearly stated objectives; an exit strategy; the ability to use overwhelming force; and that vital strategic interests must be at stake. This type of thinking is more in line with a modernist, Clausewitzian theory of military strategy, that force will be overcome by greater force, that conflict should be a goal-oriented act rather than one of continuance, that conflict is waged by state actors, and so on.

13. Gary Hart & William Lind, *America Can Win* (Bethesda, MD: Adler & Adler, 1986), pp. 240, 249.