2000-04

Information-Age Terrorism

Arquilla, John

Current History, April 2000
http://hdl.handle.net/10945/36377

"While some terrorists will eventually have the technological skills or opportunities to engage in extremely damaging cyberterrorism, this is not the only dangerous implication of the information revolution. More seriously, this revolution is enabling new forms of organization and new doctrines that will affect the spectrum of conflict, including terrorism."

Information-Age Terrorism

JOHN ARQUILLA, DAVID RONFELDT, AND MICHELE ZANINI

Today, an instance or prospect of "cyberterrorism" makes the news almost every week. The idea of terrorists surreptitiously hacking into a government, military, commercial, or socially critical computer system to introduce a virus or worm, turn off a crucial public service, steal or alter sensitive information, deface or swamp a web site, route bogus messages, or plant a Trojan horse for future activation alarms security personnel, spellbinds the media, and genuinely worries policymakers. Although fears that the Y2K problem could provide opportunities to some terrorists have not been realized, other developments since January—such as the denial-of-service attacks against a few on-line commercial enterprises based in the United States (Yahoo! and eBay, among others), and speculation that software developers secretly associated with Aum Shinrikyo cult may have placed Trojan horses in sensitive computer systems in Japan—continue to enliven the threat of cyberterrorism.

Globally Wired: Politics in Cyberspace
Fourth in a Series

Cyberterrorism thus looks like the darkest downside of the information revolution. It is dramatic and it makes for quite a story. It is also a potentially serious threat, although most instances have had more in common with graffiti vandalism than with bomb-tossing anarchism.

JOHN ARQUILLA *is a professor of defense studies at the Naval Postgraduate School and a RAND consultant.* DAVID RONFELDT *is a senior social scientist at RAND.* MICHELE ZANINI *is a doctoral fellow at the RAND Graduate School. This article draws on the authors' "Networks, Netwar, and Information-Age Terrorism," in Zalmay M. Khalilzad and John P. White, eds.,* Strategic Appraisal: The Changing Role of Information in Warfare *(Santa Monica, Calif.: RAND, 1999).*

But a focus on the drama of cyberterrorism risks overlooking the broader phenomenon of which it is only a part: the rise of what we call "netwar." Cyberterrorism and terrorist netwar are not the same thing (although at times some media conflate the two). While some terrorists will eventually have the technological skills or opportunities to engage in extremely damaging cyberterrorism, this is not the only dangerous implication of the information revolution. More seriously, this revolution is enabling new forms of organization and new doctrines that will affect the spectrum of conflict, including terrorism. Indeed, signs are already apparent that terrorist groups in the future will try to gain strength and extend their reach by organizing into transnational networks and developing swarming strategies and tactics for destroying targets, entirely apart from whether they can hack into a target's computer system.

REDEFINING CONFLICT

The information revolution is altering the nature of conflict. First, the information revolution is favoring and strengthening network forms of organization, often giving them an advantage over hierarchical forms. The rise of networks means that power is migrating to nonstate actors, who are able to organize into sprawling multi-organizational networks more readily than can traditional, hierarchical, state actors. Nonstate-actor networks are thought to be more flexible and responsive than government hierarchies in reacting to outside developments, and to be better than hierarchies at using information to improve decision making.

Second, as the information revolution deepens, conflicts will increasingly depend on information and communications. More than ever, conflicts will revolve around "knowledge" and the use of "soft

power." Adversaries will emphasize "information operations" and "perception management"—that is, media-oriented measures that aim to attract rather than coerce, and that affect how secure a society, a military, or other actor feels about its knowledge of itself and its adversaries. Psychological disruption may become as important a goal as physical destruction. Thus, major transformations are inevitable in the nature of adversaries, in the type of threats they may pose, and in how conflicts can be waged. Information-age threats are likely to be more diffused, dispersed, multidimensional, and ambiguous than traditional threats.

In light of these changes, we see netwar emerging as a mode of conflict and crime at societal levels, involving measures short of traditional war in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups that communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise, stable, and bureaucratized central command.

The term "netwar" is meant to call attention to the prospect that network-based conflict and crime will become major phenomena in the decades ahead. Various actors across the spectrum of conflict and crime are already evolving in this direction. To give a few examples, netwar is about the Middle East's Hamas more than the Palestine Liberation Organization (PLO), Mexico's Zapatistas more than Cuba's Fidelistas, and the American Christian Patriot movement more than the Ku Klux Klan.

Even in information-age conflicts, real-world events are generally more important than what happens in the virtual world of cyberspace.

This spectrum includes familiar adversaries who are modifying their structures and strategies to take advantage of networked designs, such as transnational terrorist groups, black-market proliferators of weapons of mass destruction, transnational crime syndicates, fundamentalist and ethnonationalist movements, intellectual property and high-sea pirates, and smugglers of migrants or black-market goods. Some urban gangs, back-country militias, and militant single-issue groups in the United States are also developing netwar-like attributes. In addition, a new generation of radicals and activists are just beginning to create information-age ideologies, in which identities and loyalties may shift from the nation-state to the transnational level of global civil society. New kinds of actors, such as anarchistic and nihilistic leagues of computer-hacking "cyboteurs," may also partake of netwar.

Many—if not most—netwar actors will be nonstate. Some may be agents of a state, but others may try to turn states into *their* agents. Moreover, a netwar actor may be both subnational and transnational in scope. Odd hybrids and symbioses are likely. Furthermore, some actors (for example, violent terrorist and criminal organizations) may threaten United States and other nations' interests, but other netwar actors (for example, peaceful social activists) may not. Some may aim at destruction, others at disruption.

The full spectrum of netwar proponents may thus seem broad at first. But an underlying pattern cuts across all variations: the use of network forms of organization, doctrine, strategy, and technology attuned to the information age.

NETWAR CONFIGURATIONS

The idea of an organizational structure qualitatively different from traditional hierarchical designs attracted the attention of management theorists as early as the 1960s. Today, in the business world, virtual or networked organizations are being heralded as effective alternatives to bureaucracies because of their inherent flexibility, adaptiveness, and ability to capitalize on the talents of all their members.

What has long been emerging in the business world is now becoming apparent in the organizational structures of netwar actors. In an archetypal netwar, the protagonists are likely to amount to a set of diverse, dispersed "nodes" that share a set of ideas and interests and that are arrayed to act in a fully internetted "all-channel" manner.

Networks come in three basic configurations: 1) The chain network, as in a smuggling chain where people, goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes; 2) the star, hub, or wheel network, as in a franchise or a cartel structure where a set of actors is tied to a central node or actor, and must go through that node to communicate and coordinate; and 3) the all-channel network, as in a collaborative network of militant small groups where every group is connected to the other.

We expect to observe substantial differences (and many hierarchy-network hybrids) in the spe-

cific design choices of netwar organizations. Often the organizational structure will incorporate various elements of the three different network configurations. For example, a netwar actor may have an all-channel council at its core, but use stars and chains for tactical operations. Actual network designs depend on contingent factors, such as personalities, organizational history, operational requirements, and other influences such as state sponsorship and ideology.[1]

The common feature of netwar design variants is their lack of emphasis on formal, stable, and vertical command and control. Networks largely operate by consensus, which is created through dialogue and mutual trust as opposed to bureaucratic fiat. In turn, mutual trust is fostered by a strong strategic sense of shared goals and missions, along with the belief that these goals can be attained through tactical autonomy.

Of the three network types, the all-channel has been the most difficult to organize and sustain historically, partly because it requires dense horizontal communication and coordination. But it has the most potential for collaborative undertakings, and is the type that seems to be gaining strength from the information revolution. Pictorially, an all-channel netwar actor resembles a geodesic "buckyball" (named for geodesic dome inventor Buckminster Fuller); it does not resemble a pyramid. Ideally, there is no single, central leadership, command, or headquarters—no precise heart or head that can be targeted. The network as a whole (but not necessarily each node) has little to no hierarchy, and it may have multiple leaders. Decision making and operations are decentralized, allowing for local initiative and autonomy. Thus the design may sometimes appear acephalous (headless), and at other times polycephalous (hydra-headed).

Since bureaucratic command and control is inherently impractical in an all-channel network, the capacity of this design for effective long-term performance may depend on the presence of shared principles, interests, and goals—at best, an overarching doctrine or ideology—that spans all nodes and to which the members wholeheartedly subscribe. Such a set of principles, shaped through mutual consultation and consensus-building, can enable them to be "all of one mind," although they are dispersed and devoted to different tasks. It can provide a central ideational, strategic, and operational coherence that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that the members need not resort to a hierarchy—"they know what they have to do."[2]

The capacity for netwar is afforded by the latest information and communications technologies—cellular telephones, fax machines, e-mail, World Wide Web sites, and computer conferencing. But caveats are in order. First, the new technologies, however enabling for organizational networking, may not be the only crucial technologies for a netwar actor. Traditional means of communications, such as human couriers, and mixes of old and new systems, may suffice. Second, netwar is not simply a function of the Internet; it does not take place only in cyberspace. Netwar is not Internet war. Some key battles may occur there, but a war's overall conduct and outcome will normally depend mostly on what happens in the real world. Even in information-age conflicts, real-world events are generally more important than what happens in the virtual world of cyberspace.

Third, our concept of networks does not imply that all nodes must be in constant communication, which may not make sense for a secretive, conspiratorial actor. But when communication is needed, the network's members must be able promptly to disseminate information as broadly as desired within the network and to outside audiences. Last, having access to the latest information technology in and of itself does not make a network—such design is made possible by the organization's doctrine, structure, and strategy.

THE STRATEGIC IMPLICATIONS

A network form of organization gives distinct advantages, both offensive and defensive, to its operatives. On the offense, networks are known for being adaptable, flexible, and versatile. This may be particularly the case where a set of actors can engage in swarming. Little analytic attention has been given to swarming, yet it may be a key mode of conflict in the information age. The cutting edge for this possibility is found among netwar protagonists.

Swarming occurs when the dispersed nodes of a network of forces converge on a target from multiple directions. The overall aim is the sustainable pulsing of force or fire. Once in motion,

---

[1]Moreover, terrorist network nodes can be composed of a diverse set of actors—an individual, a group, an institution, or even a state sponsor. The nodes in a network need not be identical in size, influence, or function.

[2] The quotation is from a doctrinal statement by Louis Beam about "leaderless resistance," which has strongly influenced right-wing white-power groups in the United States. See Louis Beam, *The Seditionist*, issue 12, February 1992.

swarm networks must be able to coalesce rapidly and stealthily on a target, then dissever and redisperse, immediately ready to recombine for a new pulse. In other words, information-age attacks may come in "swarms" rather than the more traditional "waves."

In terms of defensive potential, well-constructed networks tend to be redundant and diverse, making them robust and resilient in the face of adversity. Where they have a capacity for interoperability and shun centralized command and control, network designs can be difficult to crack and defeat as a whole. In particular, they may defy counterleadership targeting—attackers can find and confront only portions of the network. Moreover, the deniability built into a network may allow it to simply absorb a number of attacks on distributed nodes, leading the attacker to believe the network has been harmed when, in fact, it remains viable, and is seeking new opportunities for tactical surprise.

The difficulties of dealing with netwar actors deepen when the lines between offense and defense are blurred, or blended. When blurring is the case, it may be difficult to distinguish between attacking and defending actions, especially when an actor goes on the offense in the name of self-defense. The blending of offense and defense will often mix the strategic and tactical levels of operations. For instance, guerrillas on the defensive strategically may go on the offense tactically; the war of the mujahideen in Afghanistan provides a modern example.

The blurring of offense and defense reflects another feature of netwar: it tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal.

Thus the spread of netwar increases the challenges facing the modern nation-state. Nation-state ideals of sovereignty and authority are traditionally linked to a bureaucratic rationality in which issues and problems can be neatly divided, and specific offices can be assigned certain tasks. In netwar, matters are rarely so clear. A protagonist is likely to operate in the cracks and gray areas of society, striking where lines of authority crisscross and the operational paradigms of politicians, officials, soldiers, police officers, and related actors grow fuzzy and clash.

Against this background, we are led to a set of three policy-oriented propositions about the information revolution and its implications for netwar and counternetwar.

Hierarchies have a difficult time fighting networks

Some of the best examples of the difficulties faced by hierarchies in fighting networks are found in the failings of governments to defeat transnational criminal cartels engaged in drug smuggling, as in Colombia. The Zapatista movement in Mexico, with its legions of supporters and sympathizers among local and transnational nongovernmental organizations, shows that social netwar can put a democratizing autocracy on the defensive and pressure it to continue adopting reforms.

It takes networks to fight networks

Governments that would defend against netwar may need to adopt organizational designs and strategies like those of their adversaries. This does not mean mirroring the opponent, but rather learning to draw on the same design principles of network forms. These principles depend to some extent upon technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, and by building new mechanisms for interagency and multijurisdictional cooperation. Fighting networks also involves the ability not only to neutralize critical nodes when these exist and are identifiable (for example, key physical targets or a group of operatives shortly before a strike), but also to disrupt the information flows that enable dispersed units to coordinate their actions.

The first to master the network form will gain major advantages

In these early decades of the information age, adversaries who have adopted networking are enjoying an increase in power relative to state agencies. The strategic and structural design innovations brought by networks will give these organizations an edge over slower state actors, whose strategies and tactics are shaped by a traditional, hierarchical logic.

Counternetwar may thus require effective interagency approaches, which by their nature involve networked structures. The challenge will be to blend hierarchies and networks skillfully, while retaining enough core authority to encourage and enforce adherence to networked processes. By creating effective hybrids, governments may better confront the new threats and challenges now emerging, whether generated by terrorists, militias, criminals, or other actors.

MIDDLE EASTERN TERRORISM AND NETWAR

Terrorism seems to be evolving in the direction of violent netwar. Indeed, the netwar concept is con-

sistent with patterns and trends in the Middle East, where the newer and more active terrorist groups appear to be adopting decentralized, flexible network structures. The rise of networked arrangements in terrorist organizations is part of a wider move away from formally organized, state-sponsored groups to privately financed, loose networks of individuals and subgroups that may have strategic guidance but enjoy tactical independence. Related to these shifts is the fact that terrorist groups are taking advantage of information technology to coordinate the activities of dispersed members.

Terrorist organizations in the Middle East have diverse origins, ideologies, and structures, but can be categorized roughly into traditional and new-generation groups. Traditional groups date to the late 1960s and early 1970s, and the majority were (and some still are) formally or informally linked to the PLO. Typically, they are also relatively bureaucratic and maintain a nationalist or Marxist agenda. In contrast, most new-generation groups that arose in the 1980s and 1990s have more fluid organizational forms, and rely on Islam as a basis for their radical ideology.

Terrorist netwar may also be a battle of ideas—and to wage this form of conflict some terrorists may want the net up, not down.

The traditional, more bureaucratic groups have survived partly through support from states such as Syria, Libya, and Iran. These groups, such as the Abu Nidal Organization, the Popular Front for the Liberation of Palestine (PFLP), and three PFLP-related splinters—the PFLP–General Command, the Palestine Liberation Front, and the Democratic Front for the Liberation of Palestine—retain an ability to train and prepare for terrorist missions, although their involvement in actual operations has been limited in recent years, partly because of successful counterterrorism campaigns by Israeli and Western agencies. In contrast, the newer and less hierarchical groups, such as Hamas, the Palestinian Islamic Jihad, Hezbollah, Algeria's Armed Islamic Group, the Egyptian Islamic Group, and Osama bin Laden's terrorist network have become the most active organizations.

The new and more active generation of Middle Eastern groups has operated in and outside the region. For instance, in Israel and the occupied territories, Hamas, and to a lesser extent the Palestinian Islamic Jihad, have shown their strength over the last five years with a series of suicide bombings that have killed more than 100 people. Among the recent strikes by Egypt's Islamic Group (also known as al-Gama'a al-Islamiya) is the 1997 attack at Luxor, in which 58 tourists and 4 Egyptians were killed.

Another string of terrorist attacks (and foiled attempts) has focused attention on the loosely organized group of "Arab Afghans"—radical Islamic fighters from several North African and Middle Eastern countries who forged ties while resisting the Soviet occupation of Afghanistan. One of the leaders and founders of the Arab Afghan movement is Osama bin Laden, a Saudi entrepreneur based in Afghanistan. Bin Laden allegedly sent operatives to Yemen to bomb a hotel used by American soldiers on their way to Somalia in 1992, plotted to assassinate President Bill Clinton in the Philippines in 1994 and Egyptian President Hosni Mubarak in 1995, and played a role in the Riyadh and Khobar blasts in Saudi Arabia that resulted in the deaths of 24 Americans in 1995 and 1996. United States officials have pointed to bin Laden as the mastermind behind the American embassy bombings in Kenya and Tanzania in 1998, which claimed the lives of more than 260 people, including 12 Americans.

To varying degrees, these groups share the principles of the networked organizations—relatively flat hierarchies, decentralization and delegation of decision-making authority, and loose lateral ties among dispersed groups and individuals. Hamas, for example, is, according to the United States State Department, "loosely structured, with some elements working clandestinely and others working openly through mosques and social service institutions to recruit members, raise money, organize activities, and distribute propaganda."

Perhaps the most interesting example of terrorist netwar is Osama bin Laden's Arab Afghans, who have formed a complex network of relatively autonomous groups that are financed from private sources. Bin Laden uses his wealth and organizational skills to support and direct al Qaeda (the Base), a multinational alliance of Islamic extremists. Most of the groups that participate in this front (including Egypt's Islamic Group) remain independent, although the organizational barriers between them are fluid (for example, there have been reports of a recent inflow of Arab Afghans into Egypt's Islamic Group to reinforce the latter's operations).

At the heart of al Qaeda is bin Laden's own inner core group, which sometimes conducts missions

on its own. The goal of the alliance is opposition on a global scale to perceived threats to Islam, as indicated by bin Laden's 1996 declaration of a holy war against the United States and the West. In the document, bin Laden specifies that this holy war will be fought by irregular, light, highly mobile forces using guerrilla tactics. Although bin Laden finances Arab Afghan activities (exploiting a fortune of around $300 million, according to State Department estimates) and directs some operations, he apparently does not play a direct command-and-control role over all operatives. Bin Laden represents a key node in the Arab Afghan terror network, but the network conducts many operations without his involvement, leadership, or financing—and will continue to be able to do so should he be killed or captured.

From a netwar perspective, two interesting features of bin Laden's organization are noteworthy. First, al Qaeda is a well-financed nonstate actor that, lacking a firm state sponsor, cannot be easily targeted by coercing supportive national governments.[3] Second, bin Laden's movement is able to relocate operations swiftly in response to changing circumstances and needs. Arab Afghans associated with bin Laden have reportedly been active in several countries, including Bangladesh, Bosnia, Chechnya, India (Kashmir), Pakistan, Tajikistan, Somalia, and more recently, Kosovo. Such mobility is boosted by several local affiliates al Qaeda has in different countries, and by a sizable training establishment in Afghanistan. The training infrastructure prepares "Islamic rapid-deployment forces" that can be fielded as opportunities arise.

This group's ability to move and act quickly (and, to some extent, to swarm) when opportunities emerge hampers counterterrorist efforts to predict its actions and monitor its activities. The ability of Arab Afghan operatives to strike the American embassies in Kenya and Tanzania—and to reportedly consider targeting similar structures in Madagascar, Gambia, Togo, Liberia, Namibia, and Senegal—substantiates the claim that members of this network have the mobility and speed to operate over considerable distances.

[3]Although the Taliban regime in Afghanistan is supporting bin Laden by hosting his training infrastructure and bases, this level of sponsorship is qualitatively different from what Iran and Syria have traditionally offered to other Middle Eastern terrorists. Moreover, the relationship between the Taliban and bin Laden has often been confrontational, with the former threatening the eviction and, according to some reports, his movements and access to communications systems.

THE ROLE OF INFORMATION TECHNOLOGY

Another feature that distinguishes the newer generation of terrorist groups is its adoption of information technology. Some evidence supports the claim that the most active groups—and therefore the most decentralized groups—have embraced information technology to coordinate activities and disseminate propaganda and ideology. At the same time, the technical assets and know-how gained by terrorist groups as they seek to form into multi-organizational networks can be used for offensive purposes: an Internet connection can be used for both coordination and disruption. The anecdotes provided here are consistent with the rise in the Middle East of what has been termed "techno-terrorism," or the use by terrorists of satellite communications, e-mail, and the World Wide Web.

The bin Laden network appears to have widely adopted information technology. According to reporters who visited bin Laden's headquarters in a remote mountainous area of Afghanistan, the terrorist financier has modern computer and communications equipment. Bin Laden allegedly uses satellite phone terminals to coordinate the activities of the group's dispersed operatives, and has even devised countermeasures to ensure his safety while using such communication systems (satellite phones reportedly travel in separate convoys from bin Laden's; the Saudi financier also refrains from direct use, and often dictates his message to an assistant, who then relays it telephonically from a different location). Egyptian "Afghan" computer experts are said to have helped devise a communication network that relies on the World Wide Web, e-mail, and electronic bulletin boards so that affiliates can exchange information without running a major risk of being intercepted by counterterrorism officials.

Hamas also uses the Internet to share operational information. Hamas activists in the United States use chat rooms to plan operations and activities, and operatives use e-mail to coordinate activities across Gaza, the West Bank, and Lebanon. Hamas has realized that information can be passed securely over the Internet because counterterrorism intelligence cannot monitor accurately the flow and content of all Internet traffic. Israeli security officials cannot easily trace Hamas messages or decode their content.

The Internet is also used as a propaganda tool by Hezbollah, which manages three web sites—one for the central press office (www.hizbollah.org), another to describe its attacks on Israeli targets (www.moqawama.org), and a third for news and

information (www.almanar.com.lb). Hezbollah also regularly broadcasts footage of strikes carried out by its operatives through its television station, and has a sophisticated media center that regularly—and professionally—briefs foreign journalists on the progress of its military campaign against Israel.

COERCION, WAR, OR NEW-WORLD HARBINGER?

The evolution of terrorism in the direction of netwar will create new difficulties for counterterrorism. The types of challenges, and their severity, will depend on the doctrines that terrorists develop and employ. Some doctrinal effects will occur at the operational level, as in the relative emphasis placed on disruptive information operations as distinct from destructive combat operations. However, at a deeper level, the direction in which terrorist netwar evolves will depend on the choices terrorists make about the overall doctrinal paradigms that shape their goals and strategies.

At least three terrorist paradigms should be considered: terror as coercive diplomacy; terror as war; and terror as the harbinger of a "new world." These engage, in varying ways, distinct rationales for terrorism—as a weapon of the weak, as an assertion of identity, and as a way to break through to a new world. While much debate has existed about the overall success or failure of terrorism, the paradigm under which a terrorist operates may have a great deal to do with the likelihood of success. Coercion, for example, implies distinctive threats or uses of force, such as the often violent acts carried out by Palestinians in pursuit of independence. The norms of war often imply maximizing destruction; Osama bin Laden and his Arab Afghan associates can be viewed within this paradigm. The final paradigm aims at achieving the birth of what might be called a "new world" and may be driven by religious mania, a desire for totalitarian control, or an impulse toward ultimate chaos; the Japanese cult Aum Shinrikyo (now renamed "Aleph") is a recent example.

All three paradigms offer room for netwar and allow the rise of "cybotage"—acts of disruption and destruction against information infrastructures by terrorists, as well as by disaffected individuals with technical skills who are drawn into the terrorist milieu. But terrorist netwar may also be a battle of ideas—and to wage this form of conflict some terrorists may want the net up, not down.

Many experts argue that terrorism is moving toward ever more lethal, destructive acts. Although this is true, it is also possible that some terrorist netwars will stress disruption over destruction. Networked terrorists will no doubt continue to destroy property and kill people, but their principal strategy may move toward the nonlethal end of the spectrum, where command-and-control nodes and vulnerable information infrastructures provide rich sets of targets.

Indeed, terrorism has long been about "information"—from keeping trainees for suicide bombings away from international media, through the ways that terrorists seek to create disasters that will make the front pages, to the related debates about countermeasures that would limit freedom of the press, increase public surveillance and intelligence gathering, and heighten security over information and communications systems. Terrorist tactics focus attention on the importance of information and communications for the functioning of democratic institutions; debates about how terrorist threats undermine democratic practices may revolve around freedom of information issues.

While netwar may be waged by terrorist groups operating with any of the three paradigms, the rise of networked groups whose objective is to wage war may be the paradigm most relevant—and dangerous—to targeted governments and their instruments of power. Indeed, terrorists who perceive themselves as warriors are already inclined to strike enemy government and military assets.

Terrorism has a constant: finding ways to spread fear and alarm by means of surreptitious, surgical, asymmetrical strikes. Yet terrorism is also adaptive: the ways chosen change with the times. In the information age, cyberterrorism and cybotage may have growing appeal. But so may the creation of titanic explosions and biological or chemical disasters whose "cyber" aspects are essentially collateral—as in the telecommunications devices the terrorists use, or in the impact on the media, or in the nature of the target site (if it contains a computer switch for financial transactions, for example).

To assess whether a particular tactic or target is a result of netwar—or whether a netwar design may enhance the likelihood of terrorists' pursuing that tactic or target—analysts should examine not only how the information revolution is altering the technological orientations of terrorists, but also how it is changing their organizational and doctrinal orientations. This approach will require governments to craft responses that go beyond simple technological counters, and reengineer the way they approach the problem of terrorism in the information age. ■