

THE RELUCTANT TRANSFORMATION
OF THE AMERICAN MILITARY

John Arquilla



Ivan R. Dee
CHICAGO 2008

CHAPTER SEVEN

A New Course of Study: "Netwar 101"

SINCE THE ONSET of what the Pentagon occasionally calls "the long war" on terror, there have perhaps been no two words more commonly used to describe our adversaries than "terror networks." These words suggest shadowy cells dispersed throughout the world, relentlessly pursuing their common goal of undermining American security interests and able to stay on task with little overt control from any sort of high command. The organizational structures that distinguish these groups as networks have three fundamental forms: hubs, where one central node connects to many "spokes"; chains, good for moving people, money, and arms; and areas in which all members are connected to one another. Mohammed Atta, for example, was a hub for the 9/11 attackers. The "ratlines" that foreign fighters have followed into Iraq are classic chains. And the infamous "Hamburg cell" of al Qaeda was exemplary of the many terrorist network nodes where all members are in contact with one another. In practice, most terror networks exhibit hybrid designs that often feature skillful blends of all three of these fundamental forms.

The network form of organization, which has proved so attractive and useful to terrorists, has also impelled them to pio-

neer new modes of confrontation and conflict; for even though their networks are magnets for smart, tough, dedicated operatives, it would be suicidal for the terrorists to try to take on their betters by traditional means. They are simply too few in number and too lightly armed. For example, at its height al Qaeda has probably had no more than a few thousand fighters in the network's core groups—about as many individuals as carry rifles in an average American infantry brigade. And when the new generation of recruits—the largely unskilled one that fills out the ranks of their self-depleting kamikaze-style suicide squads in Iraq—is included, the numbers don't grow much. Even including Iraqi insurgent network allies, or resurgent Taliban in Afghanistan, the total numbers of combatants al Qaeda can field wouldn't so much as fill out one U.S. division.

In order to engage their much bigger and far more heavily armed opponents with some hope of success, al Qaeda and affiliated terrorist and insurgent networks have had to craft a new way of war—"netwar," to be precise. This is a term that my RAND Corporation colleague David Ronfeldt and I introduced in the early 1990s to describe the manner in which we believed networks would fight.

We reasoned that instead of massing forces, which has been the goal of most militaries throughout history, networks would become adept at dispersing their numerous small units in many locations. This would benefit both defense and offense, for such a loose deployment scheme would make them harder to find and destroy while at the same time allowing them the opportunity to mount swarming attacks in many different places. In an age in which ever more destructive power continues to migrate into the hands of small groups—think of the damage just nineteen al Qaeda fighters achieved on 9/11, or what a terrorist cell armed with nuclear weapons might do one day—the netwar approach seems ideally suited to their needs.

Ronfeldt and I reasoned that this kind of warfare was coming, and that the only effective way to counter it was for our

military, intelligence, and law enforcement elements to develop nimble networks of their own in the fight against the terrorists. It was, we thought, very much like the situation in the blitzkrieg era some seventy years ago, when military experts concluded that "the best way to fight a tank is with a tank." Now, we thought, "It takes a network to fight a network." Yet in all the years since we first fielded this concept for the Department of Defense, terrorists, criminals, insurgents, and even militant social activists have consistently shown a greater grasp of network principles than the U.S. military, and much more willingness to employ them in practice. Hence the need to continue to reiterate—ad nauseam, it sometimes seems—a kind of primer in network-age warfare for both senior leaders and field operatives. "Netwar 101" is what I have called this effort to raise the group consciousness of the U.S. military, first by analyzing cases of networks in battle, then by identifying the organizational, doctrinal, and strategic implications of this new phenomenon.

Over the past two decades there have been abundant examples of netwar. Among the first was the rise of a skillfully (but not centrally) coordinated network of nearly three hundred small drug operations in Colombia in the wake of American-led efforts that had resulted in the killing or capture of the leaders of the Medellín and Cali cartels. These new networks of small operators had no commander-in-chief, but they shared the common goal of producing and distributing their product, and they enjoyed secure means of communication provided by couriers, encrypted phones, and web and internet links. Soon more cocaine than ever before was making its way to the United States, and the Colombian networks had begun to forge new ties with increasingly aggressive Mexican networks that initially had specialized only in transshipping drugs.

Against this rising tide of drug networks, the American response, the multibillion-dollar "Plan Colombia," has continued

to focus on targeting "leaders," despite the fact that the networks don't rely on one or a few bosses to run the show. As you might imagine, this strategy has not worked at all. To be sure, there are other elements to the costly counterdrug plan (such as encouraging crop substitution and using herbicides to eradicate crops), but the networks have just as easily outflanked these. For example, to get around aerial spraying of their fields, the drug networks quickly shifted to interplanting coca among legitimate crops. Now Colombian troops must find these fields, then go in and pull out the coca by hand, an exceedingly slow process that leaves them at risk of being attacked while they are at work. Most troubling of all is that the new Colombian model for the cocaine business, based on the formation of many small but highly networked operators, is largely the one being followed today by drug rings from Afghanistan to Southeast Asia and beyond. If there is ever to be hope of winning the "war on drugs"—which we have now been waging formally for more than thirty years—it undoubtedly lies in our willingness and ability to learn more about how to undermine networks.

Around the same time that drug operators were becoming so fully networked, insurgents in various areas of the world also began to shift toward far more dispersed and "decontrolled" organizational forms. Sometimes this process was unwittingly helped along by their opponents who, like the United States, were single-mindedly focused on knocking out enemy leaders. For example, in Chechnya, the breakaway Russian republic, Muslim militants saw their leader Dzhokhar Dudayev tracked, targeted, and killed by Russian forces early on in their attempt at armed secession, which ran from 1994 to 1996. After Dudayev's death, however, the Chechens relied much more on operations of small fighting cells of no more than twelve to twenty militants each, bonded together by tribal and clan-based social ties, and given little direct tactical oversight. In 1996 a force of just several thousand insurgents, organized in

this loose fashion and interconnected mostly by runners and a clever mix of short-range and shortwave radios, drove a far larger Russian force from their country.

They did so in pitched battles featuring swarming attacks coming from all directions, not just classical hit-and-run guerrilla raids. And they succeeded despite the fact that the Russian forces were replete with artillery, tanks, and attack aircraft while the Chechens' heaviest weapons were rocket-propelled grenades (RPG). Even though the insurgents sawed off their gun barrels to improve RPG velocity—the better to penetrate tank armor—they were still terribly outgunned. They shouldn't have won, but they did. And the fact that the Russians came back smarter the second time, and have operated more effectively (and been far more brutal) against the Chechens, takes nothing away from the amazing initial campaign by the insurgent networks in 1996. With little or no regularly functioning central command structure, in small numbers and fielding only light weapons, they defeated one of the world's great militaries in direct battle. This was a quintessential case of netwar.

Other netwars have appeared since then, none more haunting than the Iraqi insurgency, which began in earnest in August 2003—a little more than four months after the beginning of the American military occupation—and continued unabated thereafter. The insurgents had no real central leadership, as proven by their persistence after such losses as the capture of Saddam Hussein, the killing of his sons, and the death of the leading terrorist Abu Musab al Zarqawi. Further, al Qaeda fighters were always fairly few in number, and the other rebels were so seriously divided along ethnic and religious lines that a civil war would soon break out. But all the insurgent organizational structures—more the Sunni than the Shi'a, however—emphasized both creating dense interconnectivity between trusted members and allowing great autonomy of action for individual cells. These were the core attributes that gave the

insurgents the ability to wage a protracted contest against the better-armed Americans for control of Iraq.

It turned out to be a struggle that became a quagmire for U.S. forces. By the fall of 2006, most Americans simply wanted it to end. Late in the game (in 2005), Donald Rumsfeld finally began referring publicly to the conflict as a netwar—thanks to a letter from RAND Corporation president Jim Thomson that pointed out the networked nature of the conflict. Thomson put it this way: "The Iraq insurgency demonstrates the closest manifestation yet of 'netwar,' which is characterized by flatter, more linear networks rather than the pyramidal hierarchies and command and control systems of traditional insurgent organizations." This was clearly an epiphany for Rumsfeld, whose own view of military transformation had until this point been governed by technology-oriented issues. As he put it in his seminal article on the topic in 2002, "we must begin shifting the balance in our arsenal between manned and unmanned capabilities, between short- and long-range systems, between stealthy and non-stealthy systems, between sensors and shooters, and between vulnerable and hardened systems." Rumsfeld made no explicit mention of networking at all, save for a nod to the Afghan campaign, which featured an ability to "communicate and operate seamlessly on the battlefield."

Soon after the Thomson letter, Rumsfeld was aggressively encouraging the use of more networklike small-team tactics against the insurgents, to replace the "overwhelming force" approach that had dominated U.S. conduct of the campaign. But for the most part the Pentagon demurred, taking the position that our Iraq policy was failing because Rumsfeld had not sent enough troops to the fight in the first place. This was a point of view that senior generals knew would win traction with elected officials of both parties, and with a broad spectrum of the mass public. And so Rumsfeld's belated call for change initially went unheeded, and he was sacked in the wake of off-year elections

that had seen anti-war rhetoric help the Democrats regain control of both houses of Congress. But the shift to the networked “outpost approach,” coupled with outreach designed to network with friendly tribes and former insurgents, suggests that the netwar paradigm was finally adopted in Iraq by mid-2007.

The experience of netwar in Iraq suggests that yet another key element in this new mode of conflict is the manner in which even a small degree of violence can have disproportionate perceptual effects. Netwar has a postmodern quality, one that takes advantage of the tendency in our time to view the actual fighting in any conflict as a backdrop to the more important “battle of the story” about why the war is being waged in the first place. In this regard, a small, steady trickle of casualties is all that is needed to provide a daily reminder of the “sharp practices”—and some of the outright misrepresentations—that helped sell the war to the American public in the months before the March 2003 invasion of Iraq. For his part, Rumsfeld seemed to be aware of this issue early on, concluding his article on military transformation with a cautionary note along these lines: “And finally, be straight with the American people. Tell them the truth. . . .”

The point is that “influence operations” are likely to play a major role in the outcome of any netwar and therefore must be closely coordinated with military actions in the field. In more traditional terror campaigns, occasional violence is done with a single-minded focus on gaining attention rather than on shaping a battlefield situation. In Iraq the insurgents went well beyond this simple signaling approach to terror. Instead they somehow created a full campaign in which a drumbeat of regular acts of violence was used to wield powerful influence over other Iraqis, the American public, and even world opinion. The insurgents did a better job than U.S. forces in achieving a high degree of integration between the use of force and the effects of their influence operations.

But being more attentive to the role of information could not guarantee that a nation would defeat a network in any given conflict. One need only look to the Israel-Hezbollah War that was waged during the summer of 2006. This was one of the first conflicts to erupt explicitly between a nation and a network. In this instance, Lebanon the nation-state was more an arena than an active combatant—despite the fact that Hezbollah had a formal position in the Lebanese government at the time and still does at this writing (late in 2007). The conflict was precipitated by a Hezbollah raid on an Israeli outpost that resulted in the killing of several Israelis and the capture of a few soldiers. Israeli leaders saw this action as a *casus belli*, one that gave them a justifiable context for the war, and the Israeli Defense Forces (IDF) soon began a vigorous campaign to destroy Hezbollah’s combat capabilities.

Deploying more than 100,000 troops, including heavy armor and artillery, and hundreds of advanced ground-attack aircraft, the IDF advanced into southern Lebanon with the aim of killing or capturing Hezbollah fighters and destroying their stores of missiles. Beyond the immediate battle area, which ran some twenty to twenty-five miles from Lebanon’s southern border to the Litani River—that is, in the area where it runs parallel to the border, before turning northward—the Israeli Air Force waged a relentless strategic bombing campaign that struck at targets throughout all of Lebanon. To disrupt Hezbollah’s central command and control, cell-phone towers were targeted, and supply routes were broken up with strikes against virtually every bridge leading to the battle zone.

Against this might, Hezbollah fielded perhaps as many as three thousand fighters, all organized into small teams—much like the Chechen squads of twelve to twenty fighters that had defeated the Russians ten years earlier. This gave Hezbollah many more units of maneuver than the Israelis, whose principal ground operations—aside from a handful of small, deeply

infiltrated "spotter teams"—were undertaken mostly by units comprised of at least several hundred soldiers. Hezbollah had taken the precaution of prepositioning missiles in hidden sites all across the battle zone, so Israeli efforts to disrupt the movement of weapons southward was preempted. So were Israeli attempts to disrupt Hezbollah's command and control with aerial bombing, as the small networks of fighters were prebriefed on the locations of weapons caches—the overall arsenal probably totaled about thirteen thousand missiles and rockets—throughout an area that had been subdivided into seventy-five "military zones" before the war. All the teams had to do was unearth the weapons, move to nearby firing sites when necessary, launch them, and move on. "Shoot and scoot," if you will. No stream of orders from a high command was necessary. Just aim south to make sure the rockets fell on Israeli soil.

In the event, the network fought well. Hezbollah's forces launched some two hundred missile weapons on the first day of the war, and more than two hundred on the last day of the fighting just over a month later. And when the Israelis realized that their air campaign was failing, the ground forces they unleashed were met not by guerrilla hit-and-run tactics but by a swarm of small Hezbollah teams, fighting them head on, much as the Chechens had done against the Russians in 1996. Interestingly, the "exchange ratio" in these firefights was very nearly even, with each Hezbollah casualty coming close to being matched by an Israeli. By the end of the war the Israelis had indeed killed nearly a thousand Lebanese versus just a few hundred lost on their side, but most of the deaths were suffered by Lebanese civilians who had been caught in the aerial bombing.* And this in turn hurt the Israelis in the "battle of the story" about why and how the war was being waged. In-

*A well-placed source outside the U.S. military and intelligence communities told me that Hezbollah held 183 funerals for fighters killed in direct battle with Israeli troops.

deed, much of the world came to view the Israeli use of force as disproportionate.

What's more, a majority of Israelis felt that the IDF had lost the war, even though about 90 percent of the public had supported an air-only campaign against Hezbollah, the very strategy that resulted in so much international opprobrium being heaped upon Israel. In the wake of this conflict, the high-level Winograd Commission was appointed to determine what had gone wrong, and delivered a scathing report on Israeli military performance during the conflict. The military chief of staff who had masterminded the campaign (air force Lt. Gen. Dan Halutz) felt obliged to resign. More than anything else, the war shook Israeli self-confidence. Hezbollah missile attacks on northern Israel had inflicted little real damage—just a fraction of that done by the bombing of Lebanon. But the conflict in the summer of 2006 was yet another piece of evidence suggesting that Israel was having a hard time dealing with a nettlesome network. Hezbollah had withstood the Israeli occupation of southern Lebanon for years, beginning in the 1980s, and finally drove the IDF out in 2000. Six years later the terror network had once again slipped all of Israel's heavy punches and managed to deliver more than a few of its own. For a country that had been defeating Arab national armies regularly since 1948, the inability of the IDF to defeat this Hezbollah network struck a real nerve among all Israelis.

It should strike a chord in American strategic thought as well, given our own difficulties in grappling with terror networks. But it hasn't, as the American military is, for the most part, reluctant to learn from others' experiences. The comment I have most often heard about the Israel-Lebanon War of 2006, including from a range of our general officers, is that "We would never have done it like that." Perhaps not. But the way the United States has sought to grapple with networks has been, with few exceptions, by mostly conventional military means, along with a mania for hunting down "leaders" of an

organization that can function quite well without much high-level direction. And we have continued to pursue our well-worn paths despite the fact that our experiences of the past several years suggest the urgent need to think in terms of netwar, to recognize that the hallowed principles of war have been affected by the emergence of the network. Our reluctance to make this intellectual leap imperils us the most.

*

The greatest problems bedeviling American efforts to confront and defeat hostile networks are conceptual. And the most prominent of these is the apparent unwillingness to understand the networks themselves. Instead of being seen as autonomous entities, terror networks have, all too conveniently, been viewed by U.S. leaders as wedded to nation-states. Thus in the first great conflict between nations and networks, which has been under way since September 11, 2001, we have been trying to defeat the networks by going after other nation-states.* More than any other reason, I believe, this is why we invaded Iraq. Our security establishment and senior elected leaders all think in terms of nations, not networks. We are constrained by old habits of mind, which in this case have deep roots in the general history of armed conflict.

During most of the period since the rise of modern nation-states about five hundred years ago, wars have been waged principally by states against other states. It has been logical for leaders to think in terms of confronting nations rather than networks. To be sure, in earlier eras there were occasional campaigns against bandits, pirates, smugglers, and other kinds of raiders. And Britain and other colonial powers did accumulate some experience in "small wars" during the nineteenth century. But the vast majority of fighting for the past half-millennium

*Osama bin Laden and his affiliated networks began attacking us earlier than that, but it was only in the wake of the strikes against the World Trade Center and the Pentagon that we awoke to the reality of the terror war.

took place between recognizable nations. Even the early American experience in combating the Barbary pirates was ultimately framed in terms of interstate warfare and featured an expeditionary force launched with the idea of effecting "regime change" in Tripoli, the source of so many of the depredations against American trade. When President Thomas Jefferson chose to negotiate a peace treaty with Barbary, it only put off the day when Britain's Royal Navy would have to bombard the pirate ports, and then post-Napoleonic France would be urged to invade Algeria, taking over this country and eventually controlling its neighbors as well in order finally to quell the nettlesome networks operating from their shores. Alongside the profusion of small colonial wars of this sort were the several conflicts waged throughout the world among states, quite often between the great powers themselves, culminating in two world wars.

But over the past fifty years a fundamental change in warfare has manifested itself, as most conflicts have erupted not between nations but among factions within states. Sometimes these wars have spilled over and involved other countries; but the underlying dynamic driving conflict since the 1950s has been internal. Of approximately thirty wars now going on in the world, only one clearly began as a war between states: the American invasion of Iraq. Even this conflict quickly morphed into a civil war as well as an insurgency against an occupying force. To some extent Palestinian resistance to the Israeli occupation of the West Bank and Gaza might also be construed in terms of classical international conflict—except for the fact that the Palestinians do not represent a recognized nation-state. And ongoing struggles between the Palestinian Fatah and Hamas factions clearly fall under the rubric of internal war.

Beyond Iraq and Israel, today's wars are all quite obviously internal.* From Colombia to Sudan, Somalia to Sri Lanka, and

*The continued fighting in Chechnya, a republic of Russia, is also an internal conflict, though the Chechen goal is clearly to win independence—a goal of many other insurgents around the world.

on to a host of other conflicts, the combatants are usually highly networked ethnic elements within these countries, striving bitterly against each other. Often their hope is to win independent statehood, as has been the goal of Kurdish rebels, for example, for many generations. Sometimes the aim of a rebel group is simply to achieve a more equitable distribution of societal resources, as is certainly the case in the Darfurian uprising against the central Sudanese government's policies. Undoubtedly some of the motivation for Sunni insurgents in Iraq has been to position themselves for a better political and economic arrangement in post-Saddam (and, eventually, post-American-occupation) Iraq. The vast majority of the world's violence is now being perpetrated by networks of substate factions rather than the nations themselves.

Almost all these networks are fighting in unusual ways, ranging from insurgent operations that follow the lines of classic hit-and-run guerrilla warfare to assassinations, kidnappings, and acts of sheer terror. The Tamil Tigers, the ethnic group rebelling against the Sri Lankan government, has adopted widespread suicide tactics on the battlefield. Many Tamil fighters keep vials of cyanide around their necks, an adornment that symbolizes their deep commitment to the cause of independence for their people. The Tamils and many other insurgent networks have thus been pioneering a way of fighting that flows from their organizational form: netwar, which is characterized by there being a common goal but little central control, and by fielding small fighting units so that there can be many of them.

How different this situation today is from the dawn of our own rebellious republic, when George Washington did his utmost to ensure that the Continental Army emulated European military organizational forms and was relentlessly drilled in the most conventional tactics of the time—"massed volley fire" at very short range. Washington may have been leading an insurgent movement, but he wanted to wage war in the most

conventional way possible. Contrary to the stereotypical view of the British Redcoats lined up in close order while our dispersed snipers simply picked them off, the "thin red line" more often than not squared off against an equally thin blue line of Americans.

Washington had to face sharp internal criticism of his preferred approach, especially because he won so few battles in this manner. Maj. Gen. Charles Lee was perhaps the most articulate proponent of an irregular approach, arguing that, as the historian Russell Weigley has summed up his point of view, "a war fought to attain revolutionary purposes ought to be waged in a revolutionary manner." Washington would have none of this, however, and refused to be diverted from his goal of creating a conventional army. In the end, though, Charles Lee and those of like mind seem to have won out, as the outcome of the Revolution was decided in an unconventional campaign conducted mainly by small units in the South, most notably a network of irregulars fighting with Francis Marion, the "Swamp Fox," and other hit-and-run outfits that worked in conjunction with a small regular force under the command of Nathanael Greene. This skillful blending of raiding forces and regulars wore down British Gen. George Cornwallis's army and impelled him to fall back on Yorktown—where he was trapped by the timely appearance of a French blockading fleet and forced to surrender. Yes, George Washington did march his forces down from New York to Yorktown to conduct the siege, and the French naval force under the command of the Comte de Grasse did remove any hope of escape by sea. But Cornwallis would never have found himself trapped in Yorktown had it not been for the exhausting failure of his attempts to come to grips with the irregulars.

These happy results for the networks of early American fighters had little lasting effect on the U.S. military, which quickly returned to the comfortable track of emulating the Europeans—especially the thought and practices of Napoleon

Bonaparte and his principal interpreters. Americans had a particular admiration for a Napoleonic staff officer, the Baron Antoine Henri de Jomini. His great study *The Art of War* was replete with axioms and principles and was widely studied by officers on both sides in the American Civil War. In their preface to the 1862 English edition of Jomini's book, the West Point translators went so far as to say, "General Jomini is admitted by all competent judges to be one of the ablest military critics and historians of this or any other day."

Both sides in the Civil War tried to follow Jomini's principles of offensive warfare, mass, and maneuver, among others, none of which really bore on issues of irregular warfare, and none of which worked as intended in a conflict that saw more than a million troops engaged in a theater of operations as large as Western Europe. Rifles and artillery, as well as rail and telegraph, undermined many of Jomini's formulations. It seems as if Abraham Lincoln was the only leader who saw clearly the need to diverge from strategic dogma. Lincoln consistently urged his generals to distribute their forces in a "cordon offensive" rather than to mass as many of them as possible in one place, in search of a single decisive battle. The president eventually prevailed over his recalcitrant generals by finding some soldiers who were amenable to his ideas (notably Grant, Sherman, and Sheridan). Despite Lincoln's having prevailed in the strategic debates during the Civil War, Jominian thought retained its appeal. Its principles soon returned to prominence and have become the most important guide to American strategy ever since.

Military innovation was thus stifled, and notions of irregular warfare went into almost total eclipse until the Vietnam War. A brief rebirth of unconventional thought occurred during U.S. counterinsurgency operations in the Philippines from 1899 to 1902; and the Marines operating in the Caribbean and Central America during these years, and on into the 1920s and 1930s, showed an aptitude for irregular warfare as well. But the

insights from these smaller conflicts were quickly discarded as the United States became involved in the world wars and, soon after, Korea.

Early in the 1950s, as the Korean War wound down, the cold war accelerated, and the atomic bomb was fast becoming a principal element in the arsenal of our chief adversary, the Soviet Union, there seemed to be a reawakening of latent American capacities for irregular warfare. Army special forces (SF) were created and fielded during these years, with the idea of having their twelve-man "A-teams" lead European partisans in a fight to be waged from behind the lines in areas overrun by Soviet forces in a future war. The opportunity to fight in this way never arose in Europe, but SF soon found much to do in Southeast Asia. U.S. combat involvement in the Vietnam War began with many SF teams helping mount an indigenous resistance to the advancing North Vietnamese army. The Marines soon showed that their institutional memory was intact, rekindling the small-unit capabilities and concepts of an earlier era in their "combined action platoons" (CAPs). With these units they enlisted and empowered the South Vietnamese people who, with Marine support sometimes as small as just a squad of eight to ten, secured a swath of the coast and quite a ways inland as well. The Marines also often operated unconventionally at the platoon level (forty to forty-five riflemen), mounting repeated raids from the sea on Vietcong units. In the process of doing so they created a largely pacified coastal zone that ran virtually the entire length of South Vietnam. All this was accomplished with relatively small numbers of troops and in a highly networked fashion, especially as ground forces were directly linked to Marine pilots accustomed to "putting the 'close' in close air support." But all too soon the Pentagon, which had been fighting a war of ideas about the idea of *this* war, shifted to a "big-unit" approach. And soon all went awry, with tragic end results.

Curiously, the war against the terrorists has followed a similar path. The first strategic steps the United States took were nimble and highly networked—out of necessity, as this was the only way to invade Afghanistan quickly and with any hope of success. The result was remarkable, achieved in conjunction with airpower, as already noted. But it sparked a debate that has raged ever since. A few analysts—I among them—have argued that this campaign changed the nature of war in our time. The majority, however, see the campaign, in the words used by the military historian Stephen Biddle, as “surprisingly orthodox”—though they also see it, seemingly contradictorily, as an anomaly rather than as the kind of operation that could be regularly repeated in other settings. Given that, even when friendly Afghan allies are included, the offensive was mounted with fewer than a third of the total number of Taliban and al Qaeda fighters in the field against them, the argument for the orthodoxy of this campaign grows somewhat strained. Traditional military doctrine usually calls for a numerical superiority of three-to-one at the point of contact in order to mount an offensive with reasonable expectations of success.

An important middle ground in the evaluation of Operation Enduring Freedom was staked out by the defense analyst Michael O’Hanlon, who described the Afghan campaign as a “flawed masterpiece.” Flawed because of the unwillingness of U.S. military commanders to set down some troops at the outset of the campaign—say, from the Ranger regiment, or elements from the Tenth Mountain Division—in a blocking position at Tora Bora so as to prevent Osama bin Laden’s escape with his own cadres and his Taliban allies. O’Hanlon is absolutely correct about this. A true netwar approach to the campaign would have considered the entire battlespace from the outset, and thought in terms of being able to position our forces anywhere we wished in the area of operations. Instead our thinking was far too linear, and the Tenth Mountain did not deploy to the vicinity of Tora Bora until early in 2002—in the

Anaconda operation—just a bit too late. A flawed masterpiece yes, but still a quite remarkable campaign.

One of netwar’s defining characteristics is its nonlinearity, which places a real premium on the ability to engage in lateral or multidimensional thinking. Had such an interdicting move been made in Afghanistan, it would have been “difficult and dangerous,” as O’Hanlon notes. “Yet, given the enormity of the stakes in the war, it would have been appropriate.” O’Hanlon also showed a keen sense of network warfare when he observed of our command and communications systems that the “networks were not always fast enough, especially when the political leadership needed to intercede in specific targeting decisions.” Still, despite its flaws, the Afghan campaign offered a glimpse of a radically different approach to the future of conflict. It is a troubling, disruptive view of things that imperils our long-standing beliefs about military doctrine and implies that the way we invest our resources, organize our forces, and conduct our battles may be in dire need of an overhaul. Yet there remains sharp, sustained resistance to this idea.

*

The evidence for what Martin van Creveld has called “the transformation of war” is overwhelmingly apparent to us now. Two decades ago, in his book of the same title, he was being predictive to a significant degree. But van Creveld’s more recent review of the past century of conflict relies much less on precise than on an exceptionally insightful analysis of events—from World War I right up to Iraq—that fully bears out his initial idea about the major shift in the nature of war. Yet the recent American effort to understand armed conflict, based on our own military experience, has nonetheless been quite mixed and confusing. This has been unquestionably the case since the first glimmerings of our involvement in Indochina more than

fifty years ago, and proceeding on to counterinsurgency operations in Iraq. As I have pointed out, a major reason for our difficulty in grasping the nuances of warfare against networks lies in the roots of our own strategic culture. In particular, our overemphasis on preparing for war against traditional enemies and the use of conventional tactics have not served us well. But there are two other factors at work: the mesmerizing effects of technology and the ineluctable pull of the so-called principles of war. Together with our nation-oriented mind-set, these factors have conspired to hamstring the war on terror, and they threaten to undermine hope for American military reform.

On the technology front, netwar as a concept has been co-opted by computers. The best evidence of this is that the two entities created by the Department of Defense with “netwar” in their names are almost completely focused on “computer network operations” (CNO). The navy has a network warfare command (NETWARCOM) in Norfolk, Virginia, led by a three-star admiral and dedicated almost entirely to ensuring smooth, secure information flows. The Strategic Command (formerly the Strategic Air Command, the famous SAC) in Omaha, Nebraska, also has a network warfare operation, currently under the command of a one-star (brigadier) general. This organization too is all about information security—though it has begun to think in more proactive terms about the offensive aspects of computer network warfare against our adversaries. For both these commands, “network warfare” is mostly about information systems and cyberspace-based operations.

Over the past several years I have attempted to change this perception, and leaders in Norfolk and Omaha do now acknowledge that network warfare includes an understanding of how opposing networks fight, and calls for us to build our own networked units to engage them. But today the major emphasis is still on computers. I am repeatedly told, “We’ll get cyberspace right first, then move on to the other [aspects of netwar].” Meanwhile insurgent networks ran rings around our forces in Iraq—at least until our shift to the “outpost strategy”

in 2007—and nodes in the al Qaeda network have continued to surface throughout the world.

According to the U.S. government’s official statistics, acts of terror (that is, attacks on innocent civilians) rose from just over three thousand in 2005 to more than fourteen thousand in 2006. And almost half the attacks in 2006 took place in Iraq, where the U.S. military is the most heavily deployed, suggesting that these forces can be better used. Surely it is possible to improve our military’s performance by sharing more information swiftly and distributing it widely. But we can achieve this benefit only if we redesign our organizational structures so that they can make maximum use of such information flows.

If not, and if existing hierarchies remain undisturbed, the problems of effectively processing or structuring information inflows will prove insurmountable. Perhaps the best example of this problem was provided by the army a decade ago, in its “Force XXI” exercise. In this instance the entire experimental force was fully digitized, creating an absolute cascade of information, both about friendly positions and possible enemy movements. But because no new organizational structures were introduced, the old hierarchical chain of command was swiftly overwhelmed with data and the force in the field was crippled. This is what happens when new technology is simply grafted onto existing organizational structures. Conversely, when new organizational designs arise to take advantage of new technologies, the results can be stunning. In the case of World War II-era German blitzkrieg, the relatively new weapons technology of the tank was best suited to concentration in a few armor-heavy divisions, rather than being parceled out in small numbers to all divisions, as the French army did. Skillful organizational redesign gave the Germans their advantage at the outset of the war. As in modern architecture, so it is in war: form should follow function.

The other major obstacle for the U.S. military in building a capability for network-style conflict is its unswerving devotion to the canonical principles of war. From the dawn of American

strategic culture, when George Washington strove to emulate classical European military practices, the ideas of mass, unity of command, and simplicity have dominated among our leaders in and out of uniform. To be sure, the other six concepts that make up the best-known set of principles, those articulated by the Baron Jomini and succeeding generations of classical strategists, have not been ignored. These are: the objective, the offensive, economy of force, maneuver, security, and surprise. But it is the inevitable triumph of mass that animates, for example, the doctrine of "overwhelming force" associated with Colin Powell. And it is an unwavering belief in the power of centralized leadership that fosters hierarchy and such stark phrases as President George W. Bush's "I am the decider!" The mania for simplistic strategic formulations is also evident in General Powell's public statement before Operation Desert Storm in 1991, about how the Iraqi army would be defeated in that campaign: "We're going to cut it off, then kill it." George Bush's oft-repeated formula for defeating terrorism—by spreading democracy—is yet another testament to our devotion to simplicity.

But in an age of netwar, overwhelming force is not only unnecessary but almost useless against a dispersed foe. Israeli forces vastly outnumbered and outgunned their Hezbollah opponents in Lebanon during the summer war of 2006, but those numbers made no difference to the network. Hierarchical decision-making is achingly slow, and far too balky to catch up with nimble networks, as the meager results of the first seven years of the war on terror suggest. And if terror networks have far fewer fighters than the armies of even small nation-states, what seems clear is that the networks they wage are complex, dispersed, and nonlinear. The Israelis learned this in Lebanon, and we have learned it in Iraq. Warfare is no longer simple, and to persist in treating it as a simple or straightforward phenomenon is to court disaster.

Even the other six traditional principles of war that our military cleaves to become problematic when viewed from the perspective of netwar. The "objective," for example, seems related to simplicity, as it implies winning by pursuing one very correct goal. But dispersed networks cannot be defeated by one blow; they are truly "flat" organizations, in the business sense, which can continue operating despite losses suffered in any one area. In turn, networks, by virtue of their dispersed and autonomous nature, allow for the pursuit of several objectives simultaneously. And they are able to take the offensive far more easily and broadly than a hierarchically organized armed force could ever hope to. The same is true in areas of security and surprise, where the stealthy nature of networks conveys inherent advantages over their far more visible conventional opponents. Needless to add, this almost surely means that networks also have the edge in maneuverability, as well as in their ability to achieve much with little expenditure of funds and fighters ("economy of force"). The 9/11 attacks on America—as well as earlier ones—prove this point, given that al Qaeda caused so much disruption in return for the modest investment of nineteen fighters and perhaps \$300,000.

American fixation on technological solutions, and our single-minded devotion to principles of war that are either ineffective against networks or convey an advantage to them, have gotten us into a deep hole. Can we climb out? Yes, if we are willing to embrace networks, and if we begin waging a netwar of our own, guided by new emerging principles. One of these principles is that when fighting a network, it is crucial not to attack too soon, because the hardest task lies in knowing how many bodies are in the network and where they are. If old-style thinking prevails, as it has so often recently, the more that is destroyed, the less will be known about the remainder of the network. Patience is essential in gaining the intelligence needed for waging a netwar campaign. It is necessary to wait

and watch long enough so as to be able to strike with heavy effect. Patience is perhaps the most difficult virtue for us to cultivate. Still, it is the most necessary, because, as Donald Rumsfeld noted in a speech to the Council on Foreign Relations during his last year as secretary of defense, finding the networks is the most difficult task and the one for which we are most poorly prepared. He put it this way: "If you think of the task that the military has, it's to find the enemy, it's to fix the enemy in time that you can do something about it, and finish. We have overwhelming ability to finish. We are light on the ability to find and fix." This "lightness" is caused by hierarchical "heaviness" in our fifteen separate intelligence agencies, which need to be more highly networked.

Two other emerging principles center on the need to distribute one's forces in smaller and more numerous detachments, and to decentralize decision-making in order to empower them. In Iraq the shift in early 2007 away from a few super-sized forward operating bases to a dispersed network of small outposts—more than fifty were established in Baghdad alone—was a sign of recognition of the utter futility of trying to apply "overwhelming force." Further, in May 2007 authority was granted down to the level of lieutenant colonel to negotiate local deals with insurgent and tribal leaders, making it easier to turn them against al Qaeda and greatly increasing the counter-insurgent network's capacities. But this shift came several years too late, for the campaign in Iraq was by then suffering from many other problems, not least the insurgents' great advantage in influence operations—over the Iraqi people, world observers and average Americans, and most of the political elites that govern us.

For an example of the more timely practice of netwar techniques, one can point to the initial success of the campaign in Afghanistan in the waning months of 2001, when a small network of fewer than two hundred U.S. special forces soldiers worked closely with indigenous insurgents opposed to the Tal-

iban and achieved much at low cost. Even though the fighting has continued in Afghanistan, the societal situation is far better there than in Iraq, and the cost of fighting the Taliban and al Qaeda cadres operating from their safe haven inside Pakistan remains but a fraction of the blood and treasure expended so fruitlessly in Iraq. Just as important, the context of this conflict remains favorable, as the continued American intervention is widely accepted, even to the point of having large contingents of NATO forces still deeply involved in counterinsurgent operations. In all these respects, the Afghan campaign reflects a far more positive example of our practice of netwar than does Iraq. The puzzle, of course, is why shifting to more of an Afghan model was resisted for so long as the situation unraveled in Iraq.

As heartening as the lessons from Afghanistan may be—and the signs of our finally appreciating the network dimension in Iraq too—it remains crucial to recognize that our opponents do not think solely in terms of waging war in a few countries. In a very real sense, networks know no territorial boundaries. Al Qaeda operates in sixty countries and in recent years has been involved in mounting or fomenting terrorist attacks across a swath of the world ranging from Morocco to Mindanao. Their level of activity has continued to grow. If terror networks are allowed to stay on their feet long enough they will obtain nuclear or biological weapons, making a mockery of our retaliatory threats: a global network has no "homeland" that can be held hostage for its good behavior. In short, there is no "mutual assured destruction" when a nation comes up against a nuclear-armed network. Further, networks will have many alternatives to the use of missiles as delivery systems, implying that continued investment in ballistic missile defenses is misplaced.

For all these reasons we should feel right now an exceptional sense of urgency about the need to defeat terrorist networks. This contradicts the notion of pursuing a "long war" against them; time is not on the side of nations in the struggle

against networks. Thankfully there are some signs that thoughtful analysts have “cracked the code” of netwar, and that their views are increasingly being heard in the right places. For example, the counterterrorist expert John Robb, in his *Brave New War*, eloquently captures the essence of the kind of conflict waged by widely dispersed but networked cells of “global guerrillas” that is nonlinear, aimed at “systems disruption,” and employs “swarm tactics.” Robb goes beyond merely sounding the alarm; he offers a vision of how we might prevail against these enemies by learning from and emulating their most effective organizational and doctrinal innovations. His call for a quality of “dynamic, decentralized resilience” is highly consistent with the netwar paradigm.

Another important voice is that of former Senator Gary Hart. In *The Shield and the Cloak* he addresses both the issue of reshaping the military (our “shield”) along nimbler, more networked lines, and argues for creating a network of allies (a “cloak”) that will routinely share sensitive information in timely, targeted ways. Marine Col. Thomas X. Hammes rounds out this trio. In *The Sling and the Stone* he makes the crucial linkage between netwar and the more popularly accepted notion among military officers and policymakers that we are today experiencing an era of “fourth-generation warfare” (4GW). For Hammes, the two concepts are basically the same. What makes 4GW distinct, he argues, is its reliance upon the network form of organization. As Hammes sees it, “netwar, also known as fourth-generation war, or 4GW, is the complex, long-term type of conflict that has grown out of Mao’s People’s War.” Later on he points the way to learning how to fight in this fashion: “In contrast to simply maintaining and marshaling massive assets to destroy enemy targets, 4GW, or netwar, requires the governments to focus the intellectual capital of our people.” So far, the U.S. military’s senior leaders have been slow to heed this message, but it has begun to resonate with younger officers.

Robb, Hart, and Hammes have improved awareness of the challenges in a time of war against networks. And in this awareness lies our greatest source of hope for progress and greater military effectiveness. But I am haunted by Hammes’s urging that human capital lies at the heart of our ability to wage netwar. It seems that we might get everything else right—organization and doctrine, technology and strategy—and still lose if our warriors and strategists lack the suppleness of mind needed for this new kind of conflict. This puts considerable weight on the social context of the U.S. military today. As discussed in the chapter to follow, the social arena has been the only one in which the armed forces have, with some important exceptions, embraced radical change. The irony, however, is that a number of the most salient shifts in military society over the past few decades may have produced harmful overall effects. They may impair our ability to wage netwar and thereby reduce our military’s chances of winning the war on terror.