Chapter Three

NETWORKS, NETWAR, AND INFORMATION-AGE TERRORISM

John Arquilla, David Ronfeldt, and Michele Zanini

The rise of network forms of organization is a key consequence of the ongoing information revolution. Business organizations are being newly energized by networking, and many professional militaries are experimenting with flatter forms of organization. In this chapter, we explore the impact of networks on terrorist capabilities, and consider how this development may be associated with a move away from emphasis on traditional, episodic efforts at coercion to a new view of terror as a form of protracted warfare. Seen in this light, the recent bombings of U.S. embassies in East Africa, along with the retaliatory American missile strikes, may prove to be the opening shots of a war between a leading state and a terror network. We consider both the likely context and the conduct of such a war, and offer some insights that might inform policies aimed at defending against and countering terrorism.

A NEW TERRORISM (WITH OLD ROOTS)

The age-old phenomenon of terrorism continues to appeal to its perpetrators for three principal reasons. First, it appeals as a weapon of the weak—a shadowy way to wage war by attacking asymmetrically to harm and try to defeat an ostensibly superior force. This has had particular appeal to ethno-nationalists, racist militias, religious fundamentalists, and other minorities who cannot match the military formations and firepower of their "oppressors"—the case, for example, with some radical Middle Eastern Islamist groups vis-à-vis Israel, and, until recently, the Provisional Irish Republican Army (PIRA) vis-à-vis Great Britain.

Second, terrorism has appealed as a way to assert identity and command attention—rather like proclaiming, "I bomb, therefore I am." Terrorism enables a perpetrator to publicize his identity, project it explosively, and touch the nerves of powerful distant leaders. This kind of attraction to violence transcends its instrumental utility. Mainstream revolutionary writings may view violence as a means of struggle, but terrorists often regard violence as an end in itself that generates identity or damages the enemy's identity.

Third, terrorism has sometimes appealed as a way to achieve a new future order by willfully wrecking the present. This is manifest in the religious fervor of some radical Islamists, but examples also lie among millenarian and apocalyptic groups, like Aum Shinrikyo in Japan, who aim to wreak havoc and rend a system asunder so that something new may emerge from the cracks. The substance of the future vision may be only vaguely defined, but its moral worth is clear and appealing to the terrorist.

In the first and second of these motivations or rationales, terrorism may involve retaliation and retribution for past wrongs, whereas the third is also about revelation and rebirth, the coming of a new age. The first is largely strategic; it has a practical tone, and the objectives may be limited and specific. In contrast, the third may engage a transcendental, unconstrained view of how to change the world through terrorism.

Such contrasts do not mean the three are necessarily at odds; blends often occur. Presumptions of weakness (the first rationale) and of willfulness (in the second and third) can lead to peculiar synergies. For example, Aum's members may have known it was weak in a conventional sense, but they believed that they had special knowledge, a unique leader, invincible willpower, and secret ways to strike out.

These classic motivations or rationales will endure in the information age. However, terrorism is not a fixed phenomenon; its perpetrators adapt it to suit their times and situations. What changes is the conduct of terrorism—the operational characteristics built around the motivations and rationales.

This chapter addresses, often in a deliberately speculative manner, changes in organization, doctrine, strategy, and technology that,

taken together, speak to the emergence of a "new terrorism" attuned to the information age. Our principal hypotheses are as follows:

- **Organization.** Terrorists will continue moving from hierarchical toward information-age network designs. Within groups, "great man" leaderships will give way to flatter decentralized designs. More effort will go into building arrays of transnationally internetted groups than into building stand-alone groups.
- **Doctrine and strategy.** Terrorists will likely gain new capabilities for lethal acts. Some terrorist groups are likely to move to a "war paradigm" that focuses on attacking U.S. military forces and assets. But where terrorists suppose that "information operations" may be as useful as traditional commando-style operations for achieving their goals, systemic *disruption* may become as much an objective as target *destruction*. Difficulties in coping with the new terrorism will mount if terrorists move beyond isolated acts toward a new approach to doctrine and strategy that emphasizes campaigns based on swarming.
- **Technology.** Terrorists are likely to increasingly use advanced information technologies for offensive and defensive purposes, as well as to support their organizational structures. Despite widespread speculation about terrorists using cyberspace warfare techniques to take "the Net" down, they may often have stronger reasons for wanting to keep it up (e.g., to spread their message and communicate with one another).

In short, terrorism is evolving in a direction we call *netwar*. Thus, after briefly reviewing terrorist trends, we outline the concept of netwar and its relevance for understanding information-age terrorism. In particular, we elaborate on the above points about organization, doctrine, and strategy, and briefly discuss how recent developments in the nature and behavior of Middle Eastern terrorist groups can be interpreted as early signs of a move toward netwar-type terrorism.

Given the prospect of a netwar-oriented shift in which some terrorists pursue a war paradigm, we then focus on the implications such a development may have for the U.S. military. We use these insights to consider defensive antiterrorist measures, as well as proactive counterterrorist strategies. We propose that a key to coping with information-age terrorism will be the creation of interorganizational

networks within the U.S. military and government, partly on the grounds that it takes networks to fight networks.

RECENT VIEWS ABOUT TERRORISM

Terrorism remains a distinct phenomenon while reflecting broader trends in irregular warfare. The latter has been on the rise around the world since before the end of the Cold War. Ethnic and religious conflicts, recently in evidence in areas of Africa, the Balkans, and the Caucasus, for awhile in Central America, and seemingly forever in the Middle East, attest to the brutality that increasingly attends this kind of warfare. These are not conflicts between regular, professional armed forces dedicated to warrior creeds and Geneva Conventions. Instead, even where regular forces play roles, these conflicts often revolve around the strategies and tactics of thuggish paramilitary gangs and local warlords. Some leaders may have some professional training; but the foot soldiers are often people who, for one reason or another, get caught in a fray and learn on the job. Adolescents and children with high-powered weaponry are taking part in growing numbers. In many of these conflicts, savage acts are increasingly committed without anyone taking credit—it may not even be clear which side is responsible. The press releases of the protagonists sound high-minded and self-legitimizing, but the reality at the local level is often about clan rivalries and criminal ventures (e.g., looting, smuggling, or protection rackets).[1]

Thus, irregular warfare has become endemic and vicious around the world. A decade or so ago, terrorism was a rather distinct entry on the spectrum of conflict, with its own unique attributes. Today, it seems increasingly connected with these broader trends in irregular warfare, especially as waged by nonstate actors. As Martin Van Creveld warns:

> In today's world, the main threat to many states, including specifically the U.S., no longer comes from other states. Instead, it comes from small groups and other organizations which are not states.

---

[1]For an illuminating take on irregular warfare that emphasizes the challenges to the Red Cross, see Michael Ignatieff, "Unarmed Warriors," *The New Yorker*, March 24, 1997, pp. 56–71.

> Either we make the necessary changes and face them today, or what is commonly known as the modern world will lose all sense of security and will dwell in perpetual fear.[2]

Meanwhile, for the past several years, terrorism experts have broadly concurred that this phenomenon will persist, if not get worse. General agreement that terrorism may worsen parses into different scenarios. For example, Walter Laqueur warns that religious motivations could lead to "superviolence," with millenarian visions of a coming apocalypse driving "postmodern" terrorism. Fred Iklé worries that increased violence may be used by terrorists to usher in a new totalitarian age based on Leninist ideals. Bruce Hoffman raises the prospect that religiously-motivated terrorists may escalate their violence in order to wreak sufficient havoc to undermine the world political system and replace it with a chaos that is particularly detrimental to the United States—a basically nihilist strategy.[3]

The preponderance of U.S. conventional power may continue to motivate some state and nonstate adversaries to opt for terror as an asymmetric response. Technological advances and underground trafficking may make weapons of mass destruction (WMD—nuclear, chemical, biological weapons) ever easier for terrorists to acquire.[4] Terrorists' shifts toward looser, less hierarchical organizational structures, and their growing use of advanced communications technologies for command, control, and coordination, may further empower small terrorist groups and individuals who want to mount operations from a distance.

There is also agreement about an emergence of two tiers of terror: one characterized by hard-core professionals, the other by amateur

---

[2]Martin Van Creveld, "In Wake of Terrorism, Modern Armies Prove to Be Dinosaurs of Defense," *New Perspectives Quarterly*, Vol. 13, No. 4, Fall 1996, p. 58.

[3]See Walter Laqueur, "Postmodern Terrorism," *Foreign Affairs*, Vol. 75, No. 5, September/October 1996, pp. 24–36; Fred Iklé, "The Problem of the Next Lenin," *The National Interest*, Vol. 47, Spring 1997, pp. 9–19; Bruce Hoffman, *Responding to Terrorism Across the Technological Spectrum*, RAND, P-7874, 1994; Bruce Hoffman, *Inside Terrorism*, Columbia University Press, New York, 1998; Robert Kaplan, "The Coming Anarchy," *Atlantic Monthly*, February 1994, pp. 44–76.

[4]See J. Kenneth Campbell, "Weapon of Mass Destruction Terrorism," Master's thesis, Naval Postgraduate School, Monterey, California, 1996.

cut-outs.[5] The deniability gained by terrorists operating through willing amateurs, coupled with the increasing accessibility of ever more destructive weaponry, has also led many experts to concur that terrorists will be attracted to engaging in more lethal destruction, with increased targeting of information and communications infrastructures.[6]

Some specialists also suggest that "information" will become a key target—both the conduits of information infrastructures and the content of information, particularly the media.[7] While these target-sets may involve little lethal activity, they offer additional theaters of operations for terrorists. Laqueur in particular foresees that, "If the new terrorism directs its energies toward information warfare, its destructive power will be exponentially greater than any it wielded in the past—greater even than it would be with biological and chemical weapons."[8] New planning and scenario-building is needed to help think through how to defend against this form of terrorism.[9]

Such dire predictions have galvanized a variety of responses, which range from urging the creation of international control regimes over the tools of terror (such as WMD materials and advanced encryption capabilities), to the use of coercive diplomacy against state sponsors of terror. Increasingly, the liberal use of military force against terrorists has also been recommended. Caleb Carr in particular espoused this theme, sparking a heated debate.[10] Today, many leading works

---

[5]Bruce Hoffman and Caleb Carr, "Terrorism: Who Is Fighting Whom?" *World Policy Journal*, Vol. 14, No. 1, Spring 1997, pp. 97–104.

[6]For instance, Martin Shubik, "Terrorism, Technology, and the Socioeconomics of Death," *Comparative Strategy*, Vol. 16, No. 4, October–December 1997, pp. 399–414; as well as Hoffman, 1998.

[7]See Matthew Littleton, "Information Age Terrorism," MA thesis, U.S. Naval Postgraduate School, 1995, and Brigitte Nacos, *Terrorism and the Media*, Columbia University Press, New York, 1994.

[8]Laqueur, 1996, p. 35.

[9]For more on this issue, see Roger Molander, Andrew Riddile, and Peter Wilson, *Strategic Information Warfare: A New Face of War*, RAND, MR-661-OSD, 1996; Roger Molander, Peter Wilson, David Mussington, and Richard Mesic, *Strategic Information Warfare Rising*, RAND, 1998.

[10]Caleb Carr, "Terrorism as Warfare," *World Policy Journal*, Vol. 13, No. 4, Winter 1996–1997, pp. 1–12. This theme was advocated early by Gayle Rivers, *The War*

on combating terrorism blend notions of control mechanisms, international regimes, and the use of force.[11]

Against this background, experts have begun to recognize the growing role of networks—of networked organizational designs and related doctrines, strategies, and technologies—among the practitioners of terrorism. The growth of these networks is related to the spread of advanced information technologies that allow dispersed groups, and individuals, to conspire and coordinate across considerable distances. Recent U.S. efforts to investigate and attack the bin Laden network (named for the central influence of Osama bin Laden) attest to this. The rise of networks is likely to reshape terrorism in the information age, and lead to the adoption of netwar—a kind of information-age conflict that will be waged principally by nonstate actors. Our contribution to this volume is to present the concept of netwar and show how terrorism is being affected by it.

THE ADVENT OF NETWAR—ANALYTICAL BACKGROUND[12]

The information revolution is altering the nature of conflict across the spectrum. Of the many reasons for this, we call attention to two in particular. 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 (especially all-channel networks, in which every node is connected to every other node) more readily than can traditional, hierarchical, state actors. Nonstate-actor networks are thought to be more flexible and responsive than hierarchies in reacting to outside developments, and

---

Against the Terrorists: How to Fight and Win, Stein and Day, New York, 1986. For more on the debate, see Hoffman and Carr, 1997.

[11]See, for instance, Benjamin Netanyahu, *Winning the War Against Terrorism*, Simon and Schuster, New York, 1996, and John Kerry (Senator), *The New War*, Simon & Schuster, New York, 1997.

[12]This analytical background is drawn from John Arquilla and David Ronfeldt, *The Advent of Netwar*, RAND, MR-678-OSD, 1996, and David Ronfeldt, John Arquilla, Graham Fuller, and Melissa Fuller, *The Zapatista "Social Netwar" in Mexico*, RAND, MR-994-A, forthcoming. Also see John Arquilla and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age*, RAND, MR-880-OSD/RC, 1997.

to be better than hierarchies at using information to improve decisionmaking.[13]

Second, as the information revolution deepens, conflicts will increasingly depend on information and communications matters. More than ever before, conflicts will revolve around "knowledge" and the use of "soft power."[14] 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 of its adversaries. Psychological disruption may become as important a goal as physical destruction.

Thus, major transformations are coming 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 diffuse, dispersed, multidimensional, and ambiguous than more traditional threats. Metaphorically, future conflicts may resemble the Oriental game of *Go* more than the Western game of chess. The conflict spectrum will be molded from end to end by these dynamics:

- *Cyberwar*—a concept that refers to information-oriented military warfare—is becoming an important entry at the military end of the spectrum, where the language has normally been about high-intensity conflicts (HICs).
- *Netwar* figures increasingly at the societal end of the spectrum, where the language has normally been about low-intensity conflict (LIC), operations other than war (OOTW), and nonmilitary modes of conflict and crime. [15]

---

[13]For background on this issue, see Charles Heckscher, "Defining the Post-Bureaucratic Type," in Charles Heckscher and Anne Donnelon (eds.), *The Post-Bureaucratic Organization*, Sage, Thousand Oaks, California, 1995, pp. 50–52.

[14]The concept of soft power was introduced by Joseph S. Nye in *Bound to Lead: The Changing Nature of American Power*, Basic Books, New York, 1990, and further elaborated in Joseph S. Nye, and William A. Owens, "America's Information Edge," *Foreign Affairs*, Vol. 75, No. 2, March/April 1996.

[15]For more on information-age conflict, netwar, and cyberwar, see John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol. 12, No. 2, Summer 1993, pp. 141–165, and Arquilla and Ronfeldt, 1996 and 1997.

Whereas cyberwar usually pits formal military forces against each other, netwar is more likely to involve nonstate, paramilitary, and irregular forces—as in the case of terrorism. Both concepts are consistent with the views of analysts such as Van Creveld, who believe that a "transformation of war" is under way.[16] Neither concept is just about technology; both refer to *comprehensive* approaches to conflict—comprehensive in that they mix organizational, doctrinal, strategic, tactical, and technological innovations, for offense and defense.

Definition of Netwar

To be more precise, *netwar* refers to an emerging 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 who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command. Thus, information-age netwar differs from modes of conflict and crime in which the protagonists prefer formal, stand-alone, hierarchical organizations, doctrines, and strategies, as in past efforts, for example, to build centralized movements along Marxist lines.

The term 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 string of 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. It is also about the Asian Triads more than the Sicilian Mafia, and Chicago's Gangsta Disciples more than the Al Capone Gang.

This spectrum includes familiar adversaries who are modifying their structures and strategies to take advantage of networked designs,

---

[16]Martin Van Creveld, *The Transformation of War*, Free Press, New York, 1991.

such as transnational terrorist groups, black-market proliferators of WMD, transnational crime syndicates, fundamentalist and ethnonationalist movements, intellectual property and high-sea pirates, and smugglers of black-market goods or migrants. Some urban gangs, back-country militias, and militant single-issue groups in the United States are also developing netwar-like attributes. In addition, there is a new generation of radicals and activists who 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 (e.g., violent terrorist and criminal organizations) may threaten U.S. and other nations' interests, but other netwar actors (e.g., peaceful social activists) may not. Some may aim at destruction, others at disruption. Again, many variations are possible.

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

More About Organizational Design

The notion of an organizational structure qualitatively different from traditional hierarchical designs is not recent; for example, in the early 1960s Burns and Stalker referred to the *organic* form as "a network structure of control, authority, and communication," with "lateral rather than vertical direction of communication." In organic structure,[17]

---

[17]T. Burns and G. M. Stalker, *The Management of Innovation*, Tavistock, London, 1961, p. 121.

> omniscience [is] no longer imputed to the head of the concern; knowledge about the technical or commercial nature of the here and now task may be located anywhere in the network; [with] this location becoming the ad hoc centre of control authority and communication.

In the business world, virtual or networked organizations are being heralded as effective alternatives to bureaucracies—as in the case of Eastman Chemical Company and the Shell-Sarnia Plant—because of their inherent flexibility, adaptiveness, and ability to capitalize on the talents of all members of the organization.[18]

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" who share a set of ideas and interests and who are arrayed to act in a fully internetted "all-channel" manner. Networks come in basically three types (or topologies) (see Figure 3):[19]

- 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.
- 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.
- The *all-channel* network, as in a collaborative network of militant small groups where every group is connected to every other.

Each node in the diagrams of Figure 3 may be to an individual, a group, an institution, part of a group or institution, or even a state. The nodes may be large or small, tightly or loosely coupled, and in-

---

[18]See, for instance, Jessica Lipnack and Jeffrey Stamps, *The Age of the Network*, Wiley & Sons, New York, 1994, pp. 51–78, and Heckscher, "Defining the Post-Bureaucratic Type," p. 45.

[19]Adapted from William M. Evan, "An Organization-Set Model of Interorganizational Relations," in Matthew Tuite, Roger Chisholm, and Michael Radnor (eds.), *Interorganizational Decisionmaking*, Aldine Publishing Company, Chicago, 1972.

clusive or exclusive in membership. They may be segmentary or specialized—that is, they may look alike and engage in similar activities, or they may undertake a division of labor based on specialization. The boundaries of the network may be well defined, or blurred and porous in relation to the outside environment. All such variations are possible.

Each type may be suited to different conditions and purposes, and all three may be found among netwar-related adversaries—e.g., the chain in smuggling operations, the star at the core of terrorist and criminal syndicates, and the all-channel type among militant groups that are highly internetted and decentralized. There may also be hybrids. For example, a netwar actor may have an all-channel council at its core, but use stars and chains for tactical operations. There may also be hybrids of network and hierarchical forms of organization, and hierarchies may exist inside particular nodes in a network. Some actors may have a hierarchical organization overall, but use networks for tactical operations; other actors may have an all-channel network design, but use hierarchical teams for tactical operations. Again, many configurations are possible, and it may be difficult for an analyst to discern exactly what type of networking characterizes a particular actor.

Of the three network types, the all-channel has been the most difficult to organize and sustain historically, partly because it may require dense communications. However, it gives the network form the most potential for collaborative undertakings, and it is the type

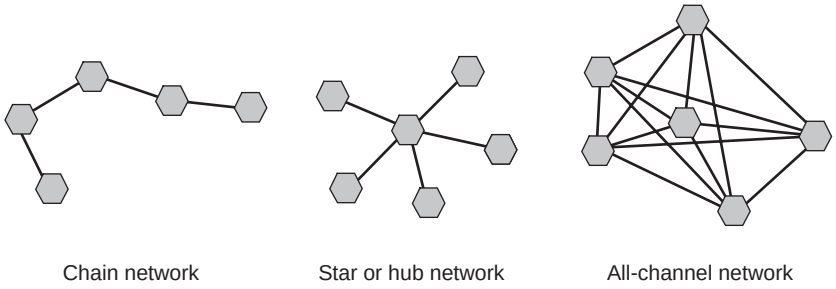

Figure 3—Types of Networks

that is gaining strength from the information revolution. Pictorially, an all-channel netwar actor resembles a geodesic "Bucky ball" (named for Buckminster Fuller); it does not resemble a pyramid. The design is flat. 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 there may be 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).[20]

The capacity of this design for effective performance over time 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," even though 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 do not have to resort to a hierarchy—"they know what they have to do."[21]

The network design may depend on having an infrastructure for the dense communication of functional information. All nodes are not necessarily 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 to disseminate information promptly and as broadly as desired within the network and to outside audiences.

---

[20]The structure may also be cellular, although the presence of cells does not necessarily mean a network exists. A hierarchy can also be cellular, as is the case with some subversive organizations. A key difference between cells and nodes is that the former are designed to minimize information flows for security reasons (usually only the head of the cell reports to the leadership), while nodes in principle can easily establish connections with other parts of the network (so that communications and coordination can occur horizontally).

[21]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 *The Seditionist*, Issue 12, February 1992.

In many respects, then, the archetypal netwar design corresponds to what earlier analysts called a "segmented, polycentric, ideologically integrated network" (SPIN):[22]

> By segmentary I mean that it is cellular, composed of many different groups. . . . By polycentric I mean that it has many different leaders or centers of direction. . . . By networked I mean that the segments and the leaders are integrated into reticulated systems or networks through various structural, personal, and ideological ties. Networks are usually unbounded and expanding. . . . This acronym [SPIN] helps us picture this organization as a fluid, dynamic, expanding one, spinning out into mainstream society.

Caveats About the Role of Technology

To realize its potential, a fully interconnected network requires a capacity for constant, dense information and communications flows, more so than do other forms of organization (e.g., hierarchies). This capacity is afforded by the latest information and communications technologies—cellular telephones, fax machines, electronic mail (e-mail), World Wide Web (WWW) sites, and computer conferencing. Moreover, netwar agents are poised to benefit from future increases in the speed of communication, dramatic reductions in the costs of communication, increases in bandwidth, vastly expanded connectivity, and integration of communication with computing technologies.[23] Such technologies are highly advantageous for a netwar actor whose constituents are geographically dispersed.

---

[22]See Luther P. Gerlach, "Protest Movements and the Construction of Risk," in B. B. Johnson and V. T. Covello (eds.), *The Social and Cultural Construction of Risk*, D. Reidel Publishing Co., Boston, Massachusetts, 1987, p. 115, based on Luther P. Gerlach and Virginia Hine, *People, Power, Change: Movements of Social Transformation*, The Bobbs-Merrill Co., New York, 1970. This SPIN concept, a precursor of the netwar concept, was proposed by Luther Gerlach and Virginia Hine in the 1960s to depict U.S. social movements. It anticipates many points about network forms of organization that are now coming into focus in the analysis not only of social movements but also some terrorist, criminal, ethno-nationalist, and fundamentalist organizations.

[23]See Wolf V. Heydenbrand, "New Organizational Forms," *Work and Occupations*, No. 3, Vol. 16, August 1989, pp. 323–357.

However, caveats are in order. First, the new technologies, however enabling for organizational networking, may not be the only crucial technologies for a netwar actor. Old 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 or the infosphere. 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, what happens in the real world is generally more important than what happens in the virtual worlds of cyberspace or the infosphere.[24] Netwar is not Internet war.

Swarming, and the Blurring of Offense and Defense

This distinctive, often ad-hoc design has unusual strengths, for both offense and defense. On the offense, networks are known for being adaptable, flexible, and versatile vis-à-vis opportunities and challenges. 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.[25]

Swarming occurs when the dispersed nodes of a network of small (and perhaps some large) forces converge on a target from multiple directions. The overall aim is the *sustainable pulsing* of force or fire. Once in motion, 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

---

[24]See Paul Kneisel, "Netwar: The Battle Over Rec.Music.White-Power," *ANTIFA INFO-BULLETIN*, Research Supplement, June 12, 1996, unpaginated ASCII text available on the Internet. Kneisel analyzes the largest vote ever taken about the creation of a new Usenet newsgroup—a vote to prevent the creation of a group that was ostensibly about white-power music. He concludes that "The *war* against contemporary fascism will be won in the 'real world' off the net; but *battles* against fascist netwar are fought and won on the Internet." His title is testimony to the spreading usage of the term *netwar*.

[25]Swarm networks are discussed by Kevin Kelly, *Out of Control: The Rise of Neo-Biological Civilization*, A William Patrick Book, Addison-Wesley Publishing Company, New York, 1994. Also see Arquilla and Ronfeldt, 1997.

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, particularly 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 example, 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. A government has difficulty assigning responsibility to a single agency—military, police, or intelligence—to respond.

Thus, the spread of netwar adds to the challenges facing the nation-state in the information age. 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 charged with taking care of specific problems. In netwar, things 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 get fuzzy and clash.

Networks Versus Hierarchies: Challenges for Counternetwar

Against this background, we are led to a set of four policy-oriented propositions about the information revolution and its implications for netwar and *counternetwar*.[26]

Hierarchies have a difficult time fighting networks. There are examples across the conflict spectrum. Some of the best are found in the failings of governments to defeat transnational criminal cartels engaged in drug smuggling, as in Colombia. The persistence of religious revivalist movements, as in Algeria, in the face of unremitting state opposition, shows the robustness of the network form. The Zapatista movement in Mexico, with its legions of supporters and sympathizers among local and transnational nongovernmental organizations (NGOs), 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 have to adopt organizational designs and strategies like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles of network forms in the information age. 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.

Whoever masters the network form first and best will gain major advantages. In these early decades of the information age, adversaries who have adopted networking (be they criminals, terrorists, or peaceful social activists) are enjoying an increase in their power relative to state agencies.

---

[26]Also see Alexander Berger, "Organizational Innovation and Redesign in the Information Age: The Drug War, Netwar, and Other Low-End Conflict," Master's Thesis, Naval Postgraduate School, Monterey, California, 1998, for additional thinking and analysis about such propositions.

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 emerging in the information age, whether generated by terrorists, militias, criminals, or other actors.[27] The U.S. Counterterrorist Center, based at the Central Intelligence Agency (CIA), is a good example of a promising effort to establish a functional interagency network,[28] although its success may depend increasingly on the strength of links with the military services and other institutions that fall outside the realm of the intelligence community.

MIDDLE EASTERN TERRORISM AND NETWAR

Terrorism seems to be evolving in the direction of violent netwar. Islamic fundamentalist organizations like Hamas and the bin Laden network consist of groups organized in loosely interconnected, semi-independent cells that have no single commanding hierarchy.[29] Hamas exemplifies the shift away from a hierarchically oriented

---

[27]For elaboration, see Arquilla and Ronfeldt, 1997, Chapter 19.

[28]Vernon Loeb, "Where the CIA Wages Its New World War," *Washington Post*, September 9, 1998. For a broader discussion of interagency cooperation in countering terrorism, see Ashton Carter, John Deutch, and Philip Zelikow, "Catastrophic Terrorism," *Foreign Affairs*, Vol. 77, No. 6, November/December 1998, pp. 80–94.

[29]Analogously, right-wing militias and extremist groups in the United States also rely on a doctrine of "leaderless resistance" propounded by Aryan nationalist Louis Beam. See Beam, 1992; and Kenneth Stern, *A Force upon the Plain: The American Militia Movement and the Politics of Hate*, Simon and Schuster, New York, 1996. Meanwhile, as part of a broader trend toward netwar, transnational criminal organizations (TCOs) have been shifting away from centralized "Dons" to more networked structures. See Phil Williams, "Transnational Criminal Organizations and International Security," *Survival*, Vol. 36, No. 1, Spring 1994, pp. 96–113; and Phil Williams, "The Nature of Drug-Trafficking Networks," *Current History*, April 1998, pp. 154–159. As noted earlier, social activist movements long ago began to evolve "segmented, polycephalous, integrated networks." For a discussion of a social netwar in which human-rights and other peaceful activist groups supported an insurgent group in Mexico, see David Ronfeldt and Armando Martinez, "A Comment on the Zapatista 'Netwar'," in John Arquilla and David Ronfeldt, 1997, pp. 369–391.

movement based on a "great leader" (like the PLO and Yasser Arafat).[30]

The netwar concept is consistent 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. Such technology may be employed by terrorists not only to wage information warfare, but also to support their own networked organizations.[31]

While a comprehensive empirical analysis of the relationship between (a) the structure of terrorist organizations and (b) group activity or strength is beyond the scope of this paper,[32] a cursory examination of such a relationship among Middle Eastern groups offers some evidence to support the claim that terrorists are preparing to wage netwar. The Middle East was selected for analysis mainly be-

---

[30]It is important to differentiate our notions of information-age networking from earlier ideas about terror as consisting of a network in which all nodes revolved around a Soviet core (Claire Sterling, *The Terror Network,* Holt, Rinehart & Winston, New York, 1981). This view has generally been regarded as unsupported by available evidence (see Cindy C. Combs, *Terrorism in the Twenty-First Century,* Prentice-Hall, New York, 1997, pp. 99–119). However, there were a few early studies that did give credit to the possibility of the rise of terror networks that were bound more by loose ties to general strategic goals than by Soviet control (see especially Thomas L. Friedman, "Loose-Linked Network of Terror: Separate Acts, Ideological Bonds," *Terrorism*, Vol. 8, No. 1, Winter 1985, pp. 36–49).

[31]For good general background, see Michael Whine, "Islamist Organisations on the Internet," draft circulated on the Internet, April 1998 *(www.ict.org.il/articles).*

[32]We assume that group activity is a proxy for group strength. Group activity can be measured more easily than group strength, and is expected to be significantly correlated with strength. The relationship may not be perfect, but it is deemed to be sufficiently strong for our purposes.

cause terrorist groups based in this region have been active in targeting U.S. government facilities and interests, as in the bombings of the Khobar Towers, and most recently, the American embassies in Kenya and Tanzania.

Middle Eastern Terrorist Groups: Structure and Actions

Terrorist groups in the Middle East have diverse origins, ideologies, and organizational structures, but can be roughly categorized into traditional and new-generation groups. Traditional groups date back to the late 1960s and early 1970s, and the majority of these 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 arose in the 1980s and 1990s, have more fluid organizational forms, and rely on Islam as a basis for their radical ideology.

The traditional, more-bureaucratic groups have survived to this day partly through support from states such as Syria, Libya, and Iran. The groups retain an ability to train and prepare for terrorist missions; however, 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 (PIJ), Hizbullah, Algeria's Armed Islamic Group (GIA), the Egyptian Islamic Group (IG), and Osama bin Laden's Arab Afghans, have become the most active organizations in and around the Middle East.

The traditional groups. Traditional terrorist groups in the Middle East include the Abu Nidal Organization (ANO), the Popular Front for the Liberation of Palestine (PFLP), and three PFLP-related splinters—the PFLP-General Command (PFLP-GC), the Palestine Liberation Front (PLF), and the Democratic Front for the Liberation of Palestine (DFLP).

The ANO was an integral part of the PLO until it became independent in 1974. It has a bureaucratic structure composed of various

functional committees.[33] The activism it displayed in the 1970s and 1980s has lessened considerably, owing to a lessening of support from state sponsors and to effective counterterrorist campaigns by Israeli and Western intelligence services.[34] The very existence of the organization has recently been put into question, given uncertainty as to the whereabouts and fate of Abu Nidal, the leader of the group.[35]

The PFLP was founded in 1967 by George Habash as a PLO-affiliated organization. It has traditionally embraced a Marxist ideology, and remains an important PLO faction. However, in recent years it has suffered considerable losses from Israeli counterterrorist strikes.[36] The PFLP-General Command split from the PFLP in 1968, and in turn experienced a schism in the mid-1970s. This splinter group, which called itself the PLF, is composed of three subgroups, and has not been involved in high-profile acts since the 1985 hijacking of the Italian cruise ship *Achille Lauro*.[37] The PFLP was subjected to another split in 1969, which resulted in the Democratic Front for the Liberation of Palestine. The DFLP resembles a small army more than a terrorist group—its operatives are organized in battalions, backed by intelligence and special forces.[38] DFLP strikes have become less frequent since the 1970s, and since the late 1980s it has limited its attacks to Israeli targets near borders.[39]

What seems evident here is that this old generation of traditional, hierarchical, bureaucratic groups is on the wane. The reasons are varied, but the point remains—their way of waging terrorism is not likely to make a comeback, and is being superseded by a new way

---

[33]Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism, 1996*, U.S. Department of State, Publication 10433, April 1997.

[34]Loeb, 1998; and John Murray and Richard H. Ward (eds.), *Extremist Groups*, Office of International Criminal Justice, University of Illinois, Chicago, 1996.

[35]Youssef M. Ibrahim, "Egyptians Hold Terrorist Chief, Official Asserts," *New York Times*, August 26, 1998.

[36]Murray and Ward, 1996.

[37]*Patterns of Global Terrorism, 1996*, and Murray and Ward, 1996.

[38]Murray and Ward, 1996.

[39]*Patterns of Global Terrorism, 1995, 1996, 1997.*

that is more attuned to the organizational, doctrinal, and technological imperatives of the information age.

The most active groups and their organization. The new generation of Middle Eastern groups has been active both in and outside the region in recent years. In Israel and the occupied territories, Hamas, and to a lesser extent the Palestinian Islamic Jihad, have shown their strength over the last four years with a series of suicide bombings that have killed more than one hundred people and injured several more.[40] Exploiting a strong presence in Lebanon, the Shi'ite Hizbullah organization has also staged a number of attacks against Israeli Defense Forces troops and Israeli cities in Galilee.[41]

The al-Gama'a al-Islamiya, or Islamic Group (IG), is the most active Islamic extremist group in Egypt. In November 1997 IG carried out an attack on Hatshepsut's Temple in Luxor, killing 58 tourists and 4 Egyptians. The Group has also claimed responsibility for the bombing of the Egyptian embassy in Islamabad, Pakistan, which left 16 dead and 60 injured.[42] In Algeria, the Armed Islamic Group (GIA) has been behind the most violent, lethal attacks in Algeria's protracted civil war. Approximately 70,000 Algerians have lost their lives since the domestic terrorist campaign began in 1992.[43]

Recently, 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

---

[40]For instance, in 1997 Hamas operatives set off three suicide bombs in crowded public places in Tel Aviv and Jerusalem. On March 21, a Hamas satchel bomb exploded at a Tel Aviv cafe, killing three persons and injuring 48; on July 30, two Hamas suicide bombers blew themselves up in a Jerusalem market, killing 16 persons and wounding 178; on September 4, three suicide bombers attacked a Jerusalem pedestrian mall, killing at least five persons (in addition to the suicide bombers), and injuring at least 181. The Palestinian Islamic Jihad has claimed responsibility (along with Hamas) for a bomb that killed 20 and injured 75 others in March 1996, and in 1995 it carried out five bombings that killed 29 persons and wounded 107. See *Patterns of Global Terrorism, 1995, 1996, 1997.*

[41]See "Hizbullah," Israeli Foreign Ministry, April 11, 1996. Available on the Internet at *http://www.israel-mfa.gov.il.*

[42]See *Patterns of Global Terrorism, 1995, 1996, 1997.*

[43]*Patterns of Global Terrorism, 1997.*

Afghanistan[44]—has come to the fore as an active terrorist outfit. One of the leaders and founders of the Arab Afghan movement, Osama bin Laden, a Saudi entrepreneur who bases his activities in Afghanistan,[45] is suspected of sending operatives to Yemen to bomb a hotel used by U.S. soldiers on their way to Somalia in 1992, plotting to assassinate President Clinton in the Philippines in 1994 and Egyptian President Hosni Mubarak in 1995, and of having a role in the Riyadh and Khobar blasts in Saudi Arabia that resulted in the deaths of 24 Americans in 1995 and 1996.[46] U.S. officials have pointed to bin Laden as the mastermind behind the U.S. embassy bombings in Kenya and Tanzania, which claimed the lives of more than 260 people, including 12 Americans.[47]

To varying degrees, these groups share the principles of the networked organization—relatively flat hierarchies, decentralization and delegation of decisionmaking authority, and loose lateral ties among dispersed groups and individuals.[48] For instance, Hamas is loosely structured, with some elements working openly through mosques and social service institutions to recruit members, raise funds, organize activities, and distribute propaganda. Palestinian security sources indicate that there are ten or more Hamas splinter groups and factions with no centralized operational leadership.[49] The Palestine Islamic Jihad is a series of loosely affiliated factions,

---

[44]"Arab Afghans Said to Launch Worldwide Terrorist War," *Paris al-Watan al-'Arabi*, FBIS-TOT-96-010-L, December 1, 1995, pp. 22–24.

[45]William Gertz, "Saudi Financier Tied to Attacks," *Washington Times*, October 23, 1996.

[46]Tim Weiner, "U.S. Sees bin Laden as Ringleader of Terrorist Network," *New York Times*, August 21, 1998; M. J. Zuckerman, "Bin Laden Indicted for Bid to Kill Clinton," *USA Today*, August 26, 1998.

[47]Pamela Constable, "bin Laden 'Is Our Guest, So We Must Protect Him'," *Washington Post*, August 21, 1998.

[48]We distinguish between deliberate and factional decentralization. Factional decentralization—prevalent in older groups—occurs when subgroups separate themselves from the central leadership because of differences in tactics or approach. Deliberate or operational decentralization is what distinguishes netwar agents from others, since delegation of authority in this case occurs because of the distinct advantages this organizational arrangement brings, and not because of lack of consensus. We expect both influences on decentralization to continue, but newer groups will tend to decentralize authority even in the absence of political disagreements.

[49]"Gaza Strip, West Bank: Dahlan on Relations with Israel, Terrorism," *Tel Aviv Yedi'ot Aharonot*, FBIS-TOT-97-022-L, February 28, 1997, p. 18.

rather than a cohesive group.[50] The pro-Iranian Hizbullah acts as an umbrella organization of radical Shiite groups, and in many respects is a hybrid of hierarchical and network arrangements; Although the formal structure is highly bureaucratic, interactions among members are volatile and do not follow rigid lines of control.[51] According to the U.S. Department of State, Egypt's Islamic Group is a decentralized organization that operates without a single operational leader,[52] while the GIA is notorious for the lack of centralized authority.[53]

Unlike traditional terrorist organizations, Arab Afghans are part of a complex network of relatively autonomous groups that are financed from private sources forming "a kind of international terrorists' Internet."[54] The most notorious element of the network is Osama bin Laden, who uses his wealth and organizational skills to support and direct a multinational alliance of Islamic extremists. At the heart of this alliance is his own inner core group, known as Al-Qaeda ("The Base"), which sometimes conducts missions on its own, but more often in conjunction with other groups or elements in the alliance. 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 such a holy war will be fought by irregular, light, highly mobile forces using guerrilla tactics.[55]

---

[50]The leader of the PIJ's most powerful faction, Fathi Shaqaqi, was assassinated in October 1995 in Malta, allegedly by the Israeli Mossad. Shaqaqi's killing followed the assassination of Hani Abed, another PIJ leader killed in 1994 in Gaza. Reports that the group has been considerably weakened as a result of Israeli counterleadership operations are balanced by the strength demonstrated by the PIJ in its recent terrorist activity. See "Islamic Group Vows Revenge for Slaying of Its Leader," *New York Times*, October 30, 1995, p. 9.

[51]Magnus Ranstorp, "Hizbullah's Command Leadership: Its Structure, Decision-Making and Relationship with Iranian Clergy and Institutions," *Terrorism and Political Violence*, Vol. 6, No. 3, Autumn 1994, p. 304.

[52]*Patterns of Global Terrorism, 1996.*

[53]"Algeria: Infighting Among Proliferating 'Wings' of Armed Groups," *London al-Sharq al-Aswat*, FBIS-TOT-97-021-L, February 24, 1997, p. 4.

[54]David B. Ottaway, "US Considers Slugging It Out With International Terrorism," *Washington Post*, October 17, 1996, p. 25.

[55]"Saudi Arabia: Bin-Laden Calls for 'Guerrilla Warfare' Against US Forces," *Beirut Al-Diyar*, FBIS-NES-96-180, September 12, 1996.

Even though bin Laden finances Arab Afghan activities and directs some operations, he apparently does not play a direct command and control role over all operatives. Rather, he is a key figure in the coordination and support of several dispersed activities.[56] For instance, bin Laden founded the "World Islamic Front for Jihad Against Jews and Crusaders."[57] And yet most of the groups that participate in this front (including Egypt's Islamic Group) remain independent, although the organizational barriers between them are fluid.[58]

From a netwar perspective, an interesting feature of bin Laden's Arab Afghan movement is its ability to relocate operations swiftly from one geographic area to another in response to changing circumstances and needs. Arab Afghans have participated in operations conducted by Algeria's GIA and Egypt's IG. Reports in 1997 also indicated that Arab Afghans transferred training operations to Somalia, where they joined the Islamic Liberation Party (ILP).[59] The same reports suggest that the Arab Afghan movement has considered sending fighters to Sinkiang Uighur province in western China, to wage a holy war against the Chinese regime.[60] This group's ability to move and act quickly (and, to some extent, to swarm) once opportunities emerge hampers counterterrorist efforts to predict its actions and monitor its activities. The fact that Arab Afghan operatives were able to strike the U.S. embassies in Kenya and Tanzania substantiates the claim that members of this network have the mobility and speed to operate over considerable distances.

---

[56]It is important to avoid equating the bin Laden network solely with bin Laden. He represents a key node in the Arab Afghan terror network, but there should be no illusions about the likely effect on the network of actions taken to neutralize him. 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.

[57]"Militants Say There Will Be More Attacks Against U.S.," *European Stars and Stripes*, August 20, 1998.

[58]For instance, there have been reports of a recent inflow of Arab Afghans into Egypt's Islamic Group to reinforce the latter's operations. See Murray and Ward, 1996, and "The CIA on Bin Laden," *Foreign Report*, No. 2510, August 27, 1998, pp. 2–3.

[59]This move was also influenced by the Taliban's decision to curb Arab Afghan activities in the territory under its control as a result of U.S. pressure. See "Arab Afghans Reportedly Transfer Operations to Somalia," *Cairo al-Arabi*, FBIS-TOT-97-073, March 10, 1997, p. 1.

[60]"Afghanistan, China: Report on Bin-Laden Possibly Moving to China," *Paris al-Watan al-'Arabi*, FBIS-NES-97-102, May 23, 1997, pp. 19–20.

Although the organizational arrangements in these groups do not match all the basic features of the network ideal,[61] they stand in contrast to more traditional groups. Another feature that distinguishes the newer generation of terrorist groups is their adoption of information technology.

Middle Eastern Terrorist Groups and the Use of Information Technology

Information technology (IT) is an enabling factor for networked groups; terrorists aiming to wage netwar may adopt it not only as a weapon, but also to help coordinate and support their activities. Before exploring how Middle Eastern terrorist groups have embraced the new technology, we posit three hypotheses that relate the rise of IT to organization for netwar:

- The greater the degree of organizational networking in a terrorist group, the higher the likelihood that IT is used to support the network's decisionmaking.
- Recent advances in IT facilitate networked terrorist organizations because information flows are becoming quicker, cheaper, more secure, and more versatile.
- As terrorist groups learn to use IT for decisionmaking and other organizational purposes, they will be likely to use the same technology as an offensive weapon to destroy or disrupt.

Middle Eastern terrorist groups provide examples of information technology being used for a wide variety of purposes. As discussed below, there is some evidence to support the claim that the most active groups—and therefore the most decentralized groups—have embraced information technology to coordinate activities and dis-

[61]While it is possible to discern a general trend toward an organizational structure that displays several features of a network, we expect to observe substantial differences (and many hierarchy/network hybrids) in how organizations make their specific design choices. Different network designs depend on contingent factors, such as personalities, organizational history, operational requirements, and other influences such as state sponsorship and ideology.

seminate propaganda and ideology.[62] 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.[63]

Arab Afghans appear 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 computers, communications equipment, and a large number of disks for data storage.[64] 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 the extremists can exchange information without running a major risk of being intercepted by counterterrorism officials.[65]

Hamas is another major group that uses the Internet to share operational information. Hamas activists in the United States use chat rooms to plan operations and activities.[66] 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 it is next to impossible for counterterrorism intelli-

---

[62]Assessing the strength of the relationship between organizational structure and use of information technology is difficult to establish. Alternative explanations may exist as to why newer groups would embrace information technology, such as age of the group (one could speculate that newer terrorist groups have on average younger members, who are more familiar with computers), or the amount of funding (a richer group could afford more electronic gadgetry). While it is empirically impossible to refute these points, much in organization theory supports our hypothesis that there is a direct relationship between a higher need for information technology and the use of network structures.

[63]"Saudi Arabia: French Analysis of Islamic Threat," *Paris al-Watan al-'Arabi*, FBIS-NES-97-082, April 11, 1997, pp. 4–8.

[64]"Afghanistan, Saudi Arabia: Editor's Journey to Meet Bin-Laden Described," *London al-Quds al-'Arabi*, FBIS-TOT-97-003-L, November 27, 1996, p. 4.

[65]"Arab Afghans Said to Launch Worldwide Terrorist War," 1995.

[66]"Israel: U.S. Hamas Activists Use Internet to Send Attack Threats," *Tel Aviv IDF Radio*, FBIS-TOT-97-001-L, 0500 GMT October 13, 1996.

gence to monitor accurately the flow and content of Internet traffic. Israeli security officials have difficulty in tracing Hamas messages and decoding their content.[67]

During a recent counterterrorist operation, several GIA bases in Italy were uncovered, and each was found to include computers and diskettes with instructions for the construction of bombs.[68] It has been reported that the GIA uses floppy disks and computers to store and process instructions and other information for its members, who are dispersed in Algeria and Europe.[69] Furthermore, the Internet is used as a propaganda tool by Hizbullah, which manages three World Wide Web sites—one for the central press office (at www.hizbollah.org), another to describe its attacks on Israeli targets (at www.moqawama.org), and the last for news and information (at www.almanar.com.lb).[70]

The presence of Middle Eastern terrorist organizations on the Internet is suspected in the case of the Islamic Gateway, a World Wide Web site that contains information on a number of Islamic activist organizations based in the United Kingdom. British Islamic activists use the World Wide Web to broadcast their news and attract funding; they are also turning to the Internet as an organizational and communication tool.[71] While the vast majority of Islamic activist groups represented in the Islamic Gateway are legitimate, one group—the Global Jihad Fund—makes no secret of its militant goals.[72] The appeal of the Islamic Gateway for militant groups may be enhanced by a representative's claim, in an Internet Newsnet article in August 1996, that the Gateway's Internet Service Provider

---

[67]"Israel: Hamas Using Internet to Relay Operational Messages," *Tel Aviv Ha'aretz*, FBIS-TOT-98-034, February 3, 1998, p. 1.

[68]"Italy: Security Alters Following Algerian Extremists' Arrests," *Milan Il Giornale*, FBIS-TOT-97-002-L, November 12, 1996, p. 10.

[69]"Italy, Vatican City: Daily Claims GIA 'Strategist' Based in Milan," *Milan Corriere della Sera*, FBIS-TOT-97-004-L, December 5, 1996, p. 9.

[70]"Hizbullah TV Summary 18 February 1998," *Al-Manar Television World Wide Webcast*, FBIS-NES-98-050, February 19, 1998. Also see "Developments in Mideast Media: January–May 1998," Foreign Broadcast Information Service (FBIS), May 11, 1998.

[71]"Islamists on Internet," FBIS Foreign Media Note-065EP96, September 9, 1996.

[72]"Islamic Activism Online," FBIS Foreign Media Note-02JAN97, January 3, 1997.

(ISP) can give "CIA-proof" protection against electronic surveillance.[73]

Summary Comment

This review of patterns and trends in the Middle East substantiates our speculations that the new terrorism is evolving in the direction of netwar, along the following lines:[74]

- An increasing number of terrorist groups are adopting networked forms of organization and relying on information technology to support such structures.
- Newer groups (those established in the 1980s and 1990s) are more networked than traditional groups.
- A positive correlation is emerging between the degree of activity of a group and the degree to which it adopts a networked structure.[75]
- Information technology is as likely to be used for organizational support as for offensive warfare.
- The likelihood that young recruits will be familiar with information technology implies that terrorist groups will be increasingly

---

[73]The Muslim Parliament has recently added an Internet Relay Chat (IRC) link and a "Muslims only" List-Serve (automatic e-mail delivery service). See "Islamic Activism Online," FBIS Foreign Media Note-02JAN97, January 3, 1997.

[74]Similar propositions may apply to varieties of netwar other than the new terrorism.

[75]We make a qualification here. There appears to be a significant positive association between the degree to which a group is active and the degree to which a group is decentralized and networked. But we cannot be confident about the causality of this relationship or its direction (i.e., whether activity and strength affect networking, or vice-versa). A host of confounding factors may affect both the way groups decide to organize and their relative success at operations. For instance, the age of a group may be an important predictor of a group's success—newer groups are likely to be more popular; popular groups are more likely to enlist new operatives; and groups that have a large number of operatives are likely to be more active, regardless of organizational structure. Another important caveat is related to the fact that it is difficult to rank groups precisely in terms of the degree to which they are networked, because no terrorist organization is thought to represent either a hierarchical or network ideal-type. While the conceptual division between newer-generation and traditional groups is appropriate for our scope here, an analytical "degree of networking" scale would have to be devised for more empirical research.

networked and more computer-friendly in the future than they are today.

TERRORIST DOCTRINES—THE RISE OF A "WAR PARADIGM"

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 kinds of 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 upon the choices terrorists make as to the overall doctrinal paradigms that shape their goals and strategies.

At least three terrorist paradigms are worth considering: terror as coercive diplomacy, terror as war, and terror as the harbinger of a "new world." These three engage, in varying ways, distinct rationales for terrorism—as a weapon of the weak, as a way to assert identity, and as a way to break through to a new world—discussed earlier in this chapter. While there has been much debate about the overall success or failure of terrorism,[76] 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, whereas norms of "war" often imply maximizing destruction.

The Coercive-Diplomacy Paradigm

The first paradigm is that of coercive diplomacy. From its earliest days, terrorism has often sought to persuade others, by means of symbolic violence, either to do something, stop doing something, or undo what has been done. These are the basic forms of coercive diplomacy,[77] and they appear in terrorism as far back as the Jewish

---

[76]See, for instance, William Gutteridge (ed.), *Contemporary Terrorism*, Facts on File, Oxford, England, 1986; Hoffman and Carr, 1997; and Combs, 1997.

[77]See Alexander George and William Simons, *The Limits of Coercive Diplomacy*, Westview Press, Boulder, 1994.

Sicarii Zealots who sought independence from Rome in the first century AD, up through the Palestinians' often violent acts in pursuit of their independence today.

The fact that terrorist coercion includes violent acts does not make it a form of war—the violence is exemplary, designed to encourage what Alexander George calls "forceful persuasion," or "coercive diplomacy as an alternative to war."[78] In this light, terrorism may be viewed as designed to achieve specific goals, and the level of violence is limited, or proportional, to the ends being pursued. Under this paradigm, terrorism was once thought to lack a "demand" for WMD, as such tools would provide means vastly disproportionate to the ends of terror. This view was first elucidated over twenty years ago by Brian Jenkins—though there was some dissent expressed by scholars such as Thomas Schelling—and continued to hold sway until a few years ago.[79]

The War Paradigm

Caleb Carr, surveying the history of the failures of coercive terrorism and the recent trends toward increasing destructiveness and deniability, has elucidated what we call a "war paradigm."[80] This paradigm, which builds on ideas first considered by Jenkins,[81] holds that terrorist acts arise when weaker parties cannot challenge an adversary directly and thus turn to asymmetric methods. A war paradigm implies taking a strategic, campaign-oriented view of violence that makes no specific call for concessions from, or other demands upon, the opponent. Instead, the strategic aim is to inflict damage, in the context of what the terrorists view as an ongoing war. In theory, this paradigm, unlike the coercive diplomacy one, does not seek a proportional relationship between the level of force em-

---

[78]Alexander George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*, United States Institute of Peace Press, Washington, DC, 1991.

[79]Brian Jenkins, *The Potential for Nuclear Terrorism*, RAND, P-5876, 1977; Thomas Schelling, "Thinking about Nuclear Terrorism," *International Security*, Vol. 6, No. 4, Spring 1982, pp. 68–75; and Patrick Garrity and Steven Maaranen, *Nuclear Weapons in a Changing World*, Plenum Press, New York, 1992.

[80]Carr, 1996.

[81]Brian Jenkins, *International Terrorism: A New Kind of Warfare*, RAND, P-5261, 1974.

ployed and the aims sought. When the goal is to inflict damage generally, and the terrorist group has no desire or need to claim credit, there is an attenuation of the need for proportionality—the worse the damage, the better. Thus, the use of WMD can be far more easily contemplated than in a frame of reference governed by notions of coercive diplomacy.

A terrorist war paradigm may be undertaken by terrorists acting on their own behalf or in service to a nation-state. In the future, as the information age brings the further empowerment of nonstate and transnational actors, "stateless" versions of the terrorist war paradigm may spread. At the same time, however, states will remain important players in the war paradigm; they may cultivate their own terrorist-style commandos, or seek cut-outs and proxies from among nonstate terrorist groups.

Ambiguity regarding a sponsor's identity may prove a key element of the war paradigm. While the use of proxies provides an insulating layer between a state sponsor and its target, these proxies, if captured, may prove more susceptible to interrogation and investigative techniques designed to winkle out the identity of the sponsor. On the other hand, while home-grown commando-style terrorists may be less forthcoming with information if caught, their own identities, which may be hard to conceal, may provide undeniable evidence of state sponsorship. These risks for states who think about engaging in or supporting terrorism may provide yet more reason for the war paradigm to increasingly become the province of nonstate terrorists—or those with only the most tenuous linkages to particular states.

Exemplars of the war paradigm today are the wealthy Saudi jihadist, Osama bin Laden, and the Arab Afghans that he associates with. As previously mentioned, bin Laden has explicitly called for war-like terrorism against the United States, and especially against U.S. military forces stationed in Saudi Arabia. President Clinton's statement that American retaliation for the U.S. embassy bombings in East Africa represented the first shots in a protracted war on terrorism suggests that the notion of adopting a war paradigm to counter terror has gained currency.

The New-World Paradigm

A third terrorist paradigm aims at achieving the birth of what might be called a "new world." It may be driven by religious mania, a desire for totalitarian control, or an impulse toward ultimate chaos.[82] Aum Shinrikyo would be a recent example. The paradigm harks back to the dynamics of millennialist movements that arose in past epochs of social upheaval, when *prophetae* attracted adherents from the margins of other social movements and led small groups to pursue salvation by seeking a final, violent cataclysm.[83]

This paradigm is likely to seek the vast disruption of political, social, and economic order. Accomplishing this goal may involve lethal destruction, even a heightened willingness to use WMD. Religious terrorists may desire destruction for its own sake, or for some form of "cleansing." But the ultimate aim is not so much the destruction of society as a rebirth after a period of chaotic disruption.

The Paradigms and Netwar

All three paradigms offer room for netwar. Moreover, all three paradigms allow the rise of "cybotage"—acts of disruption and destruction against information infrastructures by terrorists who learn the skills of cyberterror, as well as by disaffected individuals with technical skills who are drawn into the terrorist milieu. However, we note that 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. Our netwar perspective accepts this, but also holds that some terrorist netwars will stress disruption over destruction. Networked terrorists will no doubt continue to destroy things and kill people, but their principal strategy may move toward the nonlethal

---

[82]For a discussion of these motives, see Laqueur, 1996; Iklé, 1997; and Hoffman, 1998, respectively.

[83]See, for instance, Michael Barkun, *Disaster and the Millennium*, Yale University Press, New Haven, 1974; and Norman Cohn, *The Pursuit of the Millennium: Revolutionary Messianism in Medieval and Reformation Europe and Its Bearing on Modern Totalitarian Movements*, Harper Torch Books, New York, 1961.

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 the fact that trainees for suicide bombings are kept from listening to international media, through the ways that terrorists seek to create disasters that will consume 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 one most relevant to and dangerous from the standpoint of the military. Indeed, if terrorists perceive themselves as warriors, they may be inclined to target enemy military assets or interests.

INFORMATION-AGE TERRORISM AND THE U.S. AIR FORCE

Terrorists, especially those operating under a war paradigm, have every reason to seek out and target U.S. military personnel, installations, and equipment. The inability to pose direct opposition to American power may stimulate ethno-nationalist and religious revivalist movements—both types of actors may feel inherently threatened by the preeminent position of the United States in current world politics. Using a war paradigm allows terrorists an easy rationale for striking at American power, even in the absence of specific demands and without the need to claim credit for actions. Further, the high profile of the Air Force suggests that attacks upon it will be a way to grab worldwide public attention and strike at what is perceived, by some, to be a "conditionally fragile" American public ability to accept losses and casualties.[84]

---

[84]Eric V. Larson, *Casualties and Consensus: The Historical Role of Casualties in Domestic Support for U.S. Military Operations*, RAND, MR-726-RC, 1996.

The U.S. Air Force, which in many ways epitomizes American power—as the Royal Navy did in the heyday of British Empire—has symbolic value as a target of terror. It also has expensive and sophisticated equipment that increases its attractiveness to the terrorist. Further, air assets are a quintessential element of the balance of power in any region of the world, as they are an available form of American military power that may be exercised in support of U.S. interests. Given a U.S. air mastery that precludes direct challenges, a terrorist commando strategy against U.S. air assets might prove an attractive option for potential adversaries.

This option poses the prospect of a campaign with low costs and risks—much like the British use of the Special Air Service (SAS) in North Africa during World War II. In that campaign, British commandos were sent against Luftwaffe airbases, destroying over 400 aircraft between 1941 and 1943 and helping to mitigate the effects of German air superiority early in the desert war with deep strikes of up to 400 miles behind the front.[85] This irregular approach to weakening an enemy's air power has remained a vibrant strand in British strategic thought, and the SAS would reprise its role in the 1982 Falklands War, most notably by destroying 11 Argentine ground-attack aircraft in the raid on Pebble Island.[86] The potential of this type of threat to USAF bases has been acknowledged, and mitigation measures explored, in recent studies on ground-based threats to airbases.[87]

For the USAF, the prospect of terrorist attack exists across the spectrum of operations and across the types of asset—from personnel to equipment, and, increasingly, against command and control nodes.

---

[85]Paul Carell, *The Foxes of the Desert,* E. P. Dutton, New York, 1960, pp. 47–49.

[86]See Max Hastings and Simon Jenkins, *The Battle for the Falklands,* W. W. Norton, New York, 1983, pp. 186–187; Anthony Cordesmann, and Abraham Wagner, *The Lessons of Modern War,* Vol. 3, *The Afghan and Falklands Conflicts,* Westview Press, Boulder, Colorado, 1990. p. 305; and Bruce W. Watson and Peter M. Dunn (eds.), *Military Lessons of the Falklands Islands War,* Westview Press, Boulder, Colorado, 1984, pp. 153–154. For a comprehensive study of ground attacks on airbases, see Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases,* RAND, MR-553-AF, 1995, who chronicles the events that resulted in destruction of over 2000 aircraft on the ground between 1940 and 1992.

[87]See David A. Shlapak and Alan Vick, *Check Six Begins on the Ground: Responding to the Evolving Ground Threat to U.S. Air Force Bases,* RAND, MR-606-AF, 1995.

In peacetime, for example, the USAF plays a key role in maintaining a sense of American presence around the world. It is often a part of shows of force, and is an element in the American grand strategy of being open to the world regarding its military prowess—an important part of extending deterrent protection to U.S. friends and allies. Small-scale contingencies (SSC) range, on their lower-intensity end of the spectrum, from humanitarian aid delivery to peace enforcement (e.g., of "no fly" zones). Finally, the USAF will always play a key role in major theater wars (MTW), shoring up indigenous forces and multiplying the strength of other American military forces arriving in theater. U.S. air power, in this last category, may be the only viable hope of slowing down a numerically superior aggressor—and the aggressor may realize this, raising his interest in a terrorist commando strategy against the USAF.

Toward a New USAF Strategy for Coping with Information-Age Terrorism

At the most basic level, USAF strategy needs to have both defensive (antiterrorist) and proactive (counterterrorist) components. Measures must be devised to protect forces stationed at home and abroad, to strike targets belonging to groups or their sponsors, and to gather intelligence on imminent attacks or other terrorist group activities. More specifically, the USAF strategy against terrorism should encompass four generic missions:

- General, "political" deterrence
- Interdiction and strike
- Intelligence gathering
- Force protection.

General deterrence relates to the USAF's ability to prevent further terrorist actions by striking (or threatening to strike) those targets of most value to the political supporters of a given group; interdiction and strike refer to the tactical use of USAF assets in the pursuit of terrorist attackers, as well as for retaliatory response. Intelligence gathering finds information about imminent terrorist attacks and identifies terrorist group weaknesses. As its name suggests, force

protection concerns the security and safety of USAF personnel, plants, and equipment.

Each mission has different implications for how the Air Force responds to the terrorist threat. Greater emphasis on force protection, for instance, would place more weight on defensive antiterrorism. The deterrence and strike missions are inherently more proactive, while intelligence gathering can serve the causes of both anti- and counterterrorism.

The foregoing suggests that the USAF should adopt a balanced approach that emphasizes all four missions to achieve an offensive/defensive blend that can defend against and counter information-age terrorism.

Mitigation Measures

The USAF must devise measures to protect personnel, equipment and installations, and C2 nodes.

First, in the face of a significant increase in terrorist attacks (conventional or WMD) on USAF personnel and assets overseas, the USAF might consider shifting away from forward basing as much as possible, returning to forces based in the continental United States (CONUS) but with a wide network of dormant bases in the regions of interest. The principle here is similar to that articulated by Albert Wohlstetter et al. in their classic study of forward-based bomber vulnerability to surprise attack—the further forward, the more vulnerable the bombers.[88] In the future, if the terrorist threat grows substantially, a similar basing solution might be applicable. Such an option would dovetail neatly with emerging USAF doctrine regarding the surging forward of air expeditionary forces in crisis and war. While it may be difficult to secure access to a large number of bases, the redundancy created by this option would make it difficult for terrorists to predict which dormant bases to target prior to a deployment, and would help the USAF to remain engaged in key regions through "virtual presence."

---

[88]Albert Wohlstetter, F. Hoffman, R. J. Lutz, and H. S. Rowen, *Selection and Use of Strategic Air Bases*, RAND, R-266, 1954.

As attractive as moving to a preponderantly CONUS-based force might be under some circumstances, it would present a number of problems. First, there would be costs and risks to regional stability engendered by a lack of U.S. presence. For example, the USAF has been the principal stabilizer for Kuwait in the Persian Gulf region since the end of the war. Air assets are often crucial for deterrence and defense; when deterrence fails, it takes time to muster American ground and naval forces for a response. Therefore, when forward basing is deemed absolutely necessary for crisis stability, or for peace operations (e.g., "no fly" zones), the host nation must be made aware of USAF security requirements and allow the USAF an active role in preparing its antiterrorist defenses.

Also, the USAF might explore developing standardized doctrine regarding antiterrorism—perhaps along the lines of the general guidance that is provided by the Joint Staff.[89] Clearly, different regional settings impose differing security requirements, but the USAF can develop a body of generalizable thought to impart to base commanders and others charged with securing USAF assets and personnel overseas. Our research has revealed a wide variance in views about base and personnel security, as well as widely differing levels of concern about the problem.

With regard to forward basing, one must consider the risk of terrorist attack on prepositioned supplies and ordnance. The simplest solution is to move as much prepositioned equipment out to sea as possible, a step that the USAF has already partially taken. However, this approach then subjects the USAF to the same problem that the U.S. Navy has in terms of response time—the need to wait for the arrival of ships, which will, generally, take some days to reach the region in question. Depending on the weakness of the American ally in the regional setting, a delay of days can be critical. Maritime prepositioning squadrons will not provide an overall solution, but they may provide a useful hedge in a prepositioning scheme that includes both ground-based materials and those kept afloat.[90]

---

[89]Joint Staff, *Joint Tactics, Techniques and Procedures for Antiterrorism*, JP 3-07.2, March 1998.

[90]On the theme of maritime prepositioning, it might also be useful to think about the concept of mobile, floating airbases. These would be like the mobile, large islands (MOLIs) first discussed during the Cold War (see P. M. Dadant, A. A. Barbour, W. E.

The second deficiency with CONUS-basing as a solution lies in the nature of terrorist IW, which is not limited by geographical concerns. Indeed, in some respects, the highly internetted U.S. information infrastructure might make access to USAF C2 nodes easier than if an airbase were located in the northern desert of Saudi Arabia. How, then, should the terrorist information warfare threat be defended against? A simple solution is to avoid becoming too interconnected to the global information infrastructure. The USAF currently retains the robust, dedicated C2 system that it needed to operate under the most trying conditions (i.e., protracted nuclear war), so perhaps the answer lies in *not* interconnecting all sensitive communications as rapidly as possible. Paradoxically, less modernization may make for more security in some cases.

Moving toward more advanced electronic interconnectivity might undermine the security and safety of the current system, opening up a window of opportunity for cyberterror. The problem of increasing modernization and complexity is noted by Perrow and Sagan.[91]

Proactive Counterterrorism and the USAF

If terrorists are moving toward a war paradigm, then it may be appropriate for the targeted to move to a war paradigm of their own. Indeed, President Clinton deliberately invoked the language and imagery of a war paradigm in his public comments on the reasons for retaliating with missile attacks against the terrorists responsible for the 1998 U.S. embassy bombings in East Africa. The adoption of a war paradigm by the U.S. armed forces would carry deep political

---

Mooz, and J. K. Walker, *A Comparison of Methods for Improving U.S. Capability to Project Ground Forces to Southwest Asia in the 1990s*, RAND, R-2963-AF, 1984) that were envisioned to have a movement capability of some three knots per hour. MOLIs would solve the problem of where to preposition supplies, and they would reduce the vulnerability of forward-based air power to terrorist attack. MOLIs are limited to the sea, so airbases would necessarily have inherent limits on their placement. MOLIs could defend against some forms of terrorist attack but might be lucrative targets of assault by regional navies using swift missile boats. Finally, the MOLI could be an attractive target for a tactical WMD. Despite its weaknesses, the MOLI concept might have more appeal in the case of a substantial rise in terrorist activity, or in those areas where local military and WMD threats are deemed low.

[91]Charles Perrow, *Normal Accidents: Living with High-Risk Technologies*, Basic Books, New York, 1984, and Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton University Press, Princeton, New Jersey, 1993.

and security implications, especially in terms of how other countries and terrorist groups view American power. For instance, one could argue that a war paradigm would result in more unilateral U.S. actions to counter terrorism, and that increased reliance on unilateral force might create tension with allies. Also, more frequent "acts of war" against terrorism may only embolden terrorists, and encourage an increasingly destructive action-reaction process.

Examining the full impact of the adoption of a war paradigm is beyond our scope here, and a recommendation for a war paradigm must be backed by further analysis. What we are proposing is that the USAF consider adopting some principles of the war paradigm in how it defends against and counters terrorism.

If we assume—and this is an uncertain assumption—that terrorist targets can be indisputably identified, then the USAF would be suited to key missions should the United States adopt a war paradigm. Air power offers a flexible, timely strike capability, including a new generation of highly discriminate weapons. It also affords the least politically risky of the military options for striking back at terror, because it does not entail putting troops on the ground or moving significant naval assets in harm's way. Moreover, the high speed of response associated with air power will become increasingly important as terrorists acquire the capabilities to move swiftly from one theater to another and to attack with little or no warning. Thus, the USAF, with the strike capabilities afforded by air-launched cruise missiles and other smart munitions, should be considered a natural, leading element in any proactive strategy for countering terror. Beyond direct bombardment, the USAF can provide tactical mobility for special forces teams—and give them close support—should they be called upon to strike directly at key terrorist nodes.

There are three fundamental ways in which air power could support a counterterrorist war paradigm. First, the USAF could play a major role in coercive diplomatic campaigns against state sponsors of terror, along the lines of the use of air power against Qaddafi in the 1986 air raid on Tripoli or the 1998 Tomahawk strikes in Sudan and Afghanistan.[92] Another possibility is that, instead of being used for

[92]Refer to Carr, 1996, and Hoffman and Carr, 1997, for a discussion of this issue.

coercive diplomacy, the USAF could be employed for either preemptive or preventive[93] strikes against terrorist or state-sponsored sites that foment terror (such as deep underground facilities where WMD might be produced). Finally, the USAF could be the key link, along with special forces, in an information war against the terrorists in terms of both striking at the key telecommunications nodes of terrorists, and gaining information about them via IW means.[94]

The last point merits some discussion. It is commonly argued that national technical means (NTM) of intelligence gathering are aimed at Cold War-era targets (i.e., tanks, planes, silos, etc.), and are therefore poorly suited to the needs of counterterrorism. This has led to calls for greater reliance upon human intelligence (humint) in dealing with terror. Humint is carried out by human operatives often working under cover or as double agents. Unfortunately, there are two principal limitations on the usefulness of humint regarding terrorists. First, organizations such as Hamas frequently recruit members when they are quite young, precluding infiltration of seasoned agents and making it more difficult to sway existing members or convince them to give up information. Second, advancing in a terrorist organization may require committing violent acts, including murder, which are incompatible with accepted Western intelligence practices. The source's reliability will always be in question, both in terms of the inherent risks of dealing with double agents and the likelihood that views expressed by the source are skewed by personal hatreds, rivalries, or mental instability. For these reasons, it is ill-advised to pin significant hopes on the development of sufficient humint sources to wage an effective counterterrorist campaign.

Instead, it may prove optimal to tailor NTM to the new needs of countering terror, relying less on satellite surveillance and perhaps rather more on drones and other pilotless craft capable of listening in

---

[93]Preemption refers to striking first in anticipation of an incipient attack. Prevention means striking before the opponent develops the capability to attack. For example, the Israeli Six Day War of 1967 was preemptive, in that the Israelis struck in anticipation of an attack. The Israeli air raid on Osirak in 1981 was preventive, because it was a strike to prevent Iraq from obtaining a nuclear capability.

[94]See John Arquilla, *From Troy to Entebbe: Special Operations in Ancient and Modern Times,* University Press of America, Lanham, Maryland, 1996, pp. 278–280.

on terrorists' increasingly advanced telecommunications. Coupling this with a joint IW capability for penetrating terrorist C2 nodes might well create a form of "virtual humint"[95] that will prove a key to counterterrorist strategy—and provide a new concept for the intelligence community. The approach will emphasize intelligence gathering by orbital assets or by human assets on the ground. But beyond the technological aspects of this form of counterterrorism, it will be crucial to rethink how to target terrorist groups. We next discuss how U.S. strategy might evolve.

Targeting Terrorists in the Information Age

The transition from hierarchical to networked terrorist groups is likely to be uneven and gradual. The netwar perspective suggests that, for the foreseeable future, various networked forms will emerge, coexisting with and influencing traditional organizations. Such organizational diversity implies the need for a counterterrorism strategy that recognizes the differences among organizational designs and seeks to target the weaknesses associated with each.

Counterleadership strategies or retaliation directed at state sponsors may be effective for groups led by a charismatic leader who enjoys the backing of sympathetic governments, but are likely to fail if used against an organization with multiple, dispersed leaders and private sources of funding. Networked organizations rely on information flows to function, and disruption of the flows cripples their ability to coordinate actions. It is no coincidence, for instance, that while the separation between Hamas political and military branches is well documented, this terrorist group jealously guards information on the connections and degree of coordination between the two.[96]

At the same time, the two-way nature of connectivity for information networks such as the Internet implies that the dangers posed by information warfare are often symmetric—the degree to which a terrorist organization uses information infrastructure for offensive purposes may determine its exposure to similar attacks by

---

[95]We are indebted to colleague Ian Lesser for this creative term.

[96]Bluma Zuckerbrot-Finkelstein, "A Guide to Hamas," *Internet Jewish Post*, available at *http://www.jewishpost.com/jewishpost/jp0203/jpn0303.htm*.

countering forces. While it is true that terrorist organizations will often enjoy the benefit of surprise, the IW tactics available to them can also be adopted by counterterrorists.

The key task for counterterrorism, then, is the identification of organizational and technological terrorist networks. Once such structures are identified, it may be possible to insert and disseminate false information, overload systems, misdirect message traffic, preclude access, and engage in other destructive and disruptive activities to hamper and prevent terrorist operations.

POLICY IMPLICATIONS AND CONCLUSIONS FOR THE USAF

The USAF can take various steps to effectively defend against and counter terrorism that is guided by a war paradigm. Defensive ideas and options might include:

1. *Do not modernize all communications nodes.* The USAF's C2 system is robust—it is designed to withstand the strains of protracted nuclear war—and full interconnectivity may in fact allow cyberterrorists to enter where they could not in the old C2 structure.

2. *Develop defensive antiterror standards for all operating bases and across mission types.* The standards should guarantee safety without constraining flexibility in varied settings; the standards may be more rigid in peacetime and in OOTW than in wartime.

3. *If terrorism worsens, increase reliance on CONUS basing and a wide network of dormant bases to reduce vulnerability of forward-based elements to a terrorist commando strategy.* While likely to make terrorism against USAF personnel and equipment more difficult, increased CONUS basing will be controversial because it entails military and political costs. First, general (i.e., ongoing peacetime) deterrence stability may suffer from the diminution of USAF presence abroad. With decreased deterrence there may be political fallout resulting from a dramatic withdrawal from key regions such as Europe. Third, terrorists might portray such redeployments as a "retreat" that they had caused, and a great victory over American power. Fourth, CONUS basing does not limit exposure to terrorist information warfare, and the risk of suffering delays in the "just in time" deployment process may increase. These downside factors

may be mitigated, however, by negotiating with friendly countries in key regions for access to bases that would be used only in times of crisis or for occasional engagement activities. Such an option would allow for prompt demonstration or deployment of USAF assets in crisis to shore up deterrence; and regular exercises in forward areas would show that USAF reach remains extensive and that terrorism has in no way forced a retreat. Finally, defense against terrorist information warfare would both enable and support CONUS basing.

For proactive counterterrorism, the USAF might consider the following:

4. *At the doctrinal level, consider development of a war paradigm to counter the activities of groups that see themselves as waging war against the United States.* This implies extending the list of what the USAF considers targets, to include more new-generation targets such as key nodes and the network itself. The adoption of a war paradigm may extend to the need for weapons designed to disrupt terrorist information flows, especially high-energy radio-frequency (HERF) and high-power microwave (HPM) weapons. The political and security implications of the adoption of such a paradigm would be profound, perhaps profoundly controversial—and need to be factored into future analyses.

5. *At the organizational level, deepen interservice and interagency networking.* The USAF is a principal actor in a counterterrorist war paradigm, and it should be a key node in an intergency network. As noted earlier, it may take networks to fight networks—and whoever masters the network form of organization will gain the greatest advantages.[97] Countering terror will require the formation of highly effective interagency and interservice mechanisms and command structures.

6. *In the intelligence realm, develop requirements for counterterrorist operations.* The USAF has a unique operating position in the area between orbital intelligence assets and humint, neither of which is likely to be effective against information-age terror. The Air Force might develop a form of "virtual humint" based on both hacking into

[97]See Arquilla and Ronfeldt, 1997; also, John Deutch, "Terrorism: Think Again," *Foreign Policy*, Fall 1997, pp. 10–20.

terrorist telecommunications nets and developing capabilities for reading "emanations" (communications read off of terrorist computer screens before they are encrypted). The latter capability would likely require use of very small unmanned aerial vehicles (UAVs) that are teleoperated by USAF information warfare personnel. In developing a capability of this sort, the Air Force would have to remain mindful of international legal constraints on such data "snooping."

7. *Continue planning for traditional operations such as raiding key terrorist nodes (in particular, deep underground [DUG] facilities that might produce weapons of mass destruction).* This, a key element of an eventual counterterrorist war paradigm, would require careful nodal analysis of terrorist groups to inform the campaign planning process.

The seven recommendations above are grouped according to their contribution to the four generic missions in Table 1.

These policy recommendations affect all the USAF missions, so that a balanced approach is achieved. A comprehensive counterterrorism policy ensures that the USAF can leverage its capabilities to the greatest extent while targeting the "soft spots" of information-age terrorist groups. However, the rise of networked terrorist organizations calls for a change in the analysis of terrorist groups. Analysts

Table 1

USAF Generic Counterterrorism Missions and Policy Recommendations

Mission	Recommendation
Political deterrence	Plan for traditional operations, with particular emphasis on DUG facilities.
Interdiction and strike	Develop weapons to attack network and information flows.
Intelligence gathering	Develop virtual humint capabilities with UAVs. Analyze nodes to identify networks. Form interagency networks.
Force protection	Switch to more CONUS basing and develop a network of dormant bases. Limit modernization of C2 nodes. Develop defensive counterterrorism standards.

should no longer assume that terrorist groups are bureaucratic, hierarchical, stand-alone organizations.

In closing, we note that the history of the 20th century has demonstrated the crucial importance of air power to the outcome of land and naval warfare. Now, with the coming of the information age, it may well be that the history of the 21st century will show that air power proved equally useful in determining the outcome of the struggle against terrorism.