The Seven Deadly Sins of Network-Centric Warfare

by **Thomas P.M. Barnett**

Email Thomas P.M. Barnett

Biography

Putnam, 2004
The Pentagon's New Map: War and Peace in the Twenty-First Century

***Esquire,* March 2003**
The Pentagon's New Map

Global Transaction Strategy

Most of us . . .
read Vice Admiral Art Cebrowski's seminal 1998 *Proceedings* article on network-centric warfare (NCW), and if some detected a confidence too bold, that is only to be expected. Visions of the future invariably rankle, especially when they seem inevitable. Quoting Liddell Hart, "The only thing harder than getting a new idea into the military is getting an old one out," Admiral Cebrowski and coauthor John Garstka threw down the gauntlet and dared anyone to prove them wrong.

Would that I could, but the best I can muster is a devil's advocate take on what I see as network-centric warfare's seven deadly sins. Note that I don't say "mortal sins." As with any transgression, penance can be made.

1. Lust

NCW Longs for an Enemy Worthy of Its Technological Prowess

If absence makes the heart grow fonder, network-centric warfare is in for a lot of heartbreak, because I doubt we will ever encounter an enemy to match its grand assumptions regarding a revolution in military affairs. The United States currently spends more on its information technology than all but a couple of great powers spend on their entire militaries. In a world where rogue nations typically spend around $5 billion a year on defense, NCW is a path down which only the U.S. military can tread.

Meanwhile, our relatively rich allies fret about keeping up, wondering aloud about a day when they won't be able even to communicate with us. These states barely can afford the shrinking force structures they now possess, and if network-centric warfare demands the tremendous pre-conflict investments in data processing that I suspect it does, then the future of coalition warfare looks bleak indeed. Not only will our allies have little to contribute to this come-as-you-are party, they won't even be able to track the course of the "conversation."

As for potential peer competitors, forget about it—and I am not just talking money. I am a great believer in the "QWERTY effect," by which technological pathways are locked in by market victories of one standard over another.[1] No one would argue against the notion that the United States is QWERTY Central, or that our military feeds off that creativity. So the reality facing, any potential enemy is that he either has to get in line behind our QWERTY dominance or satisfy himself with chintzy knockoffs from

our far-distant past. So when Iran gets itself some North Korean missile technology, let's remember that it is only a poor copy of old Chinese technology, which is a poor copy of old Soviet technology, which is a poor derivative of old Nazi-era German technology—and, as everyone knows, our German scientists were better than their German scientists! This is why proliferation is always a lot slower than suggested by too many hyperbolic experts.

Once you get past the potential peer competitors, you are entering the universe of smaller, rogue enemies that many security experts claim will be able to adapt all this information technology into a plethora of brilliant asymmetric responses—the Radio Shack scenario. Frankly, it stretches my imagination to the limit to conjure up seriously destabilizing threats from resource-poor, small states, unless we let our lust for a bygone era distort our preparations for a far different future.

2. Sloth

NCW Slows the U.S. Military's Adaptation to a MOOTW World

Military operations other than war (MOOTWs) are the closest thinly to a sure-bet future the U.S. military faces right now, and network-centric warfare does not yet answer that mail. Beyond the affordability issues, there is the larger question of what "networked" should mean for the U.S. military: Wiring-up among ourselves? Or wiring ourselves up more to the world outside?

This is not an esoteric question for naval forces, because I see a future in which the establishment of, and support to, information networks is the crucial U.S. naval product delivered overseas to internal crises, where confusion, complexity, and chaos are the norm. We are far more likely to be called on to be the deliverers of clarity and context than sowers of blindness and vertigo, and we are far more likely to be asked to settle down all sides in a conflict than to decimate one particular side. This is where NCW's "lock-out" phraseology misleads: we will be interested in opening up pathways to resolution, not closing down pathways of conflict. That reality speaks to non-lethal approaches, reversible effects, and keeping open the channels of communication.

Increasingly, naval forces will be called on to serve as a "node connector," rather than a "node destroyer." I am talking not only about bringing crisis-involved regions back on line, but also about the military acting as Network Central for the wide array of U.S. and international agencies that populate any U.S.-led response to complex humanitarian emergencies. Just as important as our ability to talk among ourselves during, the generation and coordination of large-scale violence will be our ability to generate and coordinate the conversations of many outsiders in the prevention of small-scale violence.

Correctly focused, network-centric warfare would allow the U.S. military to come into any crisis situation and establish an information umbrella to boost the transparency of everyone's actions. Incorrectly focused, it might hamstring us along the lines of the Vietnam War. In sum, NCW's quest for information dominance is self-limiting in an era that will see the U.S. military far less involved in network wars than in mucking around where the network is not.

3. Avarice

NCW Favors the Many and Cheap; the U.S. Military Prefers the Few and Costly

Many experts rightly claim that network-centric warfare is nothing new as far as the U.S. Navy is concerned. By its nature, our worldwide, blue-water Navy always has been a networking environment. Of all the major services, it should find the onset of NCW least discombobulating. But it is no secret to anyone who has followed Navy force structure decision making this decade that we consistently have sacrificed ship numbers to technology, even as we decry the resulting stress on operational tempo and global presence.

What we are ending up with is a Navy poorly situated for an NCW era in which the network's crucial strength is its flexibility to degrade gracefully. Some point out that cruise missiles and unmanned aerial vehicles are good fixes because they allow surface combatants to operate in a standoff mode. But the future fleet cannot consist of a dozen huge platforms sitting in the middle of the ocean remotely directing operations because we as a country cannot risk losing any of these hyper-tech behemoths. NCW's bottom line must be that no node can be worth more than the connectivity it provides.

Because we are far more likely to encounter targets of influence operating in the "few and cheap" paradigm, what we should bring to the table are "the many" as opposed to "the costly." Why? The few-and-costly approach puts us in no-win situations, where our entry into crises is self-limited by our tendency—and our opponent's knowledge of that tendency—to treat the loss of any significant network node as grounds for one of two equally bad pathways: escalation or withdrawal. Because our interests typically are limited, escalation usually is the last thing we want. But because the world values our Leviathan-like role as global force of first response and last resort, a pattern of withdrawals over relatively small losses costs us dearly over the long run. A superpower navy too valuable to risk force structure losses is not one worth having. Does that mean we risk more lives? Only if we insist that the U.S. Navy primarily is about projecting destructive power ashore.

4. Pride

NCW's Lock-Out Strategies Resurrect Old Myths about Strategic Bombing

Ever since Giulio Douhet's *Command of the Air* (1921), we have heard that massed effects against an enemy's centers of gravity can lead swiftly to bloodless victory. And every war since then has seen this theory's vigorous application and subsequent refutation. Yet the notion persists and now finds new life in network-centric's "lock-out" strategy. Whether NCW's proponents admit it or not, what lies at the core of this strategy is the spurious notion that punishment equals control.

Can we, by destroying our enemy's information technology "village," somehow save it? I think not.

First, one man's information warfare is another man's international terrorism. If any hostile power tried even a smidgen of what we propose to do *en masse* via NCW, we would be hurling all sorts of war crimes accusations. The collateral damage associated with this "information technology decapitation" strategy simply is too complex to control from afar. Who dies? Society's weakest and most vulnerable. Unless we are

talking total war or some antiseptic battlefield out in the middle of nowhere, we need to own up to the reality that such massed effects are closer to weapons of mass destruction than we care to admit.

Second, our bomb-damage assessment capabilities are nowhere near capable enough to measure the massed effects of NCW's souped-up brand of information warfare. Some assume that the smaller a society's information technology quotient, the greater our ability to understand the impact of information warfare. But in my mind, less information technology equals greater social capacity for low-tech work-arounds that either negate or complicate information warfare immeasurably.

Third, while bowing to complexity theory, NCW adherents toss it out the window once they rhapsodize about lock-out strategies. Somehow, our mastery of our enemy's complexity will translate into a capacity to steer his actions down one path or another, despite the fact that NCW's game plan includes large amounts of irreversible impact. What we may well end up with in some blossoming conflict is a "dialogue of the deaf" that precludes effective communication with the other side concerning conflict resolution or—more important—avoidance of unnecessary escalation. And when that happens, we may wonder which side really had its pathways locked out.

Fourth, NCW is guilty of mirror imaging: we theorize about our own information technology vulnerability and then assume it is the same for others. In reality, our distributed society is far stronger than we realize. In truth, is there any other country in the world where you would prefer to live through a natural disaster? As for less-advanced countries, our arrogant assumptions about their limited work-around capacity say more about us than about them.

Fifth, to the extent that network-centric's immense capabilities can be harnessed to a lock-out strategy, the military needs to relate better to the universe of relevant data and subject-matter experts outside the usual realm of political-military thinking. We do not possess the decision-assessment tools at this point to steer an opponent via information dominance.

5. Anger

NCW's Speed-of-Command Philosophy Can Push Us into Shooting First and Asking Questions Later

The unspoken assumption concerning speed of command seems to be that because we receive and process data faster, we have to act on it faster. Not surprisingly, this virtuous circle can turn vicious rather quickly if commanders allow themselves to become slaves to their own computers, which essentially are dumb machines that count incredibly fast. Rushing to bad judgment is the danger.

Most worrisome are network-centric's assumptions concerning getting inside the enemy's decision loop. This makes sense as a goal, but the real focus should be on what we do once inside, not just on the blind pursuit of faster response times. Why? We always are talking about potential enemies with less advanced information technology architectures, so the potential for miscommunication and misperception is huge. We may find ourselves acting so rapidly within our enemy's decision loop that we largely are prompting and responding to our own signals, which our beleaguered target cannot process. In short, we could end up like Pavlov's dog, ringing his own bell and wondering why he's salivating so much.

It takes two to tango, so, yes, we want sufficient speed of command to get inside our opponent's decision loop, but too much speed turns what we hope is a stimulus-response interaction into a self-stimulating frenzy. The potential irony is telling:

- We rapidly fire signals to a target of influence, who does not pick them up, in part because of the strategic blindness we have inflicted on him.
- Our target's lack of response is interpreted as signifying "X" intent.
- We respond to perceived intent "X" with signal "Y," which also is missed by our target, who, perhaps, is just getting a grip on earlier signals.
- Our target's response "Z" seems incomprehensible, or we assume it is a rejection of sorts to our previous signals.
- Before you know it, we are way beyond "Z" and into some uncharted territory, but we are making incredible time!

The networked organization's great advantage is that the processing and distribution of data are sped up considerably. What this should translate into is increased time for analysis and contemplation of appropriate response, not a knee-jerk ratcheting down of response time. The goal is not to shorten our decision-making loop, but to lengthen it, and, by doing so, improve it. Otherwise, all we are doing is generating two suboptimal decisions to his one.

Now, some will declare that the enemy's decision loop is being shortened by his increasingly rapid incorporation of information technology into his command-and-control architecture. But this Chicken Little approach misleads: yes, he will improve his decision-loop timelines constantly, and so should we. But the point is not to engage in some never-ending speed race with our own worst-case fears, but rather to concentrate NCW on how best to exploit the delta between our loop time and his. Speed is not the essence here, only the means to an end. Forget that and you might as well be acting in anger.

6. Envy

NCW Covets the Business World's Self-Synchronization

There is no defense establishment more concerned with everyone singing off the same sheet of music than the U.S. military. Why? No military in the world seeks to decentralize crucial decision-making power as much. It is both our calling card and our greatest weapon—our operational flexibility. So if any military will adapt itself to NCW's ambitious goal of self-synchronization, it will be us, though we are not likely to reach the ideal state of affairs desired by network-centric warfare, which I believe seeks a dangerous slimming down of the observe-orient-decide-act (OODA) loop.

The implied goal of self-synchronization is that information technology will facilitate such a rapid movement of information as to obviate the time requirements of the "00" portion, allowing commanders to exploit speed of command. But in my mind, NCW's capacity to collapse timelines for the processing of operational data should lengthen the observe and orient portions of the loop, not encourage their virtual disappearance by outsourcing that cognitive function to silicon units. During the Cold War, a sort of "DADA loop" was forced on the U.S. military by certain bolt-from-the-blue warfighting scenarios involving the Soviet Union. But I am hard-pressed to envision post-Cold War scenarios where the U.S. military should be encouraged to deemphasize the rational thinking that must periodically interrupt whatever courses of action our commanders in

the field are empowered to pursue.

NCW's envy for the business world's market-responsive notion of self-synchronization is understandable, for there are few things in this world as complex as a major military operation. But this envy is misplaced; we create governments to deal precisely with those thorny aspects of social life that we do not trust private firms to manage under the ultimate self-synchronizing motivation known as profit seeking. And among the thorniest aspects are those we reserve for the military, entrusted as it is with the assets that generate big violence.

In addition, the crisis scenarios the U.S. military faces grow ever more ambiguous as far as U.S. national interests are concerned. Other than a rerun of Desert Storm, I don't see any crises where the United States would be well served by its military focusing on self-synchronization. A MOOTW world should encourage greater *externally* focused networking. So even if the U.S. military could achieve self-synchronization, neither the likely scenarios nor the partners we engage in them are well suited to this slam-bang approach. In fact, in many MOOTW scenarios, it is the military that should use its mighty information technology power to generate the "00" portion of the decision loop for others who ultimately will take the lead in deciding and acting.

7. Gluttony

NCW's Common Operating PictureCould Lead to Information Overload

The term "common operating picture" is apt for network-centric's vision of all players at all levels working off the same mental model. There is little doubt that computer-mediated visual presentations will shape much of the commander's perception of operational realities. That, in and of itself, is not new.

What is new is the potential for inundating all participants with an ever-increasing flow of data masquerading as information because it has been slickly packaged within the common operating picture. The danger lies in the picture's collapsing all participants' perceptions of what is tactical versus operational versus strategic, and, by doing so, creating strong incentives for all to engage in information overload in an attempt to maintain their bearings in this overly ambitious big picture. In sum, I am concerned that the push for speed of command and self-synchronization will drive all participants to an over-reliance on the common operating picture as a shared reality that is neither shared nor real.

The common operating picture cannot really be shared in the sense that ownership will remain a top-down affair. What is scary about NCW's ambition is the strain it may put on commanders at various levels to integrate the commander's intent from all other commanders and not just up the chain of command. NCW promises to flatten hierarchies, but the grave nature of military operations may push too many commanders into becoming control freaks, fed by an almost unlimited data flow. In the end, the quest for sharing may prove more disintegrating than integrating.

The infusion of information technology into hierarchical organizations typically reduces the traditional asymmetries of information that define superior-subordinate relationships. Taken in this light, the common operating picture is an attempt by military leaders to retain the high ground of command prerogative—a sort of nonstop internal spin control by commanders on what is necessarily a constantly breaking story among all participants, given their access to information that previously remained under

the near-exclusive purview of superior officers.

That gets me to the question of the common operating picture's "realness," for it suggests that the picture will be less a raw representation of operational reality than a command-manipulated virtual reality. At worst, I envisage command staff engaging in a heavy-handed enforcement of commander's intent, all in the name of shaping and protecting the common operating picture.

The temptation of information gluttony always will be with NCW. Salvation lies in the concept of information sufficiency by level of command.

* * *

I seek not to praise network-centric warfare, nor to bury it. To the extent that NCW marries the military to a networking paradigm, it moves America's defense establishment toward a future I view as inevitable. However, focusing NCW on the application of large-scale violence, or past wars, is a mistake—especially for naval forces. On a global scale, both organized violence and defense spending have migrated below the level of nation-states. For our military to remain relevant, it must reach out to that subnational environment. Networking is the answer, but it needs to be focused outwardly. This was the natural role of naval forces in U.S. history. It can be again, but only if the Navy frees itself from its Pacific War past and pointless competition with the Air Force in power projection.

---

[1] QWERTY refers to the first six letters on the upper left of the typewriter keyboard. This layout was adopted in the 19th century to minimize jamming of mechanical striking arms. It quickly became the universal standard and remains so to this day, despite being less efficient than other designs.

Dr. Barnett holds an appointment as Professor and Senior Decision Researcher at the Decision Support Department, Center for Naval Warfare Studies, U.S. Naval War College. This article is adapted from an essay he wrote for the Center for Naval Analyses, where he served on the Research Staff from 1990 to 1998. Dr. Barnett holds a Ph.D. in Government from Harvard University. **He would like to thank the following individuals for their comments on earlier drafts: Jack Batzler, Lyntis Beard, Gary Federici, Hank Gaffney, Bradd Hayes, Lawrence Modisett, Hank Kamradt, Rob Odell, Pat Pentland, and Mike McDevitt.**