The Underside of Netwar

JOHN ARQUILLA AND DAVID RONFELDT

THE fight for the future makes daily headlines. As in the bombing in Bali, its battles are not between the armies of leading states, nor are its weapons the large, expensive tanks, planes and fleets of regular armed forces. Rather, the combatants come from dark, violent terrorist networks like Osama bin Laden's al-Qaeda, drug cartels like those in Colombia and Mexico, and militant anarchists like the Black Bloc that ran amok during the Battle of Seattle. There is also a bright side to this fight, one that often benefits state interests, for it features networked civil-society activists struggling for democracy, economic freedom and human rights around the world. Both these dark- and bright-side protagonists are heralds of a new mode of conflict favoured by networked nonstate actors: netwar.

From the activists' Battle of Seattle to the terrorists' attack on Bali, these networks are proving very hard to deal with; indeed, some are winning. What all have in common is that they operate in small, dispersed units that can deploy nimbly—anywhere, anytime. All feature network forms of organization, doctrine, strategy, and technology attuned to the information age. They know how to swarm and disperse, penetrate and disrupt, connect and disconnect, as well as elude and evade. The tactics they use range from battles of ideas to acts of sabotage—and 'cybotage,' as some tactics involve the Internet.

So far, across this new landscape of conflict, the edge has gone to the networks. Hierarchy-oriented states must learn to transform themselves along networked lines, or they will face the increasingly daunting prospect of struggling against an uncontrollable, rising tide of civil and uncivil society networks enabled, and impelled forward, by the information revolution.

In September 2001, the 'age of networks,' which seemed to be dawning with such democratic promise, yielded an astounding 'attack on America,' signalling the onset of an archetypal netwar. Transnational terrorists, organized in widely dispersed, networked nodes, showed how it is possible to swarm together swiftly, on cue, then pulse to the attack simultaneously. They relied on the Internet, sometimes communicating via encrypted messages. But what really distinguished them—in particular Osama bin Laden's al-Qaeda ('the Base')—is the highly networked organizational form that they built, based on unusually tight social, religious, and kinship ties. US Secretary of State Colin Powell put it aptly: To win against terror, this network must be 'ripped apart.'

Transnational terrorists, organized in widely dispersed, networked nodes, showed how it is possible to swarm together swiftly, on cue, then pulse to the attack simultaneously

The league of hierarchical nation-states that has formed to fight this terrorism will have to build its own set of nimble networks. In the military realm, this means relying more on networks of agile special forces—of all allied nations—than on the missiles, tanks, bombers and aircraft carriers that, until now, have been the *sine qua non* of national power. Just as the terrorists' power derives more from their organizational form than from technology, so too must the military power to defeat them become more reliant upon organization and doctrine than upon advanced technical systems.

The intelligence world faces an equally urgent need for institutional redesign—away from notions of 'central' intelligence, toward the construction of transnational intelligence networks able to share what they have on a real-time basis. Swift movement of important information has played a major role in the success of networked businesses over the past decade. Now it is time for networking to redefine the approach to intelligence—the quality and timeliness of which will determine whether bin Laden's or any other terror network can indeed be 'ripped apart.'

Improved international networking among military and intelligence organizations can help win this war against terror. But this will not suffice in the long run. A balanced strategy for countering terrorist networks should also ▶

involve a much improved capacity to work with networks of civil-society NGOs around the world, many of which are engaged in social netwars. Nurturing this emergent global civil society offers the best chance for state and nonstate actors to create over time an 'integral security system' that could free all of us, ultimately, from terror. For in a truly networked world, joined as much by common values as by common wires, there will simply be little space left for such a scourge.

Above all, America's strategy (not to mention Australia's) should avoid getting mired in notions of a 'clash of civilizations.' The war against terror is not a war of Western values against Islam. Rather, it is what Jeremy Rifkin has called 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 so tribal, medieval, absolutist, and messianic that they resemble some of the more frightening figures out of Norman Cohn's *The Pursuit of the Millenium*. The more clearly these terrorists are revealed as such, the sooner they will be rejected by the vast majority of the Muslim world for which they purport to be fighting.

Yet, as much as Osama bin Laden seems a medieval rather than a modern character, the network that he has masterminded is quite sophisticated; and the continuing fight against it will remain tough and protracted. At this point, it is advisable to analyse how this struggle against terrorism is playing out across five dimensions: the organizational, narrative, doctrinal, technological, and social.

First, at the organizational level, this is a major confrontation between hierarchical/state and networked/nonstate actors. For the United States and its friends and allies, one challenge will be to learn to network better with each other. Some of this is already going on, in terms of intelligence sharing, but much more must be done to build a globally operational counter-terror network. A particular challenge for the cumbersome American bureaucracy will be to encourage deep, all-channel networking among the military, law enforcement, and intelligence elements.

In fighting al-Qaeda, the organizational challenge lies partly in determining whether this network has a single hub designed around bin Laden. If this were the case, then his death or capture would signal its defeat. However, the more a terrorist network takes the form of a multi-hub 'spider's web' design, with multiple centres and peripheries, the more redundant and resilient it will be—and the harder to defeat. In a somewhat analogous vein, note that despite the dismantling of the powerful Medellin and Cali cartels in the 1990s, a plethora of small drug smuggling organizations, many of them networked, continues to flourish in Colombia. The risk is that small, more nimble networks spring up as successors to a defeated large network.

Nurturing this emergent global civil society offers the best chance for state and nonstate actors to create over time an 'integral security system' that could free all of us from terror

Second, at the narrative level, a broad-based 'battle of the story' is being waged 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. Righteous indignation exists on both sides. The United States insists that terrorist attacks are 'acts of war' against not only America but also against 'the civilized world,' and American public opinion was quickly galvanized by the revival of the Pearl Harbor metaphor. Against this, the perpetrators exalt their own 'holy war' imagery, however, they have trouble exploiting it beyond the Islamic world. But while the United States may have the edge so far in the 'battle of the story,' in much of the world, it will have to think deeply about how to keep that edge as US forces are sent into action in or near any Middle Eastern or Muslim countries.

Third, in terms of doctrine, the al-Qaeda network has displayed a grasp of the nonlinear nature of the battlespace, and of the value of attack from multiple directions by dispersed small units. If this is indeed a war being orchestrated by al-Qaeda, its first campaign was no doubt the bombing of the Khobar Towers in Saudi Arabia in 1996, followed by a sharp shift to Africa with the embassy bombings of 1998. In between, and since, a number of other skirmishes have occurred in far-flung locales, with some smaller attacks succeeding, and others apparently being prevented by good intelligence. Thus, bin Laden and his cohorts appear to have developed a swarm-like doctrine that features a campaign of episodic, pulsing attacks at locations sprawled across global time and space where particular network nodes have

advantages for seizing the initiative, stealthily.

Against this doctrine, the United States has had seemingly little new to pose, as yet. Some staid defensive efforts to improve 'force protection' have been pursued, and the offensive part of US doctrine still appears to be based on ageing notions of strategic bombardment. Needless to say, if our ideas about netwar and the future of conflict are on the mark, the former is not likely to be a winning approach; a whole new doctrine based on small-unit swarming concepts should be developed. Indeed, the striking success of the relative handful of coalition special forces in Afghanistan during the fall of 2001 should be seen as 'a war to change all wars.'

It also seems clear that the notion of counterleadership targeting will continue to be featured—this was tried against Moammar Qaddafi in 1986, Saddam Hussein in 1991, Mohamed Aidid in 1993, and against bin Laden himself in 1998 and again at Tora Bora in 2001. Every one of these attempts has failed, and now we know that bin Laden is still out there. But this sorry record hasn't kept the United States from resorting to the strategy yet again, as this seems to form a part of its doctrinal paradigm. Taking out top leadership is not necessarily a bad idea, but network designs may be so complex and capable of reconfiguration that it makes equal sense to target brokers, gatekeepers, and other operators at strategic middle and peripheral positions.

Fourth, at the technological level, the United States possesses a vast array of very sophisticated systems, while al-Qaeda has relatively few—and has great and increasing reluctance to use advanced telecommunications because of the risks of detection and tracking. But this category cannot be analyzed quite so simply. The United States, for example, has extensive technical means for gathering intelligence and targeting information—but perhaps only a small portion of these means have much utility against dispersed, networked terrorists. Orbital assets—now the linchpins of American intelligence—may ultimately prove of little use against bin Laden. At the same time, al-Qaeda has access to commercial off-the-shelf technologies that have proven a boon to their operations.

Simply put, the allied coalition must start to build its own networks (and hybrids of hierarchies and networks) and learn to swarm the enemy, in order to keep terrorists on the run or pinned down

Last, at the social level, this network features tight religious and kinship bonds among the terrorists, who share a tribal, clannish view of 'us' versus 'them.' Al-Qaeda's edge in this dimension ties into its narrative level, with Islam being the pivot between the story of 'holy war' against 'infidels' and the network's ability to recruit and deploy hate-filled, death-bound strike forces who evince a singleness of mind and purpose. Against this, the allied coalition faces a profound defensive challenge at the social level: How will people, despite the arousal of outrage at terrorism, react to the potential need for their societies to become less open in order to become more secure?

In summary, a netwar perspective on the various dimensions of the struggle with al-Qaeda renders some interesting insights into both the context and conduct of this first major conflict of the new millennium. Bin Laden and al-Qaeda held initial advantages at the social and doctrinal levels, and in the organizational domain as well. The United States and its allies held only marginal advantages at the narrative and technological levels. In terms of strategy, there appears to have been less room for al-Qaeda to improve. However, its underpinnings might be further enhanced—and vulnerability removed—if it moves ever further away from being a hub network revolving around bin Laden.

For the United States and its allies, there is much room for improvement—most of all at the organizational and doctrinal levels. Simply put, the allied coalition must start to build its own networks (and hybrids of hierarchies and networks) and learn to swarm the enemy, in order to keep terrorists on the run or pinned down until they can be killed or captured. The United States and its allies must also seize the initiative—including by applying pressure on any states that harbour or sponsor terrorists. To be sure, the edge at the narrative level in the world at large must be maintained.

The crucial work now for coalition strategists is to develop an innovative concept of operations and build the right kinds of networks to carry off a swarming campaign against networked terrorists. For, at its heart, netwar is more about organization and doctrine than it is about technology.

John Arquilla and David Ronfeldt are RAND analysts. Their latest book is Networks and Netwars *(RAND, 2001)*

IPA