2001

Fighting The Network War

Arquilla, John

WIRED

THE NEW RULES OF ENGAGEMENT

Fighting The Network War

Conventional military power stands little chance against a band of swarming 14th-century terrorists, according to John Arquilla and David Ronfeldt, the RAND analysts who wrote the book on "netwar." Here's their five-point plan to tear apart the terror network.

Know your enemy. It's the oldest military axiom in the world. As the United States takes action against the perpetrators of the September 11 attacks, this advice has never been more apt. The first step in defeating the type of terror invoked by Osama bin Laden's al Qaeda is figuring out how the organization operates.

Think of al Qaeda as a coalition of dispersed network nodes - linked, as PCs are, to one another and to databases of information. The network uses the Internet for real-time dissemination of instructions to wage its particular brand of asymmetrical warfare - favoring an attack on a soft civilian target like an airliner over a direct assault on US forces in the field. Battling such a foe is tantamount to taking on a hybrid peer-to-peer network, in which a central source triggers the actions that are carried out by individual nodes. The good news is that the US already knows a few things about such networks; structurally, al Qaeda is similar to Colombian and Mexican drug cartels, which also feature small, nimble, and dispersed units capable of penetrating, disrupting, eluding, and evading.

The bad news: The US military is woefully unprepared to fight a war against such an enemy. Transnational terrorists have shown it's possible to swarm together swiftly, on cue, then pulse to the attack simultaneously. Simply dropping bombs on Afghanistan will do little against this kind of a decentralized foe.

To win, this network must be isolated and ripped apart, node by node. The best hope is to redesign US intelligence systems to anticipate how this new enemy thinks. The US must build its own network - a quicker, more diverse, populous, and powerful organization that includes military and nonmilitary organizations around the world - in order to wage a full-on netwar.

The term *netwar* may evoke visions of 25th-century technologies deployed from the far reaches of space. But netwar is not techwar; it's far less sexy and more sweaty.

Al Qaeda's power comes in its organization. Beyond access to the Net, the network has little in the way of technology - almost no military tech, and its members don't even use cell phones for fear of being tracked. As a result, defeating al Qaeda has less to do with technology and more to do with military doctrine. To win a netwar, the US has to rethink some of its fundamental national security principles.

Be Smart About Intelligence

The recrafting of military systems to succeed in a protracted war on terrorism starts with intelligence. The US system of central intelligence needs to evolve into a *de*centralized, transnational network that communicates in real time. Just as the swift movement of information has redefined business - stripping guesswork out of the supply chain, for example - it can alter the outcome in a netwar. All-channel data flow reduces the need for an explicit chain of command.

It's not that the military has failed to emulate business practices; it's just been disinclined to try. Unlike businesses, intelligence agencies measure bureaucratic power by the information they control. Such an approach can be fatally flawed.

This proved true in August, when a man suspected of being a member of the Armed Islamic Group (GIA) was apprehended by US authorities on illegal immigration charges in Minnesota. He came to the FBI's attention when a wary flight instructor let them know the man wanted to use a 747 flight simulator to learn how to turn - not takeoff or land - a plane. During the September attacks, he was in his jail cell. With a bit of networking, the French, who closely follow terrorist movements in their former colony, might have informed US officials that he was an extremely dangerous GIA member - warranting vigorous interrogation. The lesson: Sharing knowledge with partners enhances its value. This must become the norm.

Another way to boost the quality and quantity of intelligence is to cultivate more of an open source model - by including nongovernmental organizations, like Amnesty International, in the network. This will make it possible to draw on the knowledge of activist groups already engaged in waging social netwars around the world. Much of the intelligence we need is openly available - it's just a matter of looking in the right places.

Adding NGOs to a sensory network will also help develop loyalty to a cause. The al Qaeda network draws its strength from the tight religious and kinship bonds among its members. To be effective, the US's counternetwork will need to have its own binding, democracy-driven value system.

Manage the Memes

To win a netwar, the US must control the battle of the story. For starters, that means the US and its allies must agree on what story they're selling. Should America's response to the terrorism be phrased in terms of a war? Or should it be addressed through a law enforcement paradigm - with increased security in the streets? In the days after the attacks, American allies may well have preferred the latter. But a surge in US nationalist sentiment made clear which way the American people wanted to go. President Bush called the terrorist attacks an "act of war" - against not only America but "the civilized world."

It was an effective rallying cry and a strong show of leadership - and Bush quickly won the support of queasy allies. But there's danger in allowing the netwar to devolve into a battle of civilizations or faiths. The attacks have intensified a broad-based clash of rhetoric between Western liberal ideas about the spread of free markets, free peoples, and open societies, and Muslim convictions about the exploitative, invasive, demeaning nature of Western incursions into the Islamic world. But the war against terror must not be seen as one of Western values against Islam.

Instead, the story should focus on what Jeremy Rifkin refers to as a time war - in this case between an emerging global civilization of the 21st century and a xenophobic religious fanaticism of the 14th century (or earlier). Osama bin Laden and his cohorts are tribal, medieval, absolutist, and messianic. The best way to expose them as such is to create a self-propagating meme - a winning idea or, in business parlance, a bit of viral marketing - that reveals them for what they truly are.

Here, the US and its allies could use some help. Ideally, such a meme would be spread by respected Islamic imams who would repudiate the notion that the Koran sanctions terrorism. This is hardly far-

fetched, as even Taliban imams have ruled that bin Laden has no authority to issue fatwas. The quicker this meme replicates - by way of the Net and other media - the more likely members of the al Qaeda network will be rejected by the majority of the Muslim world for which they purport to be fighting.

Learn to Swarm

The al Qaeda network recognizes the effectiveness of swarming. It exploits the nonlinear nature of the battle space and sees the value of attacking from multiple directions with dispersed units. The more geographically diverse the targets, the more unpredictable and effective the terrorist network. Witness al Qaeda attacks on targets in Arabia, Africa, and the US during the past five years. In September, widely dispersed operatives converged on four separate targets simultaneously. They likely had the capability to strike at even more sites, and almost certainly are holding some units in reserve.

US military doctrine, on the other hand, is based on mass-and-maneuver concepts. The Pentagon must establish a new plan based on small-unit swarming. The US should learn to strike the enemy from many directions, in different places, all at once. This will keep terrorists on the run.

To make it work, the counternetwork needs special-force maneuvers, not industrial age methods suited for fighting in Europe's Fulda Gap or in the Persian Gulf. Updated battlefield intelligence practices and internetted battlefield sensors could aid in the coordination of the attacks - allowing commandos to relay information in real time without scrubbing it through the National Ground Intelligence Center or other spy shops. This isn't about war at standoff range. It's about using information to get small strike teams in the enemy's face.

Rethink Technology

In every war the US has waged, advanced technology has generally served as a big advantage. In World War II, the first computers - used in a project code-named Magic - cracked Japanese encrypted communications and helped win the battle for the Pacific. More recently, in Kosovo, electronic warfare devices spoofed Serb radar, allowing the US to wage an 11-week air campaign while losing only one plane.

In a netwar, military technology is not such an obvious advantage. The US possesses an array of sophisticated systems, like the Global Command and Control System and the Joint Surveillance and Target Attack Radar System. Al Qaeda, on the other hand, has relatively few. But against dispersed, networked terrorists, the Pentagon's high tech spy equipment is of limited value. Satellites may be able to look down on specific buildings - or tents - but they can't reveal who's in them. Same with smart bombs, which can be guided to a target - with no guarantee that anyone will be inside. This was exactly the case with the failed US missile strike against bin Laden at an al Qaeda camp in Afghanistan three years ago.

Instead of spending roughly $30 billion a year on such technology, the US military should create a range of lower-cost, Web-based intelligence tools to take on the 60-country terror network. Al Qaeda operatives communicate over the Internet by using low tech word-substitution codes rather than sophisticated encryption. They should be tracked, perhaps with more powerful versions of a marketer's cookies. Such devices could even be planted as "taggants" at sites frequented by terrorists, or as lures to attract them to "honey pots." This would also lessen reliance on the FBI Carnivore snoop system and other initiatives that undermine civil liberties.

Attack the Core

Overcoming a widely dispersed, multihub network with no center seems nearly impossible. But al Qaeda has a center. The removal of bin Laden means that the network could crumble. And therein lies hope for the West.

In some ways, al Qaeda is to terrorism as Napster is to file-sharing. True, declawing Napster did little to put an end to the swapping of MP3 files; smaller, even more decentralized P2P networks have popped up in its place. Taking out bin Laden could splinter al Qaeda into similar networks - the Gnutellas of terror. But while Gnutella can effectively operate as a file-sharing mechanism, it wouldn't be nearly as effective as a terror network. Without bin Laden at its core, al Qaeda could turn out to be a network without a mobilization mechanism.

In the end, terrorism is much bigger than Osama bin Laden. A true win in this netwar means confronting a scourge that's bigger than even al Qaeda. It means battling anyone in the world who shares these terrorists' mind-set and modus operandi. It means, eventually, taking on every node in the entire terrorist network.

RAND analysts John Arquilla (arquilla@rand.org) *and David Ronfeldt* (ronfeldt@rand.org) *cowrote* Networks and Netwars: The Future of Terror, Crime, and Militancy *(RAND, 2001).*

Warning: Uninitialized variable or array index or property (slist) in **functions.phtml** on line **910**

Warning: Variable passed to each() is not an array or object in **functions.phtml** on line **855**