A "Net Shift" for Afghanistan?

BY JOHN ARQUILLA

Some three millennia ago, the Persian philosopher Zoroaster dubbed mountainous Afghanistan "the land of the high flags." But there is far more to its identity than the powerful shaping influence of terrain upon its culture; there is above all the paradox of the Afghan peoples themselves. Xenophobic from time immemorial, they are nonetheless a mix of Aryans, Greeks, Chinese, Indians, Mongols, and others. Quintessentially isolationist, their country has always been a crossroads of trade and conquest. Indeed, the great city of Kandahar—the true capital of the Taliban—is named after Alexander the Great, who tarried there. And so for all the cool distance conveyed by the notion of the "high flags," the deeper story of Afghanistan is one of a mass mixing of peoples and of a crucial hub in the infrastructure of East-West interconnection. In short, it is a land comprised of dense, ancient social and physical networks.

Thus, the modern riddle of Afghanistan—its stubborn and successful resistance to "progress" as defined by the British in the 19th and early 20th centuries, the Russians in the 1970s–1980s, and the Americans and their allies today—can perhaps only be properly understood by viewing the land and people as a loosely aggregated, laterally connected network rather than a centralized, traditionally hierarchical nation. For even at first glance, it is clear that the age-old paradoxes have persisted right up to the present.

While most of the world was in upheaval between the rise of Hitler's Nazi regime in Germany in 1933 and the end of American involvement in Vietnam in 1975, Afghanistan was comparatively calm. The constitutional monarch, King Mohammed Zahir Shah, who ruled for almost exactly this period, had a reverence from his people that contrasted sharply with his lack of real power over them. Yet it was for the most part a profoundly peaceful time, when Afghan security was at its best despite there being virtually no national army.

Today, the paradox persists and even deepens, as efforts are made to form Afghanistan into a nation with strong, central, and legitimate levers of governance. The troubled American intervention has

John Arquilla is Professor of Defense Analysis at the Naval Postgraduate School. His most recent book is *Worst Enemy: The Reluctant Transformation of the American Military* (Ivan R. Dee, 2008).

seen the Taliban fall and rise again in an insurgency that has reestablished much of its influence throughout the country—in spite of the fact that an overwhelming majority of Afghans despise the Talibs. Another aspect of the paradox can be seen in the fact that the soldiery of the American-supported Karzai regime, although drawn from some of the world's best natural fighters, has been formed into one of the world's most poorly organized militaries.

To date, the American response has been to "double down" on its big bet in Afghanistan, sending yet more troops and rebuilding more roads in pursuit of nationbuilding. In the name of shoring up central control, a shaky, shady regime has been publicly supported by President Barack Obama, at some political cost—even in the face of scandalous, overt acts of election fraud. The principal lens through which Washington perceives Afghanistan is nation-based; but given the problematic results to date, it may be high time to recognize more fully the networked nature of Afghan society, culture, and strategic geography. And since this is a time of war, it is also incumbent to think more specifically in terms of how to fight a network—and how to fight *like* a network. Accordingly, the paradigm shift called for is to move from nationbuilding to "netwar."

the guiding notion was that dispersed nodes would launch loosely coordinated, omnidirectional attacks on more centralized foes

The Concept of Netwar

Before considering what such a shift might look like, it is necessary to convey a clear, succinct description of netwar itself, and of the networks that conduct this type of conflict. The term *netwar* was introduced by David Ronfeldt and me in a 1992 essay to describe emerging forms of low-intensity conflict, crime, and social militancy, but it was explored in more detail in our 1996 RAND report *The Advent of Netwar*. That study aimed to raise the consciousness of the government, military, and mass public regarding both the rise of networks and the distinct doctrinal innovations they would likely bring to conflict. Most specifically, the guiding notion was that fighting networks composed of many small cells would tend to "swarm" their opponents—that is, their dispersed nodes would launch loosely coordinated, omnidirectional attacks on more centralized foes.

In the 5 years between the publication of *The Advent of Netwar* and the 9/11 attacks, perhaps the most distinct example of a network swarming its opponent was the first of the modern Russo-Chechen conflicts, which was waged from 1994 to 1996. This war featured, for the most part, small bands of Chechen fighters driving one of the world's largest and more competent militaries out of their country. Interestingly, the Russians returned 3 years later and did much better by networking their own forces with friendly local clans and counterswarming the rebel Chechens.[1]

Two other important aspects of netwar swarm tactics were on display during that period. The first could be seen in the success of the student-led Otpor resistance movement in Serbia, which played a key role in toppling the Slobodan Milosevic regime after the Kosovo war of 1999. The use of social networking tools to mobilize and empower mass demonstrations proved hard to quell and became something of a model for the democratic "color revolutions" that emerged in Ukraine and Georgia.

At the same time this sort of social swarming was on the rise, cyberspace was beginning to see a significant boost in capabilities for the

same kind of activity: the simultaneous convergence of widely distributed individuals and/or linked machines on selected targets. In this case, however, the swarm was virtual rather than physical, and was conducted largely with denial-of-service attacks. These actions would typically grow out of animosity toward particular corporate actors or certain government policies, with the latter sparking the rise of swarms of "hacktivist" demonstrators. Initially, these virtual swarms were far less effective than their physical counterparts.[2] But it seems that virtual swarms have now grown in potency, too.

In terms of the uniquely distinguishing features of networks, the 1996 RAND report keyed in on the organizational dimension instead of either technological linkages (the way networks are wired) or social interactions (the "old boy network" paradigm, defined on the basis of who talks with whom). Three basic network topologies were described: "chains," "hubs," and areas of "all-channel" connectivity. For purposes of thinking about netwar, we should focus on the notion that networks typically manifest some mix of these archetypal forms. The mixtures may vary, but the three forms will undoubtedly appear, whether the network is comprised of terrorists, insurgents, transnational criminals, or even social activists.

Al Qaeda, for example, began with a small core area of all-channel connection in Afghanistan, with chains running out to operating units in several dozen countries all over the world. At these remote locations far from the core, there were mixtures of hubs (for example, Mohammed Atta, the likely field commander of the 9/11 hit team, was a hub in America) and areas of all-channel connection, such as the Hamburg cell. Marc Sageman has neatly dubbed the latter "cliques."[3]

Even after being driven from Afghanistan in late 2001 (a result that al Qaeda and the Taliban are still contesting), the network's new sanctuary in Pakistan's Federally Administered Tribal Areas (FATA) and the "virtual haven" still enjoyed in the vast wilderness of cyberspace have allowed the terrorists to maintain a roughly similar organizational structure. Their network topology is somewhat looser than in 2001, with several affiliated groups around the world adopting the al Qaeda "brand" without necessarily subordinating themselves to direct orders from the core, but the basic network functions have remained for more than a decade, despite increasing Pakistani, American, and other allied military pressure.

the narrative dimension has to do with the story that network members tell each other about the origins and purpose of their coming together

Moreover, al Qaeda's topological template for networking appears to have utility for other groups as well, in that Hizballah's organizational structure during the 2006 Lebanon war was quite similar. In this case, there was once again a core of all-channel connection with chains running to hundreds of small field units operating in southern Lebanon. But with "decontrol" being a defining characteristic of netwar, there was little central control of these field units, whose fundamental duties were to unearth cached weapons, fire them off, and then return to hide-sites. It was a concept of operations described as "shoot and scoot," which even the Israeli government–ordered Winograd Report on the war noted worked quite well against their Defense Forces.

Beyond their communications technologies, topological structures, and swarming doctrines, fighting networks—whether operating in the physical or the virtual domain—must also

U.S. Air Force (Andy Dunaway)

U.S. Soldier provides security while on mission with Iraqi soldiers

be assessed in terms of the factors that unite their adherents. These factors fall into two basic categories: narrative and social. The narrative dimension has to do with the story that network members tell each other about the origins and purpose of their coming together. In al Qaeda's case, Marc Sageman has described this element as a "grand narrative,"[4] given some of its far-reaching aspects (for example, restoration of a broad caliphate and the call to join a holy war to reduce the shadow that American power casts upon the Muslim world). At a more operational level, the narrative serves as a rough guide to action, informing cadres whom they should attack and encouraging self-synchronized actions by the many who will come under no one's direct control. American white supremacists sometimes call this paradigm "leaderless resistance."[5] David Ronfeldt and I introduced and prefer the term *panarchy* to reflect the seeking of a common goal without direct control.

In addition to the power of story to mobilize and guide masses, spark recruitment, and shore up the morale of its weary, hunted cadres, the al Qaeda network offers an example of the use of social cross-connections to tighten its bonds. Whether tribal or religious-based, the importance of a strong social aspect to networks is that it helps both to convey "staying power" to members and to foster deep levels of trust and cooperation. Indeed, when we look at the social basis of the alliance of nations currently fighting the terror networks, we see that cooperation is often quite conditional—for example, observe the deleterious effects of the divisive international debate about the U.S.-led invasion of Iraq in 2003 on the antiterrorist alliance.

Even within nations, the ability of various departments of government—military, law enforcement, intelligence, and diplomatic—to engage in the broad sharing of information among and

between their members, a true hallmark of networking, is generally impeded by a social ethos that defines individuals' identities in terms of their parent organizations. The highly problematic response of the newly formed Department of Homeland Security to Hurricane Katrina in 2005 saw many examples of the social backwardness and balkiness of traditional organizational forms in action. Hierarchies simply do not breed the kinds of social connections needed and empowered by networks.

With the foregoing in mind, it should be possible to assess the course and conduct of a strategic "net shift" as seen in an exemplary case of its application. In this instance, the case to review is Iraq.

Lessons from Iraq

From fairly early in the U.S. intervention in Iraq, it became apparent that a fundamentally different dynamic was driving the conflict. The war began in the spring of 2003 with a combination of aerial "shock and awe" and armored "thunder runs" that swiftly toppled Saddam Hussein. Yet terror and insurgency were on the rise at the same time, much of it fomented by an al Qaeda franchisee, Abu Musab al-Zarqawi, whose primary goal, embraced by Osama bin Laden late in 2004, was to spark a Sunni-Shi'a civil war.[6] Zarqawi did a great deal of damage before being killed in an air raid in the summer of 2006.

The violence continued. Neither the capture of the tyrant nor the killing of the terrorist leader could bring victory to coalition forces; they were fighting networks that did not depend on lone, charismatic commanders. Trying to defeat them with counter-leadership targeting proved fruitless and wasteful of resources, for these were networks that did a lot of self-synchronizing by sharing best practices over the Internet (for ambushes, the placement of improvised explosive devices, and so forth) or sending liaison operatives back and forth, spanning the boundaries among various network elements.

Indeed, the Iraqi insurgents exhibited several of the behaviors predicted in *The Advent of Netwar*: they operated in many small bands, used swarm tactics, and eschewed central control but were still able to pursue the common goal (that is, they existed in a state of panarchy) of resisting American occupation. The diversity of the resistance would prove one of the insurgency's most telling features. At the height of the violence, there were at least eight major network clusters made up of Sunni and Shi'a tribesmen, former military and regime members, and the foreign fighters operating throughout Iraq.[7]

The biggest clusters of insurgents fell under the broad categories of the Sunni tribes in Anbar Province, the Shi'a Mahdi army, and the die-hard supporters of Saddam. Al Qaeda operatives, while constituting a small percentage of total insurgents—by almost all measures well below one-tenth—worked closely with the Sunni tribes, giving them much additional leverage. Also, given the goal of fomenting civil war, having large numbers of al Qaeda operatives involved was less important than selecting targets carefully, with their maximum "outrage effect" always in mind.

This was not the sort of campaign that could be won by shock and awe or other traditional tactics. Yet coalition forces were to persist for nearly 4 years in their mostly conventional approach, laagering in on a relatively small number of large forward operating bases from which they occasionally poured forth on sweeps, or in reaction to insurgent attacks on Iraqis and ambushes on U.S. military patrols and convoys. There were also two major urban battles in Fallujah in 2004.

On top of all this, American airpower continued to be used liberally, guaranteeing a continuing stream of Iraqi noncombatant casualties. Finally, however—probably beginning in earnest in late 2006—the sense that networks lay at the heart of the problem in Iraq, and were the key to the solution, began to take hold high and low, and a new strategy emerged.

This conceptual shift was actually introduced by Secretary of Defense Donald Rumsfeld, who had begun referring publicly to the conflict in Iraq as a netwar in December 2004.[8] But this perspective had begun to find its way into popular consciousness even earlier. It can be seen, for example, in an article published in the *Atlantic Monthly* in the summer of 2004

the sense that networks lay at the heart of the problem in Iraq, and were the key to the solution, began to take hold, and a new strategy emerged

by renowned terrorism and irregular warfare expert Bruce Hoffman. In it, he concluded that "what we find in Iraq is the closest manifestation yet of 'netwar,' a concept defined in 1992 by the RAND analysts John Arquilla and David Ronfeldt."[9] Fareed Zakaria of *Newsweek* arrived at a similar conclusion a few months later.[10]

In the field, the officers carrying the heaviest burden in this fight—the company commanders each in charge of just a few hundred soldiers—knew they were up against a network and created a network of their own, in the form of "Companycommand.com." Tactics that worked against the terrorists anywhere were soon being diffused virtually everywhere. The essence of networking was on full display in the first flowering of this truly grassroots military network.[11] Initially, only company commanders were allowed on the site, encouraging free-flowing, frank discussion. Eventually, for "security reasons," the site was handed over to supervision from above, so some of the zip went out of the exchanges. Still, on balance, this Web site has had a hugely beneficial effect on field operations.

But awareness of the network phenomenon alone did not have an immediate impact on the course of the campaign. Rather, this new understanding allowed U.S. forces to gain a better grasp of the strengths and weaknesses of enemy field and support units—such as they were—and encouraged systematic analysis of the aforementioned five levels that seem to typify all networks. This type of analysis was much needed, since at the outset of the war the insurgent networks had the edge in every category. Organizationally, they proved supple, exhibiting a capacity for putting Louis Beam's concept of "leaderless resistance" into action. In terms of doctrine, the swarm characterized both the tactical level (for example, in coordinated attacks on truck convoys) and the operational level (with the orchestration of a drumbeat of simultaneous strikes all over Anbar Province and even reaching out elsewhere in Iraq).

The insurgents' social bonds were also tight, bearing out a point that Loretta Napoleoni made about Muslim terror networks: "Islamist armed organizations tend to be formed via social bonds."[12] These ties were reinforced by a common narrative based on resistance to American occupation, a story that grew in strength with the revelation of abuses such as those at Abu Ghraib, and the increasing toll of collateral damage on the Iraqi people. Indeed, this narrative of resistance to occupation brought together disparate groups of what David Kilcullen calls "accidental guerrillas" to join the fight.[13] These fighters almost surely had no interest in al Qaeda's grand visions of a

restored caliphate. Instead, they became allies of convenience because al Qaeda's principal adversary had come to their homeland and presided over the dispossession of the Sunnis.

The insurgent networks were even good at the technological level, the best example being their generally swifter actions in the complex electronic warfare campaign waged around improvised explosive devices (IEDs). If the coalition chose to introduce jammers, the insurgents quickly shifted to the use of base stations, which could not be jammed. The eventual "up-armoring" of vehicles was also quickly offset by the introduction of explosively formed projectiles. The swiftness of enemy reactions made it seem that they had their own version of Companycommand.com.

But there were striking weaknesses in the enemy camp, too—or at least vulnerabilities. The insurgents' organizational structures proved open enough to allow infiltration.[14] In terms of doctrine, the insurgents were not the only ones who could swarm. This tactic was parsed by coalition company commanders, as noted above, who at one point even conducted a successful Operation *Swarmer* against enemy swarms.

Finally, at the social level of analysis, kinship and other ties may have been tight within tribes, but not as tight across them, because rivalries and resentments could be exploited. And a wide chasm separated the Sunni and Shi'a, a gap broadened by Zarqawi's campaign to foment civil war and bin Laden's willingness to go along with it. Perhaps most important, though, al Qaeda cadres undermined their own narrative by their harsh conduct when they tried to consolidate their hold on Anbar—acts ranging from outright extortion to demanding bribes to operating kangaroo courts and executing dissenters. It was these excesses that sparked the rise of a counternetwork against al Qaeda, drawing members from the ranks of the insurgents themselves. It came to be known as "the Awakening Movement," and its fighters were called the "Sons of Iraq."

Under the rubric of a concept I had been recommending and calling "outpost and outreach" since the summer of 2004, the netwar against al Qaeda in Iraq got under way late in 2006. The outpost part of the scheme consisted of creating a physical network of platoon-sized outposts in which friendly Iraqi forces and Americans were collocated. This got many of our troops off the large forward operating bases that had limited their ability to develop intelligence and slowed their responses to attacks. As one of the officers who led the first wave of this netwar noted, the outposts served as "lily pads for mechanized quick-reaction forces" and "also acted as flybait . . . for the insurgents who suffered heavy casualties" when they attacked them.[15]

the outpost part of the scheme got many of our troops off the large forward operating bases that had limited their ability to develop intelligence and slowed their responses to attacks

The outreach part of the concept was aimed more at social engagement. The outposts improved response time and enabled us to swarm better at the doctrinal level, but it was the social networking phenomenon, the hallmark of the Awakening Movement, that improved intelligence coming into our system and catalyzed the creation of many more friendly nodes. Respect increased among Iraqis for the Americans' willingness to deploy their forces in small posts near the action and far from the protection afforded by big bases. That helped build up our own narrative, even as the

enemy's "story" was unraveling because of al Qaeda's many excesses in Anbar.

Even the campaign against the IED networks benefited from a shift toward a more network-analytic approach. Where technological fixes by the coalition forces—from electronic jamming to the rise of "moving fortresses" such as the mine-resistant, ambush-protected vehicle—were introduced slowly and insurgent networks fielded countermeasures swiftly, a focus at the organizational level quickly paid large dividends. It turned out that the IED networks were reliant on a relatively small number of key nodes—especially in terms of people like financiers and locations such as bomb factories—that acted as hubs from which chains of operatives (for example, "bomb placers") emanated. Once the social dynamic empowered by the outpost-and-outreach concept began to take hold, a virtual "golden seam" of information about the IED networks opened up. Once the enemy system was understood and illuminated, the means for countering it came naturally and were to prove much more successful than the previous emphasis on the earlier, technology-focused efforts to win the IED fight.

the war in Iraq has featured almost laboratory-like conditions for examining the effects of the netwar approach to counterinsurgency

For all the positive developments that flowed from reframing the campaign in Iraq along netwar lines, at this writing there is a growing risk that previous gains will soon dissipate; some of the key elements in the counterinsurgent network are either being disassembled or coming undone, due to the withdrawal of American troops from small outposts—they are largely back on the big operating bases—and the decreasing willingness to continue engaging tribal actors.

The network of outposts, while still in place, has been weakened terribly by the withdrawal of the U.S. garrisons to larger, more remote bases. This removal severs hard-forged social ties and will soon have the dire dual effects of reducing the flow of incoming intelligence and fostering a renewal of sectarian frictions. There is much evidence in the renewed violence in Iraq that this is what is happening.[16]

From a netwar perspective, the right strategy would be to keep residual American troops circulating through the small, local outposts as much as possible. These are key physical nodes in the counterinsurgent network, and a wide range of social interconnections radiates out from them. If the positive momentum in the campaign of the past 3 years is to be sustained and built upon, American soldiers must come to and through these sites regularly. This can still be done relatively easily in strategic and logistical terms—even in the face of impending sharp force drawdowns—because the total number of troops in all these outposts, throughout Iraq, never exceeded about 5 percent of overall U.S. forces in country. Even with steep reductions in total forces in Iraq, the garrisons can still be manned and supplied, and their security supported by remainder forces. The point is that the outpost network is physically small enough to be able to keep functioning despite force drawdowns that might leave a residual presence of just a few tens of thousands of soldiers.

In sum, the war in Iraq has featured almost laboratory-like conditions for examining the effects of the netwar approach to counterinsurgency, providing insights at each of the five levels of network analysis. An almost universal consensus held that the situation was dire until late 2006—in journalist Thomas Ricks's view, a

"fiasco." At that point, the net shift took place. Organizationally, coalition forces went from a relatively few large units of action on a few large bases to an order of battle comprised of hundreds of small combat teams distributed across a wide network of platoon-sized outposts.

In social terms, the network was hugely empowered by the decision to reach out and work with Sunnis who had previously been fighting alongside and/or working with the insurgents—or at least tolerating them. Their openness to switching sides was catalyzed by al Qaeda's missteps at the narrative level. The terrorists' "brand" had changed from freedom fighters against the American occupation forces to oppressors of the indigenous insurgents.

These great improvements at the organizational, social, and narrative levels made it possible for a swarming doctrine to emerge, with al Qaeda in Iraq operatives struck from every direction. This approach was further aided by the provision of some communications equipment to the Sons of Iraq who, thus connected, were able to assist in striking at swift-moving enemy units by passing along timely, targetable information to their compatriots as well as to coalition forces.

For all the ostensible differences between the campaigns in Iraq and Afghanistan—which seemingly get most of the official attention—it should be realized that there are some similarities as well. And on examination, it appears that there are good opportunities for transplanting many elements of the successful netwar campaign in Iraq to Afghanistan, as is argued in the next section. At a minimum, the "outpost and outreach" concept of operations can be taken there. But there can be even more to netwar in Afghanistan, as openings abound to craft a new narrative, build new social ties, and overwhelm the Taliban with the rekindling of a swift, smart, swarm-oriented approach.

Netwar in Afghanistan

If the conflict in Iraq started out with little in the way of netwar-style operations—which emerged only some 3 years into the campaign there—Operation *Enduring Freedom* clearly took the networked approach from the outset. This was most evident at the organizational, doctrinal, and technological levels. Instead of deploying a few hundreds of thousands of massed troops to invade Afghanistan, the offensive mounted in the fall of 2001 was conducted by 11 Special Forces A-teams—some 200 Soldiers—riding horses at the outset. They worked with and were able to empower much larger, friendly Afghan forces totaling over 10,000 fighters, but they were still organized in small, widely distributed units and outnumbered by the Taliban and al Qaeda by about 3 to 1.[17] Nevertheless, they swept their enemies before them, and drove the Taliban out of power in just a few weeks.

Their supple organizational structure aside, it was the ability of the Special Forces to strike at the Taliban simultaneously from several points, supported by at-the-ready airpower, that contributed so significantly to the swift success of this campaign. It was the essence of the swarming doctrine so naturally well suited to networks. The ground teams and the attack aircraft were further knitted together at the technological level, where information was widely and quickly shared, in part due to the skillful use of the Tactical Web Page (TWP) by the Special Forces.

Originally intended for logistical and other combat support functions, the TWP was soon used by the A-teams for battle coordination and management purposes. Tight coupling with attack aircraft made for a networked level of cooperation perhaps never seen before. The U.S. Navy, whose aircraft provided most of the sorties in the campaign—though not the majority of the tonnage dropped—made a true netwar-oriented

decision early on to refrain from predesignating targets, relying instead on the benefits to be had by allowing their pilots simply to connect directly with the network nodes on the ground. Timeliness and accuracy were greatly improved, especially when measured against the opening, air-only weeks of *Enduring Freedom*, before the Special Forces were set loose.

To be sure, the campaign was not perfect. Most of the Taliban and al Qaeda leaders and fighters got away, crossing Afghanistan's eastern border into the tribal badlands of Pakistan.

it was the failure to address the narrative aspect of the netwar with far more nuance that made it possible for the Taliban to make a comeback

Many explanations have been given for this. The leading accounts are that too few U.S. troops were on the ground and that apparently friendly Afghan allies may still have harbored soft feelings for the Taliban and al Qaeda, allowing them to escape from Tora Bora. However, a netwar-based analysis of the campaign would lead to another conclusion. For all the distributed nature of the first-wave assault, followup operations were far too linear, focusing on a step-by-step, city-by-city process of liberation.

A more fully netwar-oriented approach would have viewed the battlespace in a less linear way throughout the campaign, and elements of American follow-on forces—principally the airborne and mountain troops—should have been moved (or jumped) into blocking positions along the border quite early on. This would have been more consistent with the nonlinear logic of netwar and would likely have prevented the mass exodus of enemy fighters through our slower-moving pincers at the end of this opening campaign.

There were other problems as well, though their effects were not felt until much later. For example, at the narrative level, our close association with the Northern Alliance—seen by many as brutal Russian proxies in the Afghan civil war—made it hard to portray the campaign as a straight liberation. This point was only reinforced when some members of the Northern Alliance, appointed to positions in the new government, were perceived to behave in corrupt ways and to resort to violence to consolidate their control. Indeed, it was the failure to address the narrative aspect of the netwar with far more nuance that made it possible for the Taliban—with their own "repaired narrative" well on display—to make a comeback, starting in earnest about 2005. Needless to say, these problems at the narrative level resonated socially as well and have contributed to our difficulties over the past few years.

In the face of these mounting reverses, instead of keeping what worked about our netwar and addressing the areas in which we were deficient—the narrative and social levels—strategic choices were made that both undermined our successes and worsened our problem areas. The principal cause of the deteriorating situation in Afghanistan was the organizational shift from a network of "the many and the small" units of action to something more akin to "the few and the large." The nimble network of A-teams and other light forces gave way to a much heavier footprint. Instead of emphasizing the creation of many small outposts, a few bases became quite large—Bagram in particular.

Doctrinally, the shift to more of a big-unit style of operations made us slower to respond to fleeting targets and much less able to achieve surprise. Furthermore, this approach led to a

U.S. Air Force (Brenda Nipper)

IED killed and wounded multinational forces near German embassy and U.S. base in Kabul

fixation on hunting down enemy leaders—a problematic practice given the highly networked nature of the insurgency.[18]

Even at the technological level, there was some retrograde movement as more centralized control was imposed and enforced, even from afar. After all, the same technology that empowers networking enables over-control. These developments also contributed to the growing amount of collateral damage in counterinsurgency operations, which caused the narrative and social dimensions of the netwar effort to deteriorate. Indeed, at this point, the period roughly between the summer of 2007 and summer of 2009, it became hard to continue viewing the campaign in netwar terms.

The reconstruction efforts that have played an integral role in the campaign to stabilize Afghanistan have seen less a networked approach than a more centralized national one as well. The best evidence can be seen in the disparity between the number of active nongovernmental organizations (NGOs) operating in the country—over 150 today—versus the more than 2,000 for-profit contracting firms on the ground. While the NGO networks have made real strides in improving health, education, and the condition of women throughout the country, the private contractors have often had much less beneficial impact. Indeed, they have often bred resentment by their perceived overbearing behavior, causing many Afghans, including their leaders, to lump the NGOs in with them as targets of their opprobrium.[19]

Overall, as we consider the strategy currently pursued, the distance from netwar seems only to grow. In terms of force levels, the United States is in the process of roughly doubling its military presence to about 100,000 troops. This is clearly an attempt to replicate the claimed effects of "the surge" in Iraq, but the real improvements in Iraq had more to do with creating a network of small outposts

and reaching out to form a social network with many of the very insurgents who were fighting us until they were embraced. It was not a result driven principally by numbers.

the real-world effect of killing the wrong people is to spark blood feuds, energize enemy recruitment, and raise the risk of setting off a social revolution in Pakistan

Similarly, more troops in Afghanistan will not by themselves make a positive difference in the campaign. Instead, there need to be radical changes in organization and doctrine that will reawaken the iconic netwar qualities of being "smaller, quicker, closer." In this regard, there are a few bright spots. The Special Forces are trying to operate in this fashion, as are the Marines, who are increasingly settling in small outposts, apparently for the duration of their tours. In this respect, Green Berets and Marines seem to be rekindling some of the best attributes of the early small-unit war in Vietnam, which should be viewed as an embryonic case of the use of netwar against insurgents.[20]

But beyond the Special Forces and Marine small unit efforts, General David Petraeus is using most of his other forces to focus on winning a few big engagements (for example, Marjah), while at the same time many small outposts are being closed. The counterinsurgent network is thus, in a real sense, being dismantled in favor of a more traditional effort. Another step back from netwar can be seen in the attempt to win with a Predator bombing campaign against Taliban and al Qaeda targets located in Pakistani territory.

President Obama has quite determinedly ratcheted up the intensity of these unmanned aircraft attacks. The most difficult aspect of this approach has been that it lacks the kind of network on the ground that existed when the 11 Special Forces A-teams were set loose late in 2001. There are almost surely some operatives across the border who are providing occasional targeting information, but that is a far cry from running a swarming maneuver campaign in many places in the FATA, forcing the enemy to leave hide-sites and scramble from one location to another under fire.

Another problem with the Predator campaign—beyond its low operational utility—is that it is causing grievous damage at the social level. Inevitably, some of the damage in a bombing campaign that lacks a true ground network to link up with is done to noncombatants. "Collateral damage" may be a convenient, cool euphemism, but the real-world effect of killing the wrong people—even if only small numbers of them—is to spark blood feuds, energize enemy recruitment, and, in a case of war contagion, raise the risk of setting off a social revolution in Pakistan. Tensions in this strategically important country are already high given the sustained, American-inspired effort to foster a fuller form of democracy there at a time when Pakistanis may not yet be ready, by dint of their history and culture, to embrace our brand of political pluralism.

This last point about our "democracy project" brings the analysis back to the narrative level of netwar in Afghanistan, where this aspect of our strategy revolves around trying to build a legitimate, participatory central government in Kabul. The problems with this narrative are twofold. First, inside Afghanistan, our association with leaders perceived to be corrupt in their wielding of power has made democracy a hard "product" to market to the people. And the overt fraud that was associated with the

August 2009 election did quite grievous harm to our preferred narrative.

But there is a second problem: the American-led democracy project overall is pursued in highly inconsistent ways. For example, the United States, while striving to spread democracy to Afghanistan and Iraq, seems content to keep dealing with authoritarian rulers in Saudi Arabia, Egypt, and elsewhere throughout the 44 Muslim countries of the world. Such contradictory behavior is sheer poison for the narrative aspect of netwar. Until the pursuit of democracy is perceived as being part of a consistent policy everywhere, the persuasive power of the call to pluralism will remain much inhibited in Afghanistan and elsewhere.

What Is to Be Done?

The foregoing analysis has conveyed the sense that, in Afghanistan, a good start went badly wrong—not immediately, but surely and steadily. So the question is how to get back on course, and to identify what the netwar perspective offers by way of policy-relevant guidance. The answers are clear using the five levels of netwar analysis, and the policy shifts implied may not be all that difficult to parse, either.

At the narrative and social levels, for example, the implication is that Afghanistan is probably not a country where much effort should be given to try to form and sustain a strong central government. Instead, something looser—cantonal, like Switzerland, or confederated, as in Joseph Biden's early (and misplaced) plan for a "soft partition" of Iraq—seems far more appropriate.[21] But going beyond thinking about a new national narrative, we ought to be forging strong social ties to the many tribes that can be turned against Mullah Omar's Taliban and Osama bin Laden's al Qaeda. Just as the Anbar Awakening Movement sliced away large swaths of the insurgency in Iraq, so a similar movement can succeed in Afghanistan. Much has been said about the differences between these theaters of operations; netwar allows us to see their similarities more clearly.

These narrative and social shifts—away from centralization to something looser and more networked—would then reenergize a return to the organizational forms and doctrinal concepts that initially shone so brightly in the fall of 2001. Remote outposts in this largely rural country could be both manned and sustained with small American and allied contingents working hand in hand with friendly, newly empowered Afghan tribes. There should also be a shift away from for-profit private contractors in favor of growing the NGO networks and leveraging their already deep ties to many of the tribes by focusing on the health, education, and human rights initiatives they have done so much to carry forward. The military outposts and the NGO outreach could truly form a winning combination.

The implication here is that U.S. forces in country did not need to be doubled in size, and command and control of them does not need to be tighter. Instead, far fewer forces—probably less than 50,000—would prove sufficient for populating and supporting a physical network of small outposts and nodes in the NGO network. Reaching out to reconcilable tribal elements will then create a social network that will provide both additional friendly fighters and a cascade of intelligence about enemy numbers, dispositions, and movements.

In fact, this networked approach would allow allied forces in Afghanistan—long hampered in their ability to cooperate by balky, hierarchical, too-separate organizational structures—to coordinate their campaign efforts far better and to seize the clear initiative from the enemy. When conducted in the context of

truly irregular military operations, netwar is all about fusing "sensors and shooters"—that is, it is about using ubiquitous information flows best by allowing many small units of action *to act*, largely on their own initiative, but still within the overall rubric of campaign objectives. For this approach to take hold, senior leaders have to be willing to "hold the reins loosely," as they did in that first campaign in the fall of 2001.[22]

With the foregoing in mind, it appears that the netwar paradigm provides a fresh perspective on American endgame strategies in Afghanistan. And the options that emerge from this analysis can be easily summed up in terms of the five levels of netwar analysis. First, there is the whole question of narrative that, as has been noted, should shift away from a story about creating a strong central government in a place that has never really had one, or at least not for long. Instead, an image should be cultivated of an Afghanistan that is much more loosely confederated, with security provided by strong tribes fully able to defend their parts of the country. Secretary of Defense Robert Gates, before hewing to the "centralist line," actually seemed to be pursuing this more networked approach when he spoke of it not being useful to try to create a democratic "Valhalla" in Afghanistan.[23]

an image should be cultivated of an Afghanistan that is much more loosely confederated, with security provided by strong tribes fully able to defend their parts of the country

The benefit of returning to Gates's more limited view of central governance is that it would completely energize the social dimension of the netwar, bringing many tribes over to the counterterrorist cause—much as occurred in Anbar in Iraq—and putting the insurgents on the run. This offensive would consist of an ongoing swarming of the enemy, the third key element in the netwar that could unfold there. The added bonus to all this would be that the campaign in Afghanistan could be won *in* Afghanistan—much as the campaign in Iraq was turned around without having to take the war beyond its borders—relieving the stress and strain on the Pakistani people and polity. This is not to say that the terrorists will be granted haven in Pakistan; rather, the point is that Afghanistan's crisis can be resolved without cross-border escalation. As to terror networks in Pakistan, they can be treated to a tailor-made netwar campaign that would form part of our "global pursuit" of them.

But first, and probably most important, in order to use netwar to win in Afghanistan, we must return to the appropriate organizational design there. This facet of the netwar paradigm is perhaps the simplest to understand: we must not be a military force of the "few and the large" units of action. Instead, we must craft an armed force of the "many and the small" units of action and return to an emphasis on technologies that help us to see more and to move information swiftly among our many distributed units, more like the 11 Special Forces A-teams of 2001 and the TWP that so empowered them by linking them to each other and to the attack aircraft that helped make their victory possible.[24]

This does not mean that the campaign must be conducted entirely by special operations forces. But it does suggest that these elite troops have become, to some extent, a doctrinal laboratory for waging netwar and that their best practices should come to guide all our field forces—special or not.

All this emphasis on getting the military concept of operations right should be undertaken along with, not instead of, the rekindling

of the other key elements that, taken together, would constitute a net shift in Afghanistan. Especially important will be engaging the enemy at the level of ideas, a process reliant on the skillful use of strategic communications and public diplomacy. The netwar perspective raises our consciousness in this issue area in two key ways. First, given the inability to control the many conduits of information, from global media to word-of-mouth links in rural areas, special attention should be given to the role that physical actions play in sending messages. Unambiguously clear actions, such as closing some detention centers, firing corrupt contractors, challenging fraudulent elections, and withdrawing the bulk of our field forces, make it harder for the enemy's propaganda to take hold and more likely that our own message will come through the media clutter. Second, listening is an important aspect of strategic communications—something all good networks do that reflects their profound participatory social norm. This does not mean giving up one's values or most necessary policies, but it does mean being willing to make some changes in flexible ways, based on feedback from those we seek to influence.

With all the foregoing in mind, there is at minimum a strong case to be made for launching a serious inquiry into the prospect of making a net shift in Afghanistan. Given the success of a similar shift in Iraq, and the parlous state of affairs in the campaign against the Taliban reached by having pursued more traditional counterinsurgency approaches, it is difficult to see how a change to a more netwar-oriented approach can be resisted. A strategy that puts a focus on networks at its heart rather than on an inevitably troubled nationbuilding quest will prove more socially, culturally, and historically sensitive to the deep patterns of Afghan life. Such a netwar strategy would also allow for a smaller but smarter—and thus more effective—military campaign, while at the same time reenergizing and empowering the civil society networks that have already done so much in Afghanistan, and are poised to do so much more. A net shift now is the change we need. PRISM

Notes

[1] For a detailed description of Chechen swarm tactics in the first conflict, see Stasys Knezys and Romanas Sedlickas, *The War in Chechnya* (College Station: Texas A&M University Press, 1999). The second conflict is thoroughly and thoughtfully analyzed in Mark Kramer, "The Perils of Counterinsurgency," *International Security* 29, no. 3 (Winter 2004/2005). For analysis of a smaller example on the use of swarming—the terrorist attack on Mumbai in November 2008—see John Arquilla, "The Coming Swarm," *The New York Times*, February 15, 2009.

[2] For a thoughtful discussion of networks and their growing ability to swarm, see Howard Rheingold, *Smart Mobs: The Next Social Revolution* (Cambridge: Perseus Publishing, 2002), and Dorothy Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999), especially 228–230, which provide a good survey of early hacktivist practices.

[3] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004), especially 152–158 and 168–171.

[4] Ibid., 144.

[5] See Louis Beam, "Leaderless Resistance," *The Seditionist*, no. 12 (February 1992).

[6] On Osama bin Laden's grudging decision to acknowledge Zarqawi's leadership in Iraq, see Loretta Napoleoni, *Insurgent Iraq: Al Zarqawi and the New Generation* (New York: Seven Stories Press, 2005), 123–124.

[7] For details on these networks, see Ahmed Hashim, *Insurgency and Counter-Insurgency in Iraq* (Ithaca, NY: Cornell University Press, 2006), especially chapter 2, and John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (New York: John Wiley and Sons, Inc., 2007), 74–79.

[8] Rumsfeld's adoption of the "netwar perspective" is noted, for example, in Thomas Donnelly, "Donald Rumsfeld's War," *The Weekly Standard*, December 16, 2004.

[9] See Bruce Hoffman, "Plan of Attack," *The Atlantic Monthly* (July–August 2004).

[10] Fareed Zakaria, "How to Win the 'Netwar' in Iraq," *Newsweek*, October 11, 2004.

[11] See N. Dixon et al., *Company Command: Unleashing the Power of the Army Profession* (West Point, NY: Center for the Advancement of Leader Development and Organizational Learning, 2005). A more concise description of this network of company commanders can be found in Dan Baum, "Battle Lessons: What the Generals Don't Know," *The New Yorker*, January 17, 2005, 42–48.

[12] Napoleoni, 125.

[13] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York: Oxford University Press, 2009).

[14] Of course, infiltration went both ways, with many formations of the reconstituted Iraqi military and police being penetrated by insurgents as well.

[15] Niel Smith, "Anbar Awakens: The Tipping Point," *Military Review* (March–April 2008).

[16] See the assessment of Iraqi journalist Emad Al-Shara, "Iraq Fears Renewed Violence," *The Philadelphia Inquirer*, June 25, 2009.

[17] Stephen Biddle, *Afghanistan and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle, PA: Strategic Studies Institute, 2002), 14, fn. 30.

[18] An early warning against focusing too much on "leaders" can be found in John Arquilla, "Not Wanted: Dead or Alive," *Los Angeles Times*, December 30, 2001.

[19] See, for example, Justin Huggler, "Afghan Candidate Calls for Expulsion of 'Corrupt' NGOs," *The Independent*, September 13, 2005. This is a call that President Hamid Karzai has taken up as recently as spring of 2010.

[20] This networked approach had a major technological dimension, too—in the form of a remarkable array of unattended ground sensors. See Michael Maclear, *The Ten Thousand Day War: Vietnam: 1945–1975* (New York: St. Martin's Press, 1981), especially 207–222.

[21] A good analysis of the perils of trying to shore up central government in Afghanistan can be found in Thomas H. Johnson and M. Chris Mason, "No Sign until the Burst of Fire," *International Security* 32, no. 4 (Spring 2008), 41–77.

[22] Aside from its stirring narrative of the campaign, Doug Stanton's *Horse Soldiers: The Extraordinary Story of a Band of U.S. Soldiers Who Rode to Victory in Afghanistan* (New York: Scribner, 2009) also contains a deeply insightful analysis of the kind of power unleashed when command and control is allowed to become command and "decontrol." It is an approach that engenders some risks when the offensive is conducted by a much outnumbered force, but the returns are even higher.

[23] See Ann Scott Tyson, "Gates Predicts 'Slog' in Afghanistan," *The Washington Post*, January 28, 2009.

[24] The template for reconfiguring our organizational and technological approaches to campaigning in Afghanistan should be the remarkably insightful analysis by C.H. Briscoe et al., *Weapon of Choice: U.S. Army Special Forces in Afghanistan* (Fort Leavenworth, KS: Combat Studies Institute Press, 2004).