Networks Versus Hierarchies

- Key propositions:
  - Information revolution erodes hierarchies, favoring and strengthening networks
  - 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

- Key implication: Counternetwar will require very effective interagency mechanisms and operations

This research on the looming challenge of netwar continues to bear out a set of propositions that we identified some time ago about the information revolution and its likely implications (Arquilla and Ronfeldt, 1993):

*The information revolution favors and strengthens networks, while it erodes hierarchies.* The continued explosive growth of political, business, social, and other networks that benefit societies, as well as of criminal, terrorist, and other networks that threaten them confirm this proposition, as does the concomitant “softening” of traditional statist institutions.

*Hierarchies have a difficult time fighting networks.* Examples of this appear across the conflict spectrum. Some of the best may be found in the generally failing efforts of many governments to deal with TCOs. The persistence of religious revivalist movements, as in Algeria, often in the face of unremitting statist opposition, shows the robustness of the network form, on defense and offense. The Zapatista move-
ment in Mexico, with its legions of supporters and sympathizers among local and transnational NGOs, shows that social netwar can put a democratizing autocracy on the defensive and pressure it to continue adopting reforms.

*It takes networks to fight networks.* The case of the Southeast Asian pirates makes this point well. The first effort to cope with the resurgence of piracy was state-centered and failed miserably. The establishment of a transnational counter-piracy network proved successful in a relatively short time. This proposition may well be analogous to others in military doctrine, particularly that “it takes a tank to fight a tank.”

*Whoever masters the network form first and best will gain major advantages.* In these early years of the information age, those adversaries who have advanced at networking (e.g., criminals, terrorists, and activists) are enjoying a marked increase in their power relative to state agencies. While networking once allowed them simply to keep from being eradicated, it now allows them to compete on more nearly equal terms with states and with other hierarchically oriented adversaries. The history of Hamas and that of the Cali cartel illustrate this.

The information revolution is about both technology and organization. While technology innovation is revitalizing the network form, one must not ignore the importance of organizational innovation. Indeed, every information revolution has involved an interplay between technology and organization that affects who wins and loses. For example, a millennium before the printing revolution, the early Catholic Church had a networked organization that confronted and overcame brutal opposition from one of history’s most successful hierarchies, the Roman Empire. The Church later developed its own great hierarchies, ironically making it susceptible to dissent as the printing revolution emerged in the 16th century.

Today, those who want to defend against netwar will, increasingly, have to adopt weapons, strategies, and organizational designs like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age. These principles depend to some extent upon technological breakthroughs, but mainly on a willingness to innovate organizationally.

For U.S. policy, an early implication of our work is that counternetwar will require very effective interagency operations, which by their very nature involve networked structures. It should not be necessary, or desirable, to replace all hierarchies with networks. Rather, the challenge will be to blend these two forms skillfully, while retaining enough central authority to encourage and enforce adherence to truly networked processes. In this manner, states may come to be better prepared to confront the multitude of new threats emerging in this information age.
Current Interagency Designs Are Instructive . . . But How Adequate Are They?

- Past difficulty in moving from hierarchical “stove-pipe” to flat “dish” designs in netwar-related areas
  - Counterterrorism
  - Counternarcotics
  - Counterproliferation

- New issue areas add to complications, partly because of involvement of activist NGOs
  - Peacetime contingency operations
  - Computer and cyberspace security

Research needed to identify and refine the options for organization, doctrine, and strategy—for domestic and foreign operations

In recent years, efforts have been made to develop and streamline truly interagency task forces to cope with terrorists, drug traffickers (and other TCOs), and WMD proliferators—all areas replete with netwar-related characteristics. By any set of measures, however, results have proven mixed.

Terrorism has come to America, from the World Trade Center in New York to the Murrah Federal Building in Oklahoma City. Drug flows continue unabated, with production and transshipment sites now being moved to Northern Mexico, closer to the U.S. “market,” and imperiling Mexican sovereignty. Information, and sometimes materials, related to the production of weapons of mass destruction and/or their means of delivery are making their way to the unruly corners of the globe.

The United States in defending against these perils, but its defensive efforts are also proving problematic. Aside from the fact that each of these threat areas presents specific, nettlesome problems, U.S. efforts to address them have generally suffered from a resort to hierarchical “stove-pipe” approaches from the top, and bureaucratic “turf battles” from below. There have been well-informed efforts to move to flatter, more heterarchical, and thus more truly interagency, types of designs. But, with notable exceptions, the problems persist.

New issue areas are emerging that also require interagency approaches—and show the problems sketched above are, in a sense, generic. These new areas include peacetime contingency operations and other aspects of OOTW, which increasingly require but have yet to benefit from solid coordination with NGOs, and which are

---

1Our discussion focuses on government, but businesses are taking initiatives analogous to public interagency efforts (e.g., regarding piracy, the International Maritime Bureau).
often hamstrung by the need for consensus among a multitude of powers or transnational bureaucracies (e.g., the United Nations and NATO in the Balkans, 1991–1994).

Furthermore, interagency problems are emerging in the area of cyberspace security—likely the next addition to the list. Will bureaucratic politics hamstring government efforts to defend the U.S. (and non-U.S.) “infospheres” from a variety of netwarriors? This possibility has concerned many actors, both in and out of government, all of whom have identified the need for further research into the issues of cyberspace security and safety (Cohen, 1995; Hoffman, 1994; Chairman of the Joint Chiefs, 1993; Libicki, 1994; and Hundley and Anderson, 1994).

All of these areas, from counterterrorism through cyberspace safety and security, are relevant to the netwar phenomenon. Moreover, they all suffer from interagency problems, even though interagency cooperation is imperative in all these areas, and even though U.S. officials have been more successful in some areas (e.g., counterterrorism\(^2\)) than others. What we think would be useful, then, as part of our future research agenda, is to look for ways to prepare for counternetwar by examining, across all areas, what is working well, and what appear to be the best interagency models.

Such research should focus upon organizational matters, to at least the same degree that is often given to the search for technological fixes. For, without attention to organizational design, initiatives to make cyberspace secure will likely fall into a morass not unlike that which has, at times, plagued efforts to cope with terrorism, drug trafficking, and proliferation. The answers to the generic problems of interagency design could come from either of two directions. We could focus on figuring out the lessons for fighting netwars against the TCOs, terrorists, proliferators, and other established adversaries, then apply the lessons to the cyberspace area. Or we could address the cyberspace challenge first and try to derive insights that can be applied to the more traditional areas.

\(^2\)Intergency teamwork has reportedly worked better in counterterrorism than the other areas, partly because of the urgency to protect U.S. officials whose lives have been threatened.
Counternetwar Is Likely to Be Interagency

Build across four levels (same as for adversary):

*Organizational:* Learn to mix hierarchical and network forms in interagency mechanisms

*Doctrinal:* Institute doctrines, operational concepts that match network organization

*Technological:* Develop information, communication systems to serve interagency work

*Social:* Train teams to think and to behave in network terms

Challenge: How to make the network a source of loyalty

An implication that is emerging from our research is that U.S. efforts at counternetwar should be grounded in interagency cooperation (a variant of "jointness"). Preliminary thinking suggests redesigning and rebuilding interagency efforts across four levels—the same levels that apply to a netwar adversary. Again, this does not mean mirroring the adversary, but learning to draw on the same important design principles that he has already learned about the rise of network forms in the information age:

- At the *organizational* level—determining how to optimize the mix of hierarchical and network forms in interagency mechanisms.
- At the *doctrinal* level—instuting doctrines, operational concepts, and strategies that match the interagency approach.
- At the *technological* level—building information and communication systems (e.g., for intelligence sharing) that are interagency in design.
- At the *social* level—adopting new approaches to selecting personnel, and training teams to think and operate in network terms.

A vexing question in all this is how to make the interagency network a focus, and a source, of commitment and loyalty. Comments about past experiences with interagency work in government repeatedly raise the point that the participants tend to treat their home agency, and not the interagency mechanism, as their main allegiance and source of authority. Moreover, they often tend to regard interagency assignments as bad for their careers, compared with a line assignment in their home agency. For interagency approaches to counternetwar to work well, especially when international cooperation is involved, this problem should be resolved. A recent in-
ternational success was scored by U.S., Mexican, and five Central American agencies that shared intelligence and coordinated field actions to strike the hardest (and most successful) blow to date in the drug war.

Exasperation with the operational, bureaucratic, and the various other difficulties of dealing with terrorism, narcotics trafficking, and similar threats, now including those in cyberspace, normally leads to calls to create a "czar" for that threat domain. This may be muted by avowals that, yes, it should be an interagency czar who is skilled at coordinating. But the call—so well symbolized by the very term "czar"—still tends to signify the creation of a hierarchical superior who can centralize disparate activities. And that is part of the problem, as former senior U.S. official Paul Strassmann notes:

I never understood why everybody called the top man "czar" and not emperor, eminence, lord, majesty, king, pope, kaiser, governor, caliph, shogun, sovereign or shah. I guess that the notorious czarist profligacy, incompetence, inability to govern and dismal endings were the fate to wish on the reigning data center monarchs (Strassman, 1995, p. 479, footnote).

Management literature increasingly makes the point that information-age organizations should move away from hierarchical, centralized designs, toward ones that emphasize heterarchical teamwork (e.g., Drucker, 1993). Some of this literature points out that some multiorganizational problems may be best addressed through informal network designs that emphasize "coordination without hierarchy" (Chisholm, 1989), or designs that are tantamount to what are called "virtual corporations." In this vein, business-oriented literature that talks about the future as the "Age of the Network" puts the focus not on czars but on coordinators:

[T]he person who makes particular networks happen is the "coordinator." . . . Coordinators appear everywhere in the Age of the Network . . . Networks began developing new leaders long before computers enhanced their reach. In a richly connected environment where many potential projects are sparking, growing, diminishing, and disappearing, a new role arises, that of the coordinator, whose distinguishing characteristic is the ability to see "connections" among people (Lipnick and Stamps, 1994, p. 173).

Although czar-like leadership may be needed at first to ensure that the members of an interagency network are committed to it, coordinators are ultimately preferable to czars. But if we must use a catchy term, would "khans" not be preferable to czars? Unlike a czar, the Khan ruled with topsight. He saw the "connections" among the diverse, widely separated regions of his dominions. And he took a decentralized approach to leadership, rarely intervening in operations. He was a coordinator as well as a commander.
Needed: New Research Hubs and Centers

Observation: It will take rethinking to construct new approaches

- Centers for study of organization, doctrine, strategy, and technology to cope with netwar?
- Centers for study of "information" as a concept, academic discipline, and military science?

Learning to counter netwar is no easy task—it will take time, experience, energy, and commitment to build effective approaches to organization, doctrine, and strategy for defending against netwar. The process may be facilitated by establishing special "centers" to advance knowledge about netwar and related phenomena. Some such centers have already been established to develop knowledge about information warfare, narrowly and broadly defined, but more needs to be done in this direction, notably to internet them and to create "hubs."

Our work leads us to propose the establishment of two types of hubs. However, this call for new hubs should not be viewed as traditionalist, as they are envisioned as having limited hierarchical control, even over research agendas. Rather, they would serve primarily as "clearinghouses" for efficiently coordinating ideas, eliminating counterproductive duplication, and bridging the networks of academics, soldiers, and civilian authorities who are already devoting careful, growing attention to the societal and security issues emerging in the information age.

To construct such hubs will still require the formation of new research institutes, or centers. First, because of looming threats and vulnerabilities, it may be advisable to found a strategic institute for the study of netwar in the near future. Such a center should be devoted to both theoretical and applied issues, with the aim not only of analyzing netwars in all their varieties and guises, but also of determining what designs—organization, doctrine, strategy, technology, etc.—may be most appropriate for countering netwars at the societal and military levels.

This strategic institute should strive to provide insights needed to cope with terrorists, transnational criminals, WMD proliferators, and the other networked opponents likely to dominate the "landscape" of netwar. The institute's charter should, how-
ever, extend beyond areas in which netwar involves significant military dimensions, to include matters relating more to public diplomacy, the protection of intellectual property, and even the modes of academic training most likely to produce a generation of supple-minded netwarriors.

A second type of center, we propose, should be devoted to the study of "information." Indeed, the more we inquire into subjects like netwar and cyberwar, the more we think it may be time for a new academic discipline or field to emerge—Ronfeldt (1992) proposed calling it "cyberology"—as the demands of earlier times resulted in the fields of economics and political science. This center’s agenda should extend beyond information science and management to encompass aspects of sociology, political science, economics, psychology, and anthropology. It should draw on the traditions of cybernetics, systems theory, game theory, decision theory, as well as recent theorizing about artificial intelligence, artificial life, chaos, complexity, and information physics.

While the new views about "information" do not fit well into the standard academic disciplines and research fields, extensive intellectual ferment is occurring around the idea that all organized systems, including living organisms as well as societies, depend at their core on how information is generated, transmitted, processed, and controlled. This is leading to an "information-processing view of human organization and society" that means, according to social scientist James Beniger (1986, p. 38):

[T]he proper subject matter of the social and behavioral sciences, if they are to complement studies of the flows of matter (input-output economics) and energy (ecology), ought to be information: its generation, storage, processing, and communication to effect control.

Such a discipline may sound odd and too diverse, for it would span topics that analysts do not normally group together. Yet this diversity may embody as much coherence as any other academic discipline or field of research. University and other centers might be well advised to develop research capabilities in this respect. Policymakers and practitioners in Washington and elsewhere, at home and abroad, will have an increasing need for analyses that sort out and assess the issues raised not just by the spread and use of new information technologies, but also by what the concept of "information" is going to be all about, in military as well as broad societal terms.
Rethinking "Information"—and "Power"

This chart summarizes our point that concepts about "information" and "power" are in need of rethinking.3

As depicted above, three views of "information" appear in discussions about the information revolution. Two are widespread: The first views information in terms of the inherent message, the second in terms of the medium of production, storage, transmission, and reception. An emerging third view transcends the former two; it speculates that information may be a physical property—as physical as mass and energy, and inherent in all matter.

Meanwhile, three views of power can also be discerned that parallel these views of information—but with a reverse twist. These three views treat power, respectively, as being material, organizational (or systemic), and finally immaterial in nature. This applies to whatever strategic realm one is analyzing: political, economic, or military, all of which have material, organizational, and immaterial, ideational bases.

These considerations alter the adage that "information is power." We see that "information," generally thought to be immaterial, is increasingly seen to be a tangible part of all matter, while "power," long thought to be based mainly on material resources, is increasingly seen to be essentially immaterial, even metaphysical in nature. As information becomes more material, and power more immaterial, the two concepts become more deeply intertwined than ever.

These trends generate some implications for the theory and practice of warfare and for grand strategy in the times ahead. The three views of power, rotated against the

---

3The text for this and the next chart is summarized from Arquilla and Ronfeldt (1996).
three views of information, lead to a matrix of combinations. Three cells are notable. When power and information are viewed in their traditional senses—with power depending on material capabilities, and information being but a useful adjunct—we liken them to Mars, the Roman god of war. We identify Athena, the Greek goddess of warrior wisdom, with the far cell, which corresponds to power and information viewed in postmodern, information-age senses—here information is physical and power immaterial, and the two dynamics merge. In between, on the diagonal, is a cell in which sociosystemic views of information and power coincide. This may well be how many people think today about information and power, and most them are as yet unaware of the Athena cell.

A military force whose doctrine is built around an Athenan view should be able to defeat one built around a systems concept, and it in turn should be able to defeat one built around a Mars view. In general, a cell should represent a stronger approach than any cell beneath and/or to the left of it. This depiction parallels Martin Van Creveld’s (1989) view of military history, wherein he traces the evolution of war in terms of its being based first on the tools and materials of war, second on systems of warfare, and third on information-based technologies like the computer.

Which views or blends of information and power one prefers affects how one proceeds to think about the implications for warfare. We presume that thinking about information and power is moving in the “Athenan,” direction. More to the point, the Athenan view of information and power implies targeting whatever represents or embodies the most information on an enemy’s side. This implies ascertaining and attacking the most information-rich components of an adversary’s order of battle, a point that applies across the conflict spectrum.

An example of an implication for netwar is that counternarcotics operations should focus on attacking traffickers’ electronic funds transfers and other financial transactions, rather than trying to chase smugglers or eradicate crops that represent lower information content (Andelman, 1994). Another implication of the Athenan viewpoint is that the information age will raise the value of social and human capital, since man remains the purest, richest information system.
The “God” of War in the Information Age Is a Goddess

- Ares / Mars no longer the best referent
- Athena now the superior “deity”
  - Greek goddess of wisdom who springs fully armed from head of Zeus
  - Huntress and protectress who symbolizes reverence for the state
  - Sides with Greeks in Trojan war and proposes “gift horse” laden with soldiers
- Should we protect our knowledge with “guarded openness,” as her adherents protected her Palladium?

Metaphors and analogies can help convey new concepts like netwar by providing simplified images that work to encapsulate complex points. We provide two such metaphors or analogies in this briefing. The one raised here contrasts Mars and Athena as gods of war. The other, raised near the end of the briefing, contrasts chess and Go as paradigms of war.

Information has been associated with power, war, and the state since at least the time of the Greek gods. One normally thinks of Ares, or the Roman refinement Mars, as the god of war. But where warfare is about information, the superior deity is Athena—the Greek goddess of wisdom who sprang fully armed from Zeus’s head and became the benevolent, ethical, patriotic protectress and occasional wrathful huntress who exemplified reverence for the state.4

According to Virgil, Troy would be powerful enough to withstand all its enemies so long as it possessed and honored the Palladium, a sacred statue of Athena provided by Zeus or Athena herself. Understanding this, the Greeks arranged to steal the Trojan Palladium, symbolically denying the Trojans the benefits granted by access to the goddess of wisdom. As a result, Athena sided with the Greeks in the Trojan War, where she bested Ares on the battlefield and conceived the idea of the wooden “gift horse” secretly loaded with Greek soldiers. The Trojans made the monumental misjudgment of hauling it inside their fortress, over the protestations of the priest Laocoon and the seer Cassandra. The rest is history, and legend—and ever since,

---

4Standard sources on Greek and Roman mythology include Graves (1960) and Hamilton (1969). While Ares is refined by the Romans into Mars, Athena became Minerva. But given the Roman’s penchant for specializing their gods, Minerva is mainly a goddess of wisdom, stripped of the warrior element. Thus she does not fit our purposes here.
amining the relationship between information and power has attracted all manner of political and military theorists.

Shifting to view Athena, rather than Mars, as the emblematic god (or goddess) of war in the information age is consistent with Clausewitz's prediction: that knowledge would become capability. This shift has more than symbolic import, for it implies that we must begin to think about information as something that may have to be protected. In some ways, this notion runs counter to traditional Western democratic ideals about maximizing openness.

Besides urging that information and communications be treated as a new fourth dimension of grand strategy, our admonition is that U.S. strategic choices be reviewed across the spectrum of alternative approaches to openness. That spectrum might be framed by complete openness at one end and by preclusive security at the other. Something that might be called "guarded openness" would define the middle range of the spectrum.

Guarded openness was, in many respects, the strategy that the United States pursued during the Cold War, if not before. But it is not a static strategy—moreover, it has not even been discussed much as a strategy. However, for dealing with the present and future world, the overall profile of when to be open and when closed should be based on different principles from those that governed strategic judgment during the Cold War, especially given the decline of Russian power and the worldwide diffusion of power to a multitude of smaller actors, many of them of the nonstate variety.

If a high-level policy review were undertaken, it could help to ascertain what contextual factors are most important in determining whether to move in open, guarded, or sometimes preclusive directions in specific issue areas. Such a review would further help identify the mechanisms that should be emphasized for purposes of enhancing and protecting U.S. openness, whenever feasible. Finally, the review process could lead to the formation of national and international "knowledge strategies," in areas ranging from military innovations to commercial intellectual property.