America's Secret Weapon
By: Thomas A. Stewart
Issue: December 2001
WebFile | Print Article | Email This Article

To win the war against terrorism, we have to think like a street gang, swarm like a soccer team, and communicate like Wal-Mart. The latest thinking from the military’s greatest minds: It takes a network to beat a network.

The United States is at war with a foe that is, as the cliche has it, "a shadowy terrorist network," a multinational private army whose nodes and lines of communication reach invisibly and murderously across national borders. It's centipedal, multiheaded, hard to find, difficult to kill. Don't be fooled by familiar-seeming before-and-after images of bomb damage or shots of jet fighters streaking off the decks of aircraft carriers: This is a new kind of war -- netwar. "Netwar requires a whole new set of strategies and tactics," says John Arquilla, a consultant at the Rand Institute and a professor at the Naval Postgraduate School in Monterey, Calif. You could have seen it coming, and Arquilla, who with his Rand colleague David Ronfeldt coined the term "netwar," is among those who did. So is a forward-thinking group in the U.S. military, which has planned for what it calls "network-centric warfare." Businesspeople have for years studied military strategy and spouted military metaphors. Now the armed forces are looking at businesses like Wal-Mart and Deutsche Morgan Grenfell and boning up on economists like Brian Arthur and Kenneth Arrow -- and discovering some of netwar's most potent weapons in avant-garde theories of management and organization that were once the realm of captains of industry, not armies.

Can cutting-edge management theories improve our approach to national defense and terrorism?
Listen to the experts at "America's Secret Weapon."
A Business 2.0 Live!
panel discussion

Netwar has been molded by trends that have been reshaping big global institutions for years. One is the growing influence of "non-state actors" -- corporations, activist groups, and other nongovernmental organizations and networks. Examples are everywhere. Supranational organizations like the European Union and NAFTA perform formerly sovereign tasks. Private companies take on political responsibilities: Royal Dutch Shell has a policy on human rights. Activism and protest have globalized. A second trend is the flattening of hierarchies, both social and managerial, and their replacement with more fluid and horizontal organizational forms. Layers of middle management have been scraped away; project teams, alliances with other organizations, and outsourcing proliferate. A third factor is the explosive growth of computer and telecommunications networking. When the senior George Bush led America into Iraq a decade ago, the Internet sported a mere 500,000 host computers, mobile phones were just starting to go digital, and only psychics read Palms.
Like intersecting roads, these trends feed each other. For example, the Net helped enable nongovernmental anti-globalization activists around the world to converge on Genoa and Seattle with no formal organization managing the process. When these trends take on a military mien, the result is this: The world's most virulent aggressors are not armies whose order of battle is a tidy ziggurat of corps, divisions, and brigades, but amorphous networks of terror and crime -- groups like Osama bin Laden's al Qaeda and its affiliates, the Irish Republican Army, and Colombian narco-trafficking cartels. "Warfare is irregularizing," Arquilla says, and it's driving regular armies nuts.

No military on earth can go toe-to-toe with the U.S. armed forces. But no hierarchy on earth can keep up with a well-functioning network. "One is a football team, the other a soccer team," says Richard E. Hayes, president of Evidence Based Research, a company that advises the military on issues like command and control and information warfare. If the soccer players have enough destructive power -- and the attacks of Sept. 11 proved that they do -- they can swarm downfield, score, and be gone before the defense even buckles its chin straps.

There have always been irregular forces -- guerrillas, mobsters, revolutionaries. Mostly, however, they have been local and limited in firepower. In many cases -- Mafia and Bolshevik cadres, for example -- they have been rigidly hierarchal, with inviolable commands flowing down from the top. Netwar is different and scarier. Al Qaeda and its cousins are designed to exploit all the advantages of networking -- robustness, speed, flexibility -- that business has discovered. Communication is multidirectional. Command is shared. People are multiskilled. Trust is high.

A networked force can, up to a point, "offset a disadvantage in numbers, technology, or position," according to U.S. Navy Vice Adm. Arthur K. Cebrowski, former head of the Naval War College in Newport, R.I. They are hard to target because they have few formal procedures to disrupt and little physical infrastructure to destroy. They are hard to infiltrate because they are held together by close personal ties and intensely shared values. When they need expensive equipment, such as Boeing 767 airliners, they borrow from someone else. "Terrorists don't need much coordination," says David Alberts, director of research and strategic planning for what the Pentagon calls C3I (command, control, communications, and intelligence). "They are following a self-synchronizing approach" -- what business calls "self-managing teams." These are superb, malevolent examples of what Information Age organizations can be.

So how do you kill them?

Within days of the assaults on New York and Washington, a group of academics and consultants began e-mailing each other about America's newly infamous adversary. Anthropologists, mathematicians, and sociologists, they are experts in the little-known field of social and organizational network analysis. They study groups the same way engineers do computer and phone nets. Where are the nodes? How are they linked? Are the links many-to-many, so that each node (i.e., each person or place) connects directly with many others? Or are there central nodes, like switches, through which communication must pass? Is there a lot of redundancy in the network -- i.e., if a node is destroyed or a link is cut, are there alternative paths?

Bombnet, the group calls itself. Its most central node is Barry Wellman, who founded the International Network for Social Network Analysis in 1976. Since the attacks, the Bombnet friends have trained the tools of their trade on the al Qaeda network, trying, in the words of consultant and Bombnet participant Valdis Krebs, "to figure out what this thing looks like."

It's not an academic exercise. The Bombnet participants have counterparts -- including friends, former colleagues, and students -- inside all the intelligence agencies. They are using social network analysis to chart al Qaeda's structure and find potential vulnerabilities. Krebs, for example, analyzed the "centrality" and "connectedness" -- two important attributes of a network's design -- of the group directly associated
How important are information technology and network theory in America's new battle against terror? Tell us what you think.

Other Bombnet analysts have focused on al Qaeda's social structure. Bonnie E. Erickson of the University of Toronto is an expert on networks-at-risk, such as prisoners of war and members of outlaw societies like the Ku Klux Klan. What has come out about al Qaeda confirms her research that people in such situations rely on previously trusted relationships -- family members, old army buddies. The intensity of those ties makes it difficult to use standard tactics -- sowing distrust, for instance, by means of disinformation -- against the veterans in al Qaeda's core. "Social capital has to be very high for people to be willing to commit suicide," says Wayne Baker, a network expert at the University of Michigan Business School. "But you might not have the same levels of trust, collaboration, and reciprocity across units as you have within units." Where al Qaeda has seams, it may have weaknesses.

"That's the kind of thing this war needs," says Claudia Kennedy, the three-star Army general who was deputy chief of staff for intelligence until her retirement late last year. Analyzing networks requires maximum information -- phone and bank records, police, FBI, and other intelligence files -- on suspected terrorists and their associates. "You have to get everyone to agree to put in their data," Kennedy says. And if anyone balks, well, "you don't always have to ask for permission," she says.

Through such work, the topology of al Qaeda is slowly coming into focus -- and it's not a pretty picture for the United States. All networks have to manage a trade-off between security and robustness; lots of redundant links make a network hard to disconnect but easier to penetrate. Al Qaeda seems to do a pretty good job of getting the best of both worlds. For instance, its use of public networks, such as the Net for communications and an ancient money-transfer system called hawala for moving cash, is highly effective and protects anonymity extremely well. Al Qaeda's most important nodes -- bin Laden himself, for example -- aren't put at risk by having direct contact with operatives who are more exposed or of less certain loyalty. Peter Schwartz, co-founder of Global Business Network and an adviser to people involved in the war effort, says al Qaeda appears to be what network mavens call a SPIN: a segmented, polycentric, ideologically integrated network. Its semiautonomous pieces don't depend on each other for survival, nor does a SPIN rely on just one leader -- indeed, taking a leader out might energize the network, whose most important asset is its ideological fervor.

A SPIN is "the hardest to see or to dismantle," Schwartz says. "You need to attack it with many, many components going simultaneously at many, many points."

It takes a network to fight a network, John Arquilla believes. A group like al Qaeda doesn't put 20,000 troops in the field where they can be bombed, enfiladed, or flanked. Most of the time, it's dispersed and hidden in caves, literally or metaphorically. It's almost impossible to do wholesale damage to it, because the whole is never engaged. You nickel-and-dime it to death, over a long period of time.

A charismatic speaker who segues effortlessly from tactics in the Battle of Salamis in 480 B.C. to contemporary Russia's war on Chechnya, Arquilla teaches his students at the Naval Postgraduate School that enemies like this can be fought only with small, mobile forces using the best intelligence and arrayed
in networks similar to the ones they fight against. The intelligence must go far beyond traditional
"humint" (human intelligence) from spies in trench coats, and "sigint" (signals intelligence) from satellite
photos and intercepted radio and phone transmissions. "The networks out there -- criminal or terror --
have migrated to the Internet and World Wide Web," Arquilla says. "It gives them real-time
communications out of the realm of most of our surveillance assets." There are, of course, people who
know all the Net's back alleys. "World-class hackers ought to be treated a little like German rocket
scientists at the end of World War II," Arquilla says. Equally crucial are operations that scarf up and mine
the vast amount of "open-source" data -- phone and bank records, visa and immigration data, licenses for
transporting hazardous materials or using anti-eavesdropping equipment or flying planes -- and combine
it with clandestine intelligence.

When it comes to actual combat, netwars will be fought at distances of 3 feet, not 30,000. None of the
conventional tactics of Desert Storm could have nailed Mohamed Atta and his cronies. The forces we put
in the field ought to be small, nimble, and "packetized," Arquilla argues. "We need a military
reorganization designed to optimize the use of this good intelligence right down to the platoon level. It's
gEEKs at war."

Netwar, Arquilla says, demands examining an enemy in five different dimensions: technological, social,
narrative, organizational, and doctrinal. Technology is partly, but by no means entirely, a matter of
Tomahawks vs. truck bombs. Al Qaeda and other terror networks rely on a lot of freelance technical
expertise. For example, we know to our sorrow that al Qaeda had to go outside the organization to train
its operatives to fly airplanes. As Business 2.0 went to press, it was unclear whether recent anthrax
attacks are al Qaeda's work, but whoever is behind the scheme needed more than a chemistry set to pull
it off. By taking out or compromising technical experts like document forgers and money launderers -- or
anthrax cooks -- authorities can force a network to make itself vulnerable, says Dutch criminologist Peter
Klerks, an expert on drug-smuggling networks. Just chasing bad guys doesn't work. "The net effect is
almost negligible," he says. What works is targeting their processes and technology; if you shut down one
supplier, the bad guys have to find a new one. That disrupts their operations and creates the potential for
security leaks.

The social dimension looks at the kinds of ties -- kinship, marriage, religion -- that bind a network
together. Al Qaeda seems almost impenetrably close-knit, but its social fabric frays away from the center.
At least one suspected al Qaeda operative arrested last summer in the United Arab Emirates started
talking when authorities brought in Muslim clerics who persuaded him that al Qaeda was perverting the
faith. The FBI's hypothesis that only a few of the Sept. 11 hijackers knew that the planes were to be
turned into guided missiles also implies that trust doesn't run far in the network. There are many ways to
degraded it further. One might be described as the Whack-a-Mole approach: Grab every suspected terrorist
and associate, comb their every canceled check and telephone bill, and interrogate them to the limits of
the law. Some will talk. The more terrorists have spent a few weeks on the griddle, the more likely it is
that a network may begin mistrusting itself. "You can't undermine the religious and kinship ties," Arquilla
says, "but you can undermine the social structure and their trust in the system, and that will cramp their
style."

The narrative dimension revolves around the story the network tells about itself to maintain loyalty and
sympathy. The battle of narratives is one of the most visible elements of the war on terrorism. The United
States focuses on its story: We are attacking the Taliban, not Afghanistan; terrorists, not Muslims. Al
Qaeda fights back with tales of civilian casualties; its leader speaks in flowery Arabic of defending the
faith against Christian crusaders. Winning the clash of narratives is crucial in netwar. Americans need
forward airbases and at least grudging cooperation from military, political, and intelligence people -- and
the private sector -- in places like Syria and Pakistan. The irregulars of al Qaeda, who need sympathy and
cover, are doomed if they lose the battle of the story. "That's where the Chechens fell down terribly in
their second war" against the Russians, Arquilla says. "In the first, in 1994 to '96, they were plucky
freedom fighters. The second time around, the Chechens look like a bunch of terrorists and the Russians
portray themselves as waging a war for civilization" -- and the global sympathy that was generated by the
Chechens in the earlier campaign has diminished.

Doctrine, in military jargon, has to do with strategy and tactics. Al Qaeda, for example, seems to believe
in striking every so often against showy targets in far-flung places: the destroyer USS Cole in Yemen,
embassies in Tanzania and Kenya, the World Trade Center and Pentagon, all on different continents. "If that's their doctrine," Arquilla explains, "you can't meet it with a doctrine of overwhelming force" -- the old Powell doctrine, which worked so well against Iraq during the Gulf War. "That's just going to be trying to nail Jell-O to the wall."

**How important are information technology and network theory in America's new battle against terror?**

Tell us what you think.

Pentagon planners responsible for doctrine -- some of them, anyway -- endorse many netwar precepts. But the Pentagon has its own version, called network-centric warfare. The idea first took hold in the Navy; Vice Adm. Cebrowski was an early promulgator. For Cebrowski, network-centric warfare stands in contrast with "platform-centric warfare," in which military strategy revolves around the platform -- such as an aircraft carrier or a unit of infantry.

Network-centric war begins with an intelligence network, sometimes called a "sensor grid." This grid collates real-time information from every kind of sensor -- from satellites in space to sharp-eyed soldiers -- to create a shared image of battlefield conditions. Parallel to the sensor grid is a "shooter grid": carriers and battleships, fighters and bombers, commandos and copters. Connecting them is an "information grid" of computers and communication devices. The idea is to achieve "information superiority" and almost instantaneous responsiveness. In theory, a sensor ought to be able to spot a target and see it destroyed by whichever shooter -- regardless of branch of service -- is best positioned to take it out, the way taxi dispatchers call out fares and cabbies put dibs on them. Strategists call aircraft carriers, missiles, and bombers "peripherals" -- like printers and keyboards. "In a network, 'commander's intent' and a set of rules of engagement take the place of direct orders," says C3I's Alberts. "I'm counting on you to read the situation and respond accordingly. It's a far more robust and effective organizational method."

If earlier soldiers idealized Napoleon or Patton, network-centric warriors admire Wal-Mart, where point-of-sale scanners (part of the sensor grid) share information on a near real-time basis with suppliers (comparable to the shooter grid) and also produce data that is mined to help leaders develop new strategic or tactical plans. Wal-Mart, says the Navy's Cebrowski, is an example of "translating information superiority into competitive advantage."

**Can cutting-edge management theories improve our approach to national defense and terrorism?**

Listen to the experts at

"America's Secret Weapon."

A Business 2.0 Live! panel discussion

That's the theory, anyway. Will it work in practice? We are but weeks into a war on terror networks that could last decades, and the military is a long way from really putting netwar principles into action. Still, some of the challenges of waging real-life netwar were apparent even before the World Trade Center attacks. Arquilla, who helped Cebrowski develop the military's idea of network-centric warfare, thinks it doesn't go far enough. "You ought to think about the small and the many, not the few and the large," he says. That's hard to take for the old guard in the Pentagon, which cherishes its hulking carrier groups and other industrial age systems. Arquilla says the military's idea of total information superiority is a pipe dream. "The only phrase worse than 'information superiority' is 'infinite justice,'" he says. The temptation it poses is to devote enormous treasure and time to processing every last bit of data, while not paying enough attention to structuring and sharing information in ways that people can act on: Data, data everywhere, but not a chance to think.

More problematic, Arquilla says, are "the cultures of the different organizations that control and disseminate information in different ways." Interservice rivalries are bad enough -- and actually not as
fierce as they once were. But waging netwar requires an extraordinary sharing of information and resources among the military, intelligence agencies, the FBI, and local police forces -- not to mention their counterparts in the scores of nations where terror cells lurk. "This is a problem that falls into almost every crack we have," Alberts says. Beyond that, the reported missed opportunity, just days into the conflict, to blast a convoy in which Taliban leader and bin Laden protector Mullah Mohamed Omar was traveling because of the need to first go through a military lawyer shows that we haven't achieved the streamlined command-and-control and instantaneous action that netwar envisions. In Arquilla's battle of the narratives, the West started out ahead, given the widespread moral revulsion over the Sept. 11 attacks. But the counteroffensive -- wrapping terror's cause in Palestinian and Islamic cloaks -- did better than it ought to have, and the early U.S. response was, by Defense Secretary Donald Rumsfeld's own admission, inadequate. U.S. policymakers now seem to grasp the importance of the narrative struggle. But the United States needs to expand its efforts and take them into the Muslim heartland over television and radio and through public statements from Islamic academics, theologians, and others.

Netwar is new, and innovators in war, like innovators in business, often have first-mover advantages. It takes a while to learn how to defeat an innovative enemy. But the United States seems to have learned the overarching lesson of netwar: It is fought with every means, military and other, with no front line and little distinction between offense and defense. It requires patience -- and fury. Since al Qaeda shows itself as little as possible, the United States needs to develop the ability to swarm over it when it does appear, attacking with enormous speed and ferocity from every possible direction.

Between those moments, the United States needs to exploit its own considerable advantages. Gary Anderson at the Center for Emerging Threats and Opportunities, who helps school the Marine Corps in war games, says, "The terrorist side doesn't have the capability to conduct large, flexible operations and put on events like a campaign. They don't do sequels." The United States, by contrast, "can lean on them all the time. If we do that and take advantage of fast-moving opportunities, we can take away their flexibility."

In an odd way, al Qaeda might be too virtual, too Information Age, for its own good. It is amorphous and unstructured; chase it relentlessly, hit it hard and in the right places, and its very lightness of being becomes a fatal liability, not a strength. "In the 19th-century Indian wars, we could put infantry in the field in the wintertime and keep the pressure on year-round," Anderson says. "And that's why we will win this one -- we can keep up a tempo that they can't sustain." It could take years. But it wouldn't be the first time that an organization with a great brand name, lots of assets, and strong cash flow withstood a terrifying assault from a new kind of foe, picked up a few new tricks, and then crushed its attacker. ✦