SUMMARY

Netwar is the lower-intensity, societal-level counterpart to our earlier, mostly military concept of cyberwar. Netwar has a dual nature, like the two-faced Roman god Janus, in that it is composed of conflicts waged, on the one hand, by terrorists, criminals, and ethnonationalist extremists; and by civil-society activists on the other. What distinguishes netwar as a form of conflict is the networked organizational structure of its practitioners—with many groups actually being leaderless—and the suppleness in their ability to come together quickly in swarming attacks. The concepts of cyberwar and netwar encompass a new spectrum of conflict that is emerging in the wake of the information revolution.

This volume studies major instances of netwar that have occurred over the past several years and finds, among other things, that netwar works very well. Whether the protagonists are civil-society activists or "uncivil-society" criminals and terrorists, their netwars have generally been successful. In part, the success of netwar may be explained by its very novelty—much as earlier periods of innovation in military affairs have seen new practices triumphant until an appropriate response is discovered. But there is more at work here: The network form of organization has reenlivened old forms of licit and illicit activity, posing serious challenges to those—mainly the militaries, constabularies, and governing officials of nation states—whose duty is to cope with the threats this new generation of largely nonstate actors poses.

Strategists and policymakers in Washington and elsewhere have already begun to discern the dark side of the netwar phenomenon, es-

pecially as manifested in terrorist and criminal organizations. This growing awareness is quite evident in recent official studies of this burgeoning problem: *Patterns of Global Terrorism: 1999* (State Department, 2000), *International Crime Threat Assessment* (Interagency Working Group, 2000), and *Global Trends 2015* (National Intelligence Council, 2000). But strategists and policymakers still have much work to do to harness the brighter, civil-society-building potential of networked nonstate actors. Thus, a fundamental challenge in the coming decade will be to focus on the opportunities that may arise from closer cooperation with nongovernmental organizations (NGOs) and other nonstate actors.

For the U.S. Department of Defense, a range of possibilities opens up, from encouraging the early involvement of appropriate NGO networks in helping to detect and head off a looming crisis, to working closely with them in the aftermath of conflicts to improve the effectiveness of U.S. forces still deployed, to reduce the residual hazards they face, and to strengthen the often fragile peace. In short, American policymakers and strategists must continue to keep an eye on the perils posed by criminal and terrorist networks. But they must enlarge their vision and their practices to encompass the tremendous opportunities likely to attend the rise of a network-based realm devoted to the protection of human rights, the spread of democratic values, and the formation of deep coalitions between states and civil-society NGOs. Netwar, the emergent mode of conflict of choice for networked nonstate actors, has two faces—and both matter very much.

In this volume, we and our colleagues examine various types of netwar, from the most violent to the most socially activist. In so doing, we find that, despite the variety, all networks that have been built for waging netwar may be analyzed in terms of a common analytic framework. There are five levels of theory and practice that matter: the technological, social, narrative, organizational, and doctrinal levels. A netwar actor must get all five right to be fully effective.

While a network's level of technological sophistication does make a difference—and people do tend to think that netwar depends heavily on technology—the other levels have just as much, if not more, of an effect on the potential power of a given group. One key level is the social basis for cooperation among network members. When social ties

are strong, building mutual trust and identity, a network's effectiveness is greatly enhanced. This can be seen most clearly in ethnically based terror, crime, and insurgent groups in which clan ties bind together even the loosest, most dispersed organization.

Among civil-society netwarriors, the narrative level of analysis may matter most. Sharing and projecting a common story about their involvement in an activist network enliven and empower these groups, and attract their audiences. The narrative level is also important to practitioners of the dark side of netwar, but it may be more necessary for civil-society networks to emphasize this level and get it right because they are less likely to be held together by the kinds of ethnic or clan ties so common among crime and terror networks.

In trying to confront or cope with a networked adversary, it is important to assess the opponent's strengths and weaknesses at the technological, social, and narrative levels. Yet, the defining level of a netwar actor is its organizational design. Analysts must realize that the structures of networks may feature much variety—from simple chain or line networks, to less simple hub or star designs, to complex all-channel designs, any and all of which may be blended into sprawling multihub and spider's-web networks. To cope with a network, analysts must first learn what *kind* of network it is and then draw on the best methods for analysis. In the past, intelligence assessments of adversaries have tended to focus on their hierarchical leadership structures. This is insufficient for analyzing netwar actors—which, like some of today's terrorist networks, may well consist of various small, dispersed groups that are linked in odd ways and do not have a clear leadership structure.

Another important level of analysis is to parse just what sort of doctrine the netwar actor is employing. Most networks—of both the civil and uncivil variety—will have a great capacity for swarming. This does not mean that all will swarm all the time, or even that all will swarm well. Moreover, few netwar actors have an explicit doctrine for swarming. But most are moving in that direction. Swarming is the key doctrinal approach for which to prepare.

The most potent netwarriors will not only be highly networked and have a capacity to swarm, they will also be held together by strong so-

cial ties, have secure communications technologies, and project a common "story" about why they are together and what they need to do. These will be the most serious adversaries. But even those networks that are weak on some levels (e.g., technological) may pose stiff challenges to their nation-state adversaries. With this in mind, it is necessary to go beyond just diagnosing the nature of the networked nonstate opponent in a given conflict. It will become crucial for governments and their military and law enforcement establishments to begin networking themselves. Perhaps this will become the greatest challenge posed by the rise of netwar.

Chapter One

THE ADVENT OF NETWAR (REVISITED)[1]

John Arquilla and David Ronfeldt

Editors' abstract. This introductory chapter provides a reprise of many of the points we have made about the netwar concept since 1993. In this book, we depict netwar as having two major faces, like the Roman god Janus—one dominated by terrorists and criminals that is quite violent and negative, and another evinced by social activists that can be militant but is often peaceable and even promising for societies. Indeed, the book is structured around this theme.

The information revolution is altering the nature of conflict across the spectrum. We call attention to two developments in particular. First, this 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, because they are able to organize into sprawling multiorganizational networks (especially "all-channel" networks, in which every node is connected to every other node) more readily than can traditional, hierarchical, state actors. This means that conflicts may increasingly be waged by "networks," perhaps more than by "hierarchies." It also means that whoever masters the network form stands to gain the advantage.

Second, as the information revolution deepens, the conduct and outcome of conflicts increasingly depend on information and communications. More than ever before, conflicts revolve around "knowledge"

[1]Our netwar concept predates, and should not be confused with, the U.S. military's network warfare simulation (NETWARS) system.

and the use of "soft power."[2] Adversaries are learning to emphasize "information operations" and "perception management"—that is, media-oriented measures that aim to attract or disorient 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.

These propositions cut across the entire conflict spectrum. Major transformations are thus 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 nonlinear, and ambiguous than industrial-age threats. Metaphorically, then, future conflicts may resemble the Oriental game of *Go* more than the Western game of chess. The conflict spectrum will be remolded from end to end by these dynamics.

A CONCEPT AND ITS BRIEF HISTORY

Back in 1992, while first wondering about such propositions and writing about *cyberwar* as a looming mode of military conflict, we thought it would be a good idea to have a parallel concept about information-age conflict at the less military, low-intensity, more social end of the spectrum. The term we coined was *netwar*, largely because it resonated with the surety that the information revolution favored the rise of network forms of organization, doctrine, and strategy. Through netwar, numerous dispersed small groups using the latest communications technologies could act conjointly across great distances. We had in mind actors as diverse as transnational terrorists, criminals, and even radical activists. Some were already moving from hierarchical to new information-age network designs.

We fielded the netwar concept in our first journal article, "Cyberwar Is Coming" (1993), then provided a full exposition in our RAND report, *The Advent of Netwar* (1996). Additional insights were advanced in the concluding chapter of our book, *In Athena's Camp* (1997). Elaborations appeared in multiauthored RAND volumes on *The Zapatista*

[2]The concept of soft power was introduced by Nye (1990), and further elaborated in Nye and Owens (1996).

"Social Netwar" in Mexico (Ronfeldt et al., 1998) and *Countering the New Terrorism* (Lesser et al., 1999). Our study *The Emergence of Noopolitik: Toward an American Information Strategy* (1999) observed that many socially minded nongovernmental organizations (NGOs) were already using netwar strategies to enhance their soft power. Our recent study *Swarming and the Future of Conflict* (2000) is mainly about developing a new military doctrine for wielding "hard" power, but it generally advances our view that swarming is likely to become the dominant approach to conflict across the spectrum, including among netwar actors. While the Zapatista study provided early evidence for this, short opinion pieces on the military war in Kosovo (1999) and the activist "Battle for Seattle"(1999) identified new cases.[3]

As these writings have spread, the netwar concept has struck a chord with a growing number of theorists, futurists, journalists, and practitioners. In forward-looking books, scholars as diverse as Manuel Castells (1997), Chris Hables Gray (1997), and David Brin (1998) have used the concept for discussing trends at the mostly nonmilitary end of the conflict spectrum. For several years, a web site maintained by Jason Wehling carried a wide range of articles about netwar, social activism, and information-age conflict, leading off with a paper he had written about the netwar concept (1995). Meanwhile, interesting flurries of discussion about netwar arose on email lists related to the Zapatista movement in Mexico following the armed uprising in January 1994. Harry Cleaver's writings (e.g., 1995, 1998, 1999) are particularly illuminating. They show that Mexico became a laboratory for the emergence of a new, non-Leninist model of radicalism. The Zapatista leader, Subcomandante Marcos, even averred in 1999 that netwar described the Zapatista movement, and that *counternetwar* instructed the strategy of its military and paramilitary opponents. For its part, the high command of the Mexican military also espoused admiration for the concept during 2000.[4] Also in 2000, a leader of the International Campaign to Ban Landmines (ICBL), Jody Williams, remarked in a

[3]John Arquilla and David Ronfeldt, "Need for Networked, High-Tech Cyberwar," *Los Angeles Times*, June 20, 1999, pp. A1, A6; John Arquilla and David Ronfeldt, "A Win for Netwar in Seattle," December 1999, posted on the web site for the Highlands Forum.

[4]Both the Zapatista and the Mexican army leadership had read the RAND report analyzing the Zapatista movement as a case of social netwar (Ronfeldt et al., 1998).

radio interview that she had heard that RAND researchers were developing the netwar concept to help governments control movements like the ICBL. Elsewhere, the concept cropped up in marginal rants and ruminations by militants associated with various left-wing, right-wing, and eclectic religious movements who posted on Usenet discussion groups.

Meanwhile, officials and analysts in U.S. and European government, military, and police circles began showing an interest in the concept. They were finding it difficult to deal with terrorists, criminals, and fanatics associated with militias and extremist single-issue movements, largely because these antagonists were organizing into sprawling, loose, "leaderless" networks, overcoming their former isolated postures as stand-alone groups headed by "great men." U.S. and European officials realized that these troublesome trends put a premium on interagency communication and coordination, for everything from intelligence sharing to tactical operations. But this implied a degree of cross-jurisdictional and international networking, especially for intelligence sharing, that is difficult for state hierarchies to accomplish. The concepts of netwar and counternetwar attracted some interest because they had a potential for motivating officials to build their own networks, as well as hybrids of hierarchies and networks, to deal with the networked organizations, doctrines, and strategies of their information-age adversaries. A special issue of the journal *Studies in Conflict and Terrorism* on "Netwar Across the Spectrum of Conflict" (1999) may have helped heighten awareness of this.[5]

Our formulation of the netwar concept has always emphasized the organizational dimension. But we have also pointed out that an organizational network works best when it has the right doctrinal, technological, and social dynamics. In our joint work, we have repeatedly insisted on this. However, writers enamored of the flashy, high-tech aspects of the information revolution have often depicted netwar (and cyberwar) as a term for computerized aggression waged via stand-off attacks in cyberspace—that is, as a trendy synonym for in-

[5]This special issue was partly assembled and edited by David Ronfeldt. Some text in this section comes from his introduction to that issue.

fowar, information operations, "strategic information warfare," Internet war, "hacktivism," cyberterrorism, cybotage, etc.[6]

Thus, in some quarters, the Serb hacks of NATO's web site in 1999 were viewed as netwar (or cyberwar). Yet, little was known about the perpetrators and the nature of their organization; if they amounted to just a few, clever, government-sponsored individuals operating from a site or two, then the netwar dimensions of this case were minimal, and it was just a clever instance of minor cybotage. This case also speaks to another distortion: These Serbs (presumably they were Serbs) aimed to bring a piece of "the Net" down. Yet, in a full-fledged ethnonationalist, terrorist, criminal, or social netwar, the protagonists may be far more interested in keeping the Net up. They may benefit from using the Internet and other advanced communications services (e.g., fax machines and cellular telephones) for purposes that range from coordinating with each other and seeking recruits, to projecting their identity, broadcasting their messages to target audiences, and gathering intelligence about their opponents.

With respect to Serbia, then, a better case of netwar as we define it was the effort by Serbia's reformist Radio B-92, along with a supportive network of U.S. and European government agencies and NGOs, to broadcast its reportage back into Serbia over the Internet, after B-92's transmitters were shut down by the Milosevic regime in 1998 and again in 1999. For a seminal case of a worldwide netwar, one need look no further than the ICBL. This unusually successful movement consists of a loosely internetted array of NGOs and governments, which rely heavily on the Internet for communications. Through the personage of one of its many leaders, Jody Williams, this netwar won a well-deserved Nobel peace prize.[7]

---

[6]For an interesting paper by a leading proponent of hacktivism, see Wray (1998).

[7]See speech by Jody Williams accepting the Nobel Peace Prize in 1997, www.waging peace.org/articles/nobel_lecture_97_williams.html; and the speech she gave at a gathering of recipients at the University of Virginia in 1998, www.virginia.edu/nobel/transcript/jwilliams.html, as well as Williams and Goose (1998).

DEFINING NETWAR[8]

To be precise, the term netwar refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, 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 organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command. Thus, netwar differs from modes of conflict and crime in which the protagonists prefer to develop formal, stand-alone, hierarchical organizations, doctrines, and strategies as in past efforts, for example, to build centralized movements along Leninist lines. Thus, for example, netwar is about the Zapatistas more than the Fidelistas, Hamas more than the Palestine Liberation Organization (PLO), the American Christian Patriot movement more than the Ku Klux Klan, and the Asian Triads more than the Cosa Nostra.[9]

The term *netwar* is meant to call attention to the prospect that network-based conflict and crime will become major phenomena in the decades ahead. Various actors across the spectrum of conflict and crime are already evolving in this direction. This includes familiar adversaries who are modifying their structures and strategies to take advantage of networked designs—e.g., transnational terrorist groups, black-market proliferators of weapons of mass destruction (WMD), drug and other crime syndicates, fundamentalist and ethnonationalist movements, intellectual-property pirates, and immigration and refugee smugglers. Some urban gangs, back-country militias, and militant single-issue groups in the United States have also been developing netwar-like attributes. The netwar spectrum also includes a new generation of revolutionaries, radicals, and activists who are beginning to create information-age ideologies, in which identities and

[8]This section reiterates but also updates our earlier formulations about the nature of netwar (notably those in Arquilla and Ronfeldt, 1996; Ronfeldt et al., 1998; and Arquilla, Ronfeldt, and Zanini, 1999). Readers who are already familiar with this work may prefer to skip this section.

[9]This is just a short exemplary statement. Many other examples could be noted. Instead of Hamas, for example, we might mention the Committee for the Defense of Legitimate Human Rights (CDLHR), an anti-Saudi organization based in London.

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 engage in netwar.

Many—if not most—netwar actors will be nonstate, even stateless. Some may be agents of a state, but others may try to turn states into *their* agents. Also, a netwar actor may be both subnational and transnational in scope. Odd hybrids and symbioses are likely. Furthermore, some bad actors (e.g., terrorist and criminal groups) may threaten U.S. and other nations' interests, but other actors (e.g., NGO activists in Burma or Mexico) may not—indeed, some actors who at times turn to netwar strategies and tactics, such as the New York–based Committee to Protect Journalists (CPJ), may have salutary liberalizing effects. Some actors may aim at destruction, but more may aim mainly at disruption and disorientation. 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

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. In the scholarly literature (e.g., Evan, 1972), networks come in basically three types or topologies (see Figure 1.1):

- The *chain* or line 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 *hub*, star, or wheel network, as in a franchise or a cartel where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other.

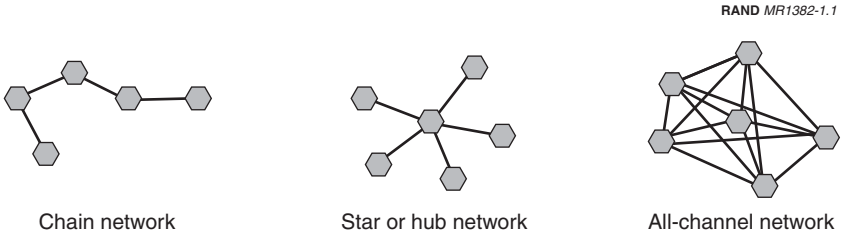

Figure 1.1—Three Basic Types of Networks

- The *all-channel* or full-matrix network, as in a collaborative network of militant peace groups where everybody is connected to everybody else.

Each node in the diagrams may refer to an individual, a group, an organization, part of a group or organization, or even a state. The nodes may be large or small, tightly or loosely coupled, and inclusive 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, or of any node included in it, may be well-defined, or blurred and porous in relation to the outside environment. Many 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 hub 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 of the three types, with different tasks being organized around different types of networks. For example, a netwar actor may have an all-channel council or directorate at its core but use hubs and chains for tactical operations. There may also be hybrids of network and hierarchical forms of organization. For example, traditional hierarchies may exist inside particular nodes in a network. Some actors may have a hierarchical organization overall but use network designs for tactical operations; other actors may have an all-channel network design

overall 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 characterizes a particular network.

Of the three network types, the all-channel has been the most difficult to organize and sustain, partly because it may require dense communications. But it is the type that gives the network form its new, high potential for collaborative undertakings and that is gaining new strength from the information revolution. Pictorially, an all-channel netwar actor resembles a geodesic "Bucky ball" (named for Buckminster Fuller); it does not look like a pyramid. The organizational 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; there may be multiple leaders. Decisionmaking 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).[10]

The capacity of this design for effective performance over time may depend on the existence of shared principles, interests, and goals—perhaps an overarching doctrine or ideology—which spans all nodes and to which the members subscribe in a deep way. Such a set of principles, shaped through mutual consultation and consensus-building, can enable members to be "all of one mind" even though they are dispersed and devoted to different tasks. It can provide a central ideational 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 because "they know what they have to do."[11]

The network design may depend on having an infrastructure for the dense communication of functional information. This does not mean that all nodes must be in constant communication; that may not

[10]The structure may also be cellular. However, 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.

[11]The quotation is from a doctrinal statement by Beam (1992) about "leaderless resistance," which has strongly influenced right-wing white-power groups.

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.

In many respects, then, the archetypal netwar design corresponds to what earlier analysts (Gerlach, 1987, p. 115, based on Gerlach and Hine, 1970) called a "segmented, polycentric, ideologically integrated network" (SPIN):

> 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.[12]

Caveats About the Role of Technology

Netwar is a result of the rise of network forms of organization, which in turn is partly a result of the computerized information revolution.[13] 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 communication technologies—cellular telephones, fax machines, electronic mail (email), web sites, and computer conferencing. Such technologies are highly advantageous for netwar actors whose constituents are geographically dispersed.

---

[12]The SPIN concept is a precursor of the netwar concept. 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, doctrine, and strategy that are now coming into focus in the analysis not only of social movements but also of some terrorist, criminal, ethnonationalist, and fundamentalist organizations.

[13]For explanation of this point, see Ronfeldt (1996), Arquilla and Ronfeldt (1996), and other sources cited in those documents.

But two caveats are in order. First, the new technologies, however enabling for organizational networking, are not absolutely necessary for a netwar actor. Older technologies, like human couriers, and mixes of old and new systems may do the job in some situations. The late Somali warlord, Mohamed Farah Aidid, for example, proved very adept at eluding those seeking to capture him while at the same time retaining full command and control over his forces by means of runners and drum codes (see Bowden, 1999). Similarly, the first Chechen War (1994–1996), which the Islamic insurgents won, made wide use of runners and old communications technologies like ham radios for battle management and other command and control functions (see Arquilla and Karasik, 1999). So, netwar may be waged in high-, low-, or no-tech fashion.

Second, netwar is not simply a function of "the Net" (i.e., the Internet); it does not take place only in "cyberspace" or the "infosphere." Some *battles* may occur there, but a *war's* overall conduct and outcome will normally depend mostly on what happens in the "real world"—it will continue to be, even in information-age conflicts, generally more important than what happens in cyberspace or the infosphere.[14]

Netwar is not solely about Internet war (just as cyberwar is not just about "strategic information warfare"). Americans have a tendency to view modern conflict as being more about technology than organization and doctrine. In our view, this is a misleading tendency. For example, social netwar is more about a doctrinal leader like Subcomandante Marcos than about a lone, wild computer hacker like Kevin Mitnick.

[14]This point was raised specifically by Paul Kneisel, "Netwar: The Battle over Rec.Music.White-Power," *ANTIFA INFO-BULLETIN*, Research Supplement, June 12, 1996, which is available on the Internet. He 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*.

A Capacity for 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 tend to be 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, [15] which is quite different from traditional mass- and maneuver-oriented approaches to conflict. Yet swarming may become the key mode of conflict in the information age (Arquilla and Ronfeldt, 2000, and Edwards, 2000), and the cutting edge for this possibility is found among netwar protagonists.

Swarming is a seemingly amorphous, but deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions. This notion of "force and/or fire" may be literal in the case of military or police operations, but metaphorical in the case of NGO activists, who may, for example, be blocking city intersections or emitting volleys of emails and faxes. Swarming will work best—perhaps it will only work—if it is designed mainly around the deployment of myriad, small, dispersed, networked maneuver units. Swarming occurs when the dispersed units of a network of small (and perhaps some large) forces converge on a target from multiple directions. The overall aim is *sustainable pulsing*—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. The capacity for a "stealthy approach" suggests that, in netwar, attacks are more likely to occur in "swarms" than in more traditional "waves." The Chechen resistance to the Russian army and the Direct Action Network's operations in the anti–World Trade Organization "Battle of Seattle" both provide excellent examples of swarming behavior.

---

[15]The first mention of "swarm networks" we encountered was in Kelly (1994). A recent discussion, really about "swarm intelligence" rather than swarm networks, is in Bonabeau, Dorigo, and Theraulaz (1999).

Swarming may be most effective, and difficult to defend against, where a set of netwar actors do not "mass" their forces, but rather engage in dispersion and "packetization" (for want of a better term). This means, for example, that drug smugglers can break large loads into many small packets for simultaneous surreptitious transport across a border, or that NGO activists, as in the case of the Zapatista movement, have enough diversity in their ranks to respond to any discrete issue that arises—human rights, democracy, the environment, rural development, whatever.

In terms of their defensive potential, networks tend to be redundant and diverse, making them robust and resilient in the face of attack. When 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—a favored strategy in the drug war as well as in overall efforts to tamp organized crime in the United States. Thus, whoever wants to attack a network is limited—generally, only portions of a network can be found and confronted. Moreover, the deniability built into a network affords the possibility that it may simply absorb a number of attacks on distributed nodes, leading an attacker to believe the network has been harmed and rendered inoperable when, in fact, it remains viable and is seeking new opportunities for tactical surprise.

The difficulty of dealing with netwar actors deepens 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 where an actor goes on the offense in the name of self-defense. For example, the Zapatista struggle in Mexico demonstrates anew the blurring of offense and 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, as in the war of the *mujahideen* in Afghanistan during the 1980s, and in both recent Chechen wars with the Russians.

Operating in the Seams

The blurring of offense and defense reflects another feature of netwar (albeit one that is exhibited in many other policy and issue areas): 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. This makes it difficult if not impossible for a government to assign responsibility to any single agency—e.g., military, police, or intelligence—to be in charge of responding.

As Richard Szafranski (1994, 1995) illuminated in his discussions of how information warfare ultimately becomes "neo-cortical warfare," the challenge for governments and societies becomes "epistemological." A netwar actor may aim to confound people's fundamental beliefs about the nature of their culture, society, and government, partly to foment fear but perhaps mainly to disorient people and unhinge their perceptions. This is why a netwar with a strong social content—whether waged by ethnonationalists, terrorists, or social activists—may tend to be about disruption more than destruction. The more epistemological the challenge, the more confounding it may be from an organizational standpoint. Whose responsibility is it to respond? Whose roles and missions are at stake? Is it a military, police, intelligence, or political matter? When the roles and missions of defenders are not easy to define, both deterrence and defense may become problematic.

Thus, the spread of netwar adds to the challenges facing the nation state in the information age. Its sovereignty and authority are usually exercised through bureacracies in which issues and problems can be sliced up 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 a society, striking where lines of authority crisscross and the operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash. Moreover, where transnational participation is strong, a netwar's protagonists may expose a local government to challenges to its sovereignty and legitimacy by arousing foreign governments and business corporations to put pressure on the local government to alter its domestic policies and practices.

NETWORKS VERSUS HIERARCHIES: CHALLENGES FOR COUNTERNETWAR

These observations and the case studies presented in this volume lead to four policy-oriented propositions about the information revolution and its implications for netwar and counternetwar (Arquilla and Ronfeldt, 1993, 1996):[16]

Hierarchies have a difficult time fighting networks. There are examples of this across the conflict spectrum. Some of the best are found in the failings of many 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 both the defensive and offensive robustness of the network form. The Zapatista movement in Mexico, with its legions of supporters and sympathizers among local and transnational 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 want to 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 that he has already learned about the rise of network forms in the information age. These principles depend to some extent on technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, perhaps especially 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 are advanced at networking (be they criminals, terrorists, or peaceful social activists, including ones acting in concert with states) are enjoying an increase in their power relative to state agencies. While networking once allowed them simply to keep from being suppressed, it now allows them to compete on more nearly equal terms with states and other hierarchically oriented actors. The histories of

[16]Also see Berger (1998) for additional observations about such propositions.

Hamas and of the Cali cartel illustrate this; so do the Zapatista movement in Mexico and the International Campaign to Ban Landmines.

Counternetwar may thus require very effective interagency approaches, which by their nature involve networked structures. It is not necessary, desirable, or even possible to replace all hierarchies with networks in governments. Rather, the challenge will be to blend these two forms skillfully, while retaining enough core authority to encourage and enforce adherence to networked processes. By creating effective hybrids, governments may become better prepared to confront the new threats and challenges emerging in the information age, whether generated by ethnonationalists, terrorists, militias, criminals, or other actors. (For elaboration, see Arquilla and Ronfeldt, 1997, Ch. 19.)

However, governments tend to be so constrained by hierarchical habits and institutional interests that it may take some sharp reverses before a willingness to experiment more seriously with networking emerges. The costs and risks associated with failing to engage in institutional redesign are likely to be high—and may grow ever higher over time. In the most difficult areas—crime and terrorism—steps to improve intra- and international networking are moving in the right direction. But far more remains to be done, as criminal and terrorist networks continuously remake themselves into ever more difficult targets.

RECENT CASES OF NETWAR

Since we first wrote about netwar over seven years ago, there have been at least ten prominent (i.e., front-page) instances of its employment, in conflicts ranging from social activist campaigns to violent ethnic insurgencies (see Table 1.1). The netwar record has been generally successful. In these ten cases, which feature networked nonstate actors confronting states or groups of states, five netwars have achieved substantial success. Three have achieved limited success, while one (Burma) has yet to prove either a success or failure, and an-

Table 1.1

Prominent Cases of Netwar, 1994–2000

Campaign	Dates	Outcome	Type
Protracted Netwars			
EZLN[a]	1994–	Limited success	Autonomist
ICBL	1998–	Limited success	Globalist
Burma	1996–	Failing?	Mixed
Drug Cartels	1994–	Substantial success	Autonomist
Chechnya I	1994–1996	Substantial success	Autonomist
Chechnya II	1999–2000	Failure	Autonomist
Short-Duration Netwars			
Greenpeace	1994	Limited success	Globalist
Battle of Seattle	1999	Substantial success	Globalist
East Timor	1999	Substantial success	Autonomist
Serb Opposition	2000	Substantial success	Mixed

[a]Zapatista National Liberation Army.

other (Chechnya) must be judged, currently, as a failure.[17] Most of these cases, and the reasons for their success or the lack thereof, are discussed in detail in the following chapters.

The limits on some successes and the one failure imply a need to take a balanced view of netwar, analyzing the conditions under which it is most likely to succeed, fail, or fall somewhere in between. Clearly, there is enough success here to make netwar worth examining more closely. But it is important not to "tout" netwar, as Robert Taber (1970) once did guerrilla war. He was sharply rebutted by Lewis Gann (1970), who pointed out that guerrillas, far from being unstoppable, have of-

[17]Both Russo-Chechen conflicts are included as netwars, because of the extent to which the Chechens have relied upon networked forms of organization, both in field actions and in the struggle to win the "battle of the story." Arquilla and Karasik (1999) describe the Chechen victory in the 1994–1996 conflict as a clear triumph for networking but also posed concerns that the Russians would learn from this defeat—as they have learned from defeats throughout their history—and would improve, both in the field and in the arena of world perception. They have gotten better in the second conflict, driving the Chechens to their southern mountain redoubts and convincing state and nonstate actors around the world that Russian forces are fighting on behalf of a world community opposed to terrorism.

ten been defeated. Netwar will also have its ups and downs. Our purpose is to uncover and get a deeper understanding of its dynamics.

In Table 1.1, the cases are divided into those conflicts that were or have been drawn out, and those focused on specific crises—a useful distinction often made in studies of conflict. Interesting insights emerge. For example, the two most successful protracted campaigns were waged violently by ethnonationalists and criminals who sought freedom from state controls. The short-duration successes also included some use of violence (in two cases), and a global civil society reaction (that threatened a forceful response) to state violence in the other. And, though more muted, most of the other cases have violent aspects.

The table distributes netwars by type along a spectrum ranging from those that are globalist in orientation (e.g., the anti-landmine campaign), to those that are autonomist at the opposite end (e.g., the 1994 Chechen effort to secede from Russia). In the middle lie mixed cases where the objective is to gain power locally, but these netwars depend on the protagonists being able to open their societies to democratic, globalist influences.

The two unsuccessful netwar campaigns (in Russia and Burma) have featured networks confronting hierarchical authoritarian governments that have been willing to use substantial force to assert—in the case of Russia, to reassert—their hold on power. These networks' losses to hierarchies, combined with the fact that the principal successes to date have been gained by violent "uncivil society" actors, suggest being cautious about the claims for netwar. That said, the nonviolent International Campaign to Ban Landmines and the Greenpeace effort to curb nuclear testing both achieved reasonable measures of success without engaging in any violence whatsoever. This is a hopeful sign. And, while the civil society campaign to free Burma from authoritarian rule is a partial failure to date, this is a continuing campaign whose ultimate outcome is yet unknown.

Finally, these netwar conflicts feature an uneven split between those about globalist issues—aimed at fostering the rise of a rights- and ethics-based civil society—and the more frequent, somewhat darker "autonomist" variety of netwar, featuring nonstate actors trying to get

out from under state controls. Most of the limited successes that have been achieved thus far are globalist in orientation, while most of the substantial successes (save for the Battle of Seattle and Serbia) have been autonomist. It will be interesting, as the instances of netwar increase over time, to see whether this pattern holds. The outcomes of the globalist cases suggest the prevalence of negotiated solutions, while the autonomist conflicts may, in general, have a much more inherently desperate character that drives them to greater violence and less willingness to reach accommodation. All this we will watch in the years to come. For now, these early cases have helped us to develop this taxonomy of netwar, further refining the concept.

Will netwar continue to empower nonstate actors, perhaps reducing the relative power advantage enjoyed by nation states? Civil society networks have already made much use of social netwar as a tool for advancing a globalist, ethics-based agenda focused on broadening and deepening human rights regimes—often in the context of an ongoing effort to foster movement from authoritarian rule to democracy (e.g., Burma). But there is another side of nonstate-actor-oriented netwar, characterized not by globalist impulses, but rather by the desire to avoid state control of a network's criminal, terrorist, or ethnic-separatist agenda (e.g., Hamas and Chechens). While the globalist netwars seem devoted to nonviolent tools of struggle, the autonomists may employ both means of engagement—often with a greater emphasis on violence.

VARIETIES OF NETWAR—DUAL PHENOMENA

Netwar is a deduced concept—it derives from our thinking about the effects and implications of the information revolution. Once coined, the concept helps show that evidence is mounting about the rise of network forms of organization, and about the importance of "information strategies" and "information operations" across the spectrum of conflict, including among ethnonationalists, terrorists, guerrillas, criminals, and activists.[18] Note that we do not equate ethnonational-

[18]These are not the only types of netwar actors; there are others. For example, corporations may also engage in netwars—or find themselves on the receiving end of netwar campaigns.

ists, terrorists, guerrillas, criminals, and activists with each other—each has different dynamics. Nor do we mean to tarnish social activism, which has positive aspects for civil society.[19] We are simply calling for attention to a cross-cutting meta-pattern about network forms of organization, doctrine, and strategy that we might not have spotted, by induction or deduction, if we had been experts focused solely on any one of those areas.

Netwar can be waged by "good" as well as "bad" actors, and through peaceful as well as violent measures. From its beginnings, netwar has appealed to a broad cross-section of nonstate actors who are striving to confront or cope with their state authorities. Ethnonationalists, criminals, and terrorists—all have found new power in networking. But so too have emerging global civil society actors who have emphasized nonviolent efforts to win the "battle of the story"—a more purely informational dimension of netwar—rather than the violent swarming characteristic of its darker side. Both categories of actors seem to realize, even if only implicitly, that, in the future, conflict will become even more "irregularized," with the set-piece confrontations and battles of earlier eras largely disappearing. While the U.S. military remains focused—in terms of budgetary emphasis, doctrine, and force structure—on the traditional forms of conflict, the rise of netwar should prompt a shift to a nimble "turn of mind," one far less attuned to fighting in the Fulda Gap or the Persian Gulf and more focused on engaging a range of odd new adversaries across a densely interconnected "global grid."

The duality of netwar in the real world—dark-side criminals and terrorists on the one hand, but enlightening civil society forces on the other—is mirrored in the virtual world of cyberspace, which is increasingly utilized for crime and terror (still embryonic), along with social activism. At present, social activism is far more robust and established in the cyber realm than is crime or terror. Will this continue to be the case? We think so. Activists will become more adept at integrating the mobilizing force of the Internet with the power and appeal of messages aimed at spreading and protecting human rights. Even

[19]See discussion in Ronfeldt (1996).

so, criminal and terrorist organizations will learn how to manipulate the infosphere with increasing skill.

Thus, netwar has two faces, like the Roman god Janus. Janus was the god of doors and gates, and thus of departures and returns, and new beginnings and initiatives. This, in a sense, meant he was the god of communications, too. His double face, one old and looking back, the other younger and peering forward, conveyed that he was an inherently dual god. At the beginning of creation, he partook in the separation of order from chaos. In Roman times, he was identified with the distinction between war and peace, for the gate to his temple at the Forum was kept ceremoniously closed in times of peace and open in times of war—which meant the gates were rarely closed. At the start of the 21st century, the world is again at a new beginning. It is uncertain whether it will be an era of peace or conflict; but how matters turn out will depend to some degree on which face of netwar predominates.

This volume explores the two faces of netwar, in three parts. The first part is composed of three chapters that chronicle the increasingly networked nature of major types of "uncivil-society" actors for whom violence is a principal mode of expression. The analyses by Michele Zanini and Sean Edwards of Arab terrorist groups, by Phil Williams of transnational criminal networks, and by John Sullivan of street-level gangs and hooligans, all speak to the increasingly sophisticated usage of the new information technologies to enhance both these groups' organizational and operational capabilities.

The second part of the book examines the rise of social netwar, again with three chapters. These chapters examine social netwars waged by networked civil society actors against various types of states. Tiffany Danitz and Warren Strobel show the limitations (but also some successful facets) of social netwar when waged against a resolute dictatorship that maintains a system virtually closed to civil society. Our own chapter on Mexico finds that an "NGO swarm" was quite effective in transforming a rural insurgency into a mostly peaceable netwar in a then rather authoritarian system. Paul de Armond provides insights into the full mobilizing potential of social netwar when conducted in a free society like the United States.

The final part considers the future of netwar, particularly regarding how technology, organization, and doctrine interact. Dorothy Denning assesses whether activists, hacktivists, or cyberterrorists may gain the most influence from exploiting the new information technologies. Luther Gerlach's chapter, though focused on environmental activism, identifies the dynamics of organizations that are segmentary, polycentric, and integrated as a network—from leaderlessness to operational fluidity. We think these dynamics apply, in varying degrees, to all the types of actors examined in the first two parts of the book. Our concluding chapter addresses likely trends in both the theory and practice of netwar—from how to draw on academic theories about networks, to how to think strategically about netwar itself. Thus, Part III should make the reader aware of both the perils and the promises of netwar, while also providing analytical guideposts for future studies of this phenomenon.

BIBLIOGRAPHY

Arquilla, John, and Theodore Karasik, "Chechnya: A Glimpse of Future Conflict?" *Studies in Conflict and Terrorism*, Vol. 22, No. 3, July–September 1999, pp. 207–230.

Arquilla, John, and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy,* Vol. 12, No. 2, Summer 1993, pp. 141–165. Available as RAND reprint RP-223.

Arquilla, John, and David Ronfeldt, *The Advent of Netwar,* Santa Monica, Calif.: RAND, MR-789-OSD, 1996.

Arquilla, John, and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy,* Santa Monica, Calif.: RAND, MR-1033-OSD, 1999.

Arquilla, John, and David Ronfeldt, *Swarming and the Future of Conflict*, Santa Monica, Calif.: RAND, DB-311-OSD, 2000.

Arquilla, John, and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997.

Arquilla, John, David Ronfeldt, and Michele Zanini, "Information-Age Terrorism and the U.S. Air Force," in Ian O. Lesser et al., *Countering the New Terrorism,* Santa Monica, Calif.: RAND, MR-989-AF, 1999.

Beam, Louis, "Leaderless Resistance," *The Seditionist*, Issue 12, February 1992 (text can also be located sometimes on the web).

Berger, Alexander, *Organizational Innovation and Redesign in the Information Age: The Drug War, Netwar, and Other Low-End Conflict,* master's thesis, Monterey, Calif.: Naval Postgraduate School, 1998.

Bonabeau, Eric, Marco Dorigo, and Guy Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems,* Oxford: Oxford University Press, 1999.

Bowden, Mark, *Blackhawk Down: A Story of Modern War,* New York: Atlantic Monthly Press, 1999.

Brin, David, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, Mass.: Addison-Wesley, 1998.

Castells, Manuel, *The Information Age: Economy, Society and Culture,* Vol. II, *The Power of Identity,* Malden, Mass.: Blackwell Publishers, 1997.

Cleaver, Harry, "The Zapatistas and the Electronic Fabric of Struggle," 1995, www.eco.utexas.edu/faculty/Cleaver/zaps.html, printed in John Holloway and Eloina Pelaez, eds., *Zapatista! Reinventing Revolution in Mexico*, Sterling, Va.: Pluto Press, 1998, pp. 81–103.

Cleaver, Harry, "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric," *Journal of International Affairs*, Vol. 51, No. 2, Spring 1998, pp. 621–640.

Cleaver, Harry, *Computer-Linked Social Movements and the Global Threat to Capitalism,* July 1999, www.eco.utexas.edu/faculty/Cleaver/polnet.html.

Edwards, Sean J.A., *Swarming on the Battlefield: Past, Present and Future,* Santa Monica, Calif.: RAND, MR-1100-OSD, 2000.

Evan, William M., "An Organization-Set Model of Interorganizational Relations," in Matthew Tuite, Roger Chisholm, and Michael Rad-

nor, eds., *Interorganizational Decisionmaking*, Chicago: Aldine Publishing Company, 1972, pp. 181–200.

Gann, Lewis, *Guerrillas in History,* Stanford, Calif.: Hoover Institution Press, 1970.

Gerlach, Luther P., "Protest Movements and the Construction of Risk," in B. B. Johnson and V. T. Covello, eds., *The Social and Cultural Construction of Risk*, Boston: D. Reidel Publishing Co., 1987, pp. 103–145.

Gerlach, Luther P., and Virginia Hine, *People, Power, Change: Movements of Social Transformation,* New York: The Bobbs-Merrill Co., 1970.

Gray, Chris Hables, *Postmodern War: The New Politics of Conflict*, New York: The Guilford Press, 1997.

Kelly, Kevin, *Out of Control: The Rise of Neo-Biological Civilization,* New York: A William Patrick Book, Addison-Wesley Publishing Company, 1994.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Jenkins, *Countering the New Terrorism*, Santa Monica, Calif.: RAND, MR-989-AF, 1999.

Nye, Joseph S., *Bound to Lead: The Changing Nature of American Power,* New York: Basic Books, 1990.

Nye, Joseph S., and William A. Owens, "America's Information Edge," *Foreign Affairs,* Vol. 75, No. 2, March/April 1996, pp. 20–36.

Ronfeldt, David, *Tribes, Institutions, Markets, Networks—A Framework About Societal Evolution,* Santa Monica, Calif.: RAND, P-7967, 1996.

Ronfeldt, David, John Arquilla, Graham Fuller, and Melissa Fuller, *The Zapatista "Social Netwar" in Mexico*, Santa Monica, Calif.: RAND, MR-994-A, 1998.

Szafranski, Colonel Richard, "Neo-Cortical Warfare? The Acme of Skill," *Military Review*, November 1994, pp. 41–55.

Szafranski, Colonel Richard, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal*, Spring 1995, pp. 56–65.

Taber, Robert, *The War of the Flea*, New York: Citadel, 1970.

Toffler, Alvin, and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-First Century*, Boston: Little, Brown and Company, 1993.

Van Creveld, Martin, *The Transformation of War*, New York: Free Press, 1991.

Wehling, Jason, *"Netwars" and Activists Power on the Internet,* March 25, 1995—as circulated on the Internet (and once posted at www.teleport.com/~jwehling/OtherNetwars.html).

Williams, Jody, and Stephen Goose, "The International Campaign to Ban Landmines," in Maxwell A. Cameron, Robert J. Lawson, and Brian W. Tomlin, eds., *To Walk Without Fear: The Global Movement to Ban Landmines*, New York: Oxford University Press, 1998, pp. 20–47.

Wray, Stefan, *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics,* paper for a conference on The World Wide Web and Contemporary Cultural Theory, Drake University, November 1998, www.nyu.edu/projects/wray/wwwhack.html.

Chapter Two

THE NETWORKING OF TERROR IN THE INFORMATION AGE

Michele Zanini and Sean J.A. Edwards

Editors' abstract. Middle East Arab terrorists are on the cutting edge of organizational networking and stand to gain significantly from the information revolution. They can harness information technology to enable less hierarchical, more networked designs—enhancing their flexibility, responsiveness, and resilience. In turn, information technology can enhance their offensive operational capabilities for the war of ideas as well as for the war of violent acts. Zanini and Edwards (both at RAND) focus their analysis primarily on Middle East terrorism but also discuss other groups around the world. They conclude with a series of recommendations for policymakers. This chapter draws on RAND research originally reported in Ian Lesser et al., Countering the New Terrorism *(1999).*

INTRODUCTION

The information revolution has fueled the longest economic expansion in U.S. history and led to impressive productivity gains in recent years. Along with these benefits, however, has come the dark side of information technology—cyberterrorism. The idea of terrorists surreptitiously hacking into a computer system to introduce a virus, steal sensitive information, deface or swamp a web site, or turn off a crucial public service seriously concerns computer security personnel around the world. High profile attacks—such as the denial-of-service (DOS) attacks against major e-commerce sites Yahoo! and eBay in 1999 or the ongoing "cyber-jihad" against Israeli and American web sites being waged by Pakistani-based hackers in support of the Pales-

tinian "al-Aqsa" Intifadah—continue to raise the specter of cyberterrorism.

The information age is affecting not only the types of targets and weapons terrorists choose, but also the ways in which such groups operate and structure their organizations. Several of the most dangerous terrorist organizations are using information technology (IT)—such as computers, software, telecommunication devices, and the Internet—to better organize and coordinate dispersed activities. Like the large numbers of private corporations that have embraced IT to operate more efficiently and with greater flexibility, terrorists are harnessing the power of IT to enable new operational doctrines and forms of organization. And just as companies in the private sector are forming alliance networks to provide complex services to customers, so too are terrorist groups "disaggregating" from hierarchical bureaucracies and moving to flatter, more decentralized, and often changing webs of groups united by a common goal.

The rise of networked terrorist groups is part of a broader shift to what Arquilla and Ronfeldt have called "netwar."[1] Netwar refers to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war in which the 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. Netwar differs from modes of conflict in which the actors prefer formal, stand-alone, hierarchical organizations, doctrines, and strategies, as in past efforts, for example, to build centralized revolutionary movements along Marxist lines.

This chapter assesses the degree to which—and how—networked terrorist groups are using IT, particularly in the Middle East. The analysis reviews past trends and offers a series of educated guesses about how such trends will evolve in the future. The first section discusses the organizational implications of netwar, especially the degree to which IT is enabling different forms of terrorist structures and command, control, and communications (C3). The second section examines past ev-

[1]The netwar concept is explained and discussed more thoroughly in Chapter One of this volume.

idence of terrorist use of IT for offensive netwar, such as destructive and disruptive attacks on information systems and for perception management. The third section contains a speculative look at how future terrorist uses of IT could develop in the near to medium term. The final section concludes with implications for counterterrorism policy.

ORGANIZATIONAL NETWORKING AND TECHNOLOGY ACQUISITION

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 often are arrayed to act in a fully internetted "all-channel" manner. The potential effectiveness of the networked design compared to traditional hierarchical designs attracted the attention of management theorists as early as the 1960s.[2] Today, in the business world, virtual or networked organizations are heralded as effective alternatives to traditional bureaucracies because of their inherent flexibility, adaptiveness, and ability to capitalize on the talents of all of their members.

Networked organizations share three basic sets of features. First, communication and coordination are not formally specified by horizontal and vertical reporting relationships, but rather emerge and change according to the task at hand. Similarly, relationships are often informal and marked by varying degrees of intensity, depending on the needs of the organization. Second, internal networks are usually complemented by linkages to individuals outside the organization, often spanning national boundaries. Like internal connections, external relationships are formed and wind down according to the life cycle of particular joint projects. Third, both internal and external ties are enabled not by bureaucratic fiat, but rather by shared norms and

[2]In 1961, 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,

> 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.

values, as well as by reciprocal trust. Internally, the bulk of the work is conducted by self-managing teams, while external linkages compose "a constellation involving a complex network of contributing firms or groups" (Monge and Fulk, 1999, pp. 71–72).

The Emergence of Networked Terrorist Groups in the Greater Middle East

What has been emerging in the business world is now becoming apparent in the organizational structures of the newer and more active terrorist groups, which 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 that, nonetheless, enjoy tactical independence.

For example, in the Greater Middle East, terrorist organizations have diverse origins, ideologies, and organizational structures but can be categorized roughly into traditional and new-generation groups. Traditional groups date to the late 1960s and early 1970s, and the majority were (and some still are) formally or informally linked to the Palestine Liberation Organization (PLO). Typically, they are also relatively bureaucratic and maintain a nationalist or Marxist agenda.[3] These groups have utilized autonomous cells as part of their organizational structure, but the operation of such cells is guided by a hierarchy through clear reporting relationships and virtually little horizontal coordination.

In contrast, the newer and less hierarchical groups (such as Hamas; the Palestinian Islamic Jihad; Hizbollah; Algeria's Armed Islamic Group; the Egyptian Islamic Group; and Osama bin Laden's terrorist

[3]The traditional, more bureaucratic groups have survived partly through support from states such as Syria, Libya, and Iran. These groups—such as the Abu Nidal Organization, the Popular Front for the Liberation of Palestine (PFLP), and three PFLP-related splinters (the PFLP-General Command, the Palestine Liberation Front, and the Democratic Front for the Liberation of Palestine)—retain an ability to train and prepare for terrorist missions; however, their involvement in actual operations has been limited in recent years, partly because of counterterrorism campaigns by Israeli and Western agencies and the ongoing peace process.

network, al-Qaeda) have become the most active organizations (Office of the Coordinator for Counterterrorism, 2000). In these loosely organized groups with religious or ideological motives, operatives are part of a network that relies less on bureaucratic fiat and more on shared values and horizontal coordination mechanisms to accomplish its goals.

The new and more active generation of Middle Eastern groups has operated both inside and outside the region. For instance, in Israel and the occupied territories, Hamas and to a lesser extent the Palestinian Islamic Jihad have demonstrated their strength over the last five years with a series of suicide bombings that have killed more than 100 people. In Egypt, the Islamic Group (also known as al-Gama'a al-Islamiya) carried out a 1997 attack at Luxor, killing 58 tourists and four Egyptians. Another string of terrorist attacks (and foiled attempts) has focused attention on a loosely organized group of "Arab Afghans"—radical Islamic fighters from several North African and Middle Eastern countries who have forged ties while resisting the Soviet occupation of Afghanistan. One of the leaders and founders of the Arab Afghan movement is Osama bin Laden, a Saudi entrepreneur based in Afghanistan.[4]

To varying degrees, these groups share the principles of the networked organization—relative flatness, decentralization and delegation of decisionmaking authority, and loose lateral ties among dispersed groups and individuals. Hamas, for example, is loosely structured with

> some elements working clandestinely and others working openly through mosques and social service institutions to recruit members, raise money, organize activities, and distribute propaganda (Office of the Coordinator for Counterterrorism, 2000, p. 74).

[4]Bin Laden allegedly sent operatives to Yemen to bomb a hotel used by American soldiers on their way to Somalia in 1992, plotted to assassinate President Bill Clinton in the Philippines in 1994 and Egyptian President Hosni Mubarak in 1995, and played a role in the Riyadh and Khobar blasts in Saudi Arabia that resulted in the deaths of 24 Americans in 1995 and 1996. U.S. officials have also pointed to bin Laden as the mastermind behind the American embassy bombings in Kenya and Tanzania in 1998, which claimed the lives of more than 260 people, including 12 Americans, and in the bombing of the *U.S.S. Cole* in Yemen, in which 17 American sailors were killed.

The pro-Iranian Hizbollah in southern Lebanon acts as an umbrella organization of radical Shiite groups and in many respects is a hybrid of hierarchical and network arrangements—although the organizational structure is formal, interactions among members are volatile and do not follow rigid lines of control (Ranstorp, 1994, p. 304).

Perhaps the most interesting example of a terrorist netwar actor is Osama bin Laden's complex network of relatively autonomous groups that are financed from private sources. Bin Laden uses his wealth and organizational skills to support and direct al-Qaeda (The Base), a multinational alliance of Islamic extremists. Al-Qaeda seeks to counter any perceived threats to Islam—wherever they come from—as indicated by bin Laden's 1996 declaration of a holy war against the United States and the West in general. In the declaration, bin Laden specified that such a holy war was to be waged by irregular, light, highly mobile forces. Although bin Laden finances al-Qaeda (exploiting a fortune of several million dollars, according to U.S. State Department estimates) 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 nodes.[5]

There are reports that communications between al-Qaeda's members combine elements of a "hub-and-spoke" structure (where nodes of operatives communicate with bin Laden and his close advisers in Afghanistan) and a wheel structure (where nodes in the network communicate with each other without reference to bin Laden) (Simon and Benjamin, 2000, p. 70). Al-Qaeda's command-and-control structure includes a consultation council ("majlis al shura"), which discusses and approves major undertakings, and possibly a military committee.[6] At the heart of al-Qaeda is bin Laden's inner core group, which sometimes conducts missions on its own. Most of the other

[5]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 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.

[6]See indictment testimony from U.S. District Court, Southern District of New York, *United States of America vs. Osama bin Laden et al.,* 98 Cr. and S(2) 98 Cr. 1023 (LBS) (www.library.cornell.edu/colldev/mideast/usavhage.htm).

member organizations remain independent, although the barriers between them are permeable. According to U.S. District Court testimony in New York, al-Qaeda has forged alliances with Egypt's Islamic Group (leading to an alleged influx of bin Laden operatives into its structure), the National Front in the Sudan, the government of Iran, and Hizbollah. Media reports also indicate that bin Laden has ties with other far-flung Islamic armed groups, such as Abu Sayyaf in the Philippines, as well as with counterparts in Somalia, Chechnya, and Central Asia.[7]

Command, Control, Communications, and the Role of IT

Lateral coordination mechanisms facilitate the operations of networked groups. In turn, such coordination mechanisms are enabled by advances in information technology—including increases in the speed of communication, reductions in the costs of communication, increases in bandwidth, vastly expanded connectivity, and the integration of communication and computing technologies (see Heydebrand, 1989). More specifically, new communication and computing technologies allow the establishment of networks in three critical ways (Monge and Fulk, 1999, p. 84).

First, new technologies have greatly reduced transmission time, enabling dispersed organizational actors to communicate and coordinate their tasks. This phenomenon is not new—in the early 20th century, the introduction of the telephone made it possible for large corporations to decentralize their operations through local branches.

Second, new technologies have significantly reduced the cost of communication, allowing information-intensive organizational designs such as networks to become viable.[8] As Thompson (1967) observed,

---

[7]See, for instance, Kurlantzick, 2000, and FBIS, 1997a and 1997b.

[8]The current IT revolution has not only increased the capacity and speed of communications networks, it has driven down telephone communication costs as well. The value and benefit of the Internet also rise as more servers and users link together online. Because the value of a network grows roughly in line with the square of the number of users, the benefit of being online increases exponentially with the number of connections (called Metcalfe's Law, attributed to Robert Metcalfe, a pioneer of computer networking). The number of users worldwide has already climbed to more than 350 million and may reach 1 billion within four years. See "Untangling e-conomics," *The Economist*, September 23, 2000.

in the past, organizations sought to reduce coordination and communications costs by centralizing and colocating those activities that are inherently more coordination-intensive. With the lowering of coordination costs, it is becoming increasingly possible to further disaggregate organizations through decentralization and autonomy.

Third, new technologies have substantially increased the scope and complexity of the information that can be shared, through the integration of computing with communications. Such innovations as tele- and computer conferencing, groupware, Internet chat, and web sites allow participants to have "horizontal" and rich exchanges without requiring them to be located in close proximity.

Thus, information-age technologies are highly advantageous for a netwar group whose constituents are geographically dispersed or carry out distinct but complementary activities.[9] IT can be used to plan, coordinate, and execute operations. Using the Internet for communication can increase speed of mobilization and allow more dialogue between members, which enhances the organization's flexibility, since tactics can be adjusted more frequently. Individuals with a common agenda and goals can form subgroups, meet at a target location, conduct terrorist operations, and then readily terminate their relationships and redisperse.

The bin Laden network appears to have adopted information technology to support its networked mode of operations. According to reporters who visited bin Laden's headquarters in a remote mountainous area of Afghanistan, the terrorist financier has modern computer and communications equipment. Bin Laden allegedly uses satellite phone terminals to coordinate the activities of the group's dispersed operatives and has even devised countermeasures to ensure his safety while using such communication systems.[10] Satellite phones reportedly travel in separate convoys from bin Laden's; the Saudi financier

[9]This is not to say that hierarchical terrorist groups will not also adopt IT to improve support functions and internal command, control, and communications. Aum Shinrikyo was highly centralized around the figure of Shoko Asahara and its structure was cohesive and extremely hierarchical; yet the use the IT was widespread within the group. See Cameron, 1999, p. 283.

[10]Afghanistan's ruling Taliban leaders have repeatedly claimed that bin Laden's movements and access to communications have been severely restricted.

also refrains from direct use, often dictating his message to an assistant, who then relays it telephonically from a different location. Bin Laden's operatives have used CD-ROM disks to store and disseminate information on recruiting, bomb making, heavy weapons, and terrorist operations.[11] Egyptian computer experts who fought alongside bin Laden in the Afghan conflict are said to have helped him devise a communications network that relies on the web, email, and electronic bulletin boards so that members can exchange information (FBIS, 1995).

This is a trend found among other terrorist actors in the Middle East. Counterterrorist operations targeting Algerian Armed Islamic Group (GIA) bases in the 1990s uncovered computers and diskettes with instructions for the construction of bombs (FBIS, 1996a). In fact, it has been reported that the GIA makes heavy use of floppy disks and computers to store and process orders and other information for its members, who are dispersed in Algeria and Europe (FBIS, 1996b). The militant Islamic group Hamas also uses the Internet to share and communicate operational information. Hamas activists in the United States use chat rooms to plan operations and activities. Operatives use email to coordinate actions across Gaza, the West Bank, and Lebanon. Hamas has realized that information can be passed relatively securely over the Internet because counterterrorism intelligence cannot accurately monitor the flow and content of all Internet traffic. In fact, Israeli security officials cannot easily trace Hamas messages or decode their content (more on this below).

In addition, terrorist networks can protect their vital communication flows through readily available commercial technology, such as encryption programs. Examples from outside the Middle East point in this direction—according to one report, Animal Liberation Front (ALF) cells in North America and Europe use the encryption program Pretty Good Privacy (PGP) to send coded email and share intelligence (Iuris, 1997, p. 64). New encryption programs emerging on the commercial market are becoming so sophisticated that coded emails may soon be extremely difficult to break. In fact, strong encryption pro-

[11]U.S. intelligence agencies recently obtained computer-disk copies of a six-volume training manual used by bin Laden to train his recruits (Kelley, 2000).

grams are being integrated into commercial applications and network protocols so that soon encryption will be easy and automatic (see Denning and Baugh, 1997). Rumors persist that the French police have been unable to decrypt the hard disk on a portable computer belonging to a captured member of the Spanish/Basque organization ETA (Fatherland and Liberty) (Denning and Baugh, 1997). It has also been suggested that Israeli security forces were unsuccessful in their attempts at cracking the codes used by Hamas to send instructions for terrorist attacks over the Internet (Whine, 1999, p. 128). Terrorists can also use steganography—a method of hiding secret data in other data such as embedding a secret message within a picture file (Denning and Baugh, 1997). Terrorists can also encrypt cell phone transmissions, steal cell phone numbers and program them into a single phone, or use prepaid cell phone cards purchased anonymously to keep their communications secure.[12]

The latest communications technologies are thus enabling terrorists to operate from almost any country in the world, provided they have access to the necessary IT infrastructure; and this affects the ways in which groups rely on different forms of sponsorship. Some analysts have argued that networked terrorists may have a reduced need for state support—indeed, governmental protection may become less necessary if technologies such as encryption allow a terrorist group to operate with a greater degree of stealth and safety (Soo Hoo, Goodman, and Greenberg, 1997, p. 142). Others point to the possibility that groups will increasingly attempt to raise money on the web, as in the case of Pakistan's Lashkar-e-Taiba ("Army of the Pure").[13]

[12]Cloned cell phones can either be bought in bulk (the terrorist discards the phone after use) or a phone number can be stolen and programmed into a single cell phone just before using it. A special scanner is used to "snatch" legitimate phone numbers from the airwaves, i.e., the Electronic Serial Number (ESN) and Mobile Identification Number (MIN). See Denning and Baugh, 1997.

[13]Lashkar and its parent organization, Markaz-e-Dawa wal Irshad (Center for Islamic Invitation and Guidance), have raised so much money, mostly from sympathetic Wahhabis in Saudi Arabia, that they are reportedly planning to open their own bank. See Stern, 2000.

Networked Organizations and IT: Mitigating Factors

To be sure, there are limits to how much reliance terrorist networks will place on information-age technology. For the foreseeable future, electronically mediated coordination will not be able to entirely supplant face-to-face exchanges, because uncertainty and risk will continue to characterize most organizational choices and interactions among individuals.[14] Moreover, informal linkages and the shared values mentioned above—which are critical enablers of networked designs—can only be fostered through personal contact. As Nohria and Eccles argue,

> electronically mediated exchange can increase the range, amount, and velocity of information flow in a network organization. But the viability and effectiveness of this electronic network will depend critically on an underlying network of social relationships based on face-to-face interaction (Nohria and Eccles, "Face-to-Face: Making Network Organizations Work," in Nohria and Eccles, 1992, pp. 289–290).

Moreover, while IT-enabled communication flows can greatly help a network coordinate dispersed activities (thus increasing its flexibility and responsiveness), they can also present a security risk. Communication over electronic channels can become a liability, since it leaves digital "traces." For instance, FBI officials have recently acknowledged that they used an Internet wiretap program called "Carnivore" to track terrorist email correspondence at least 25 times. According to *Newsweek*, Carnivore's ability to track Osama bin Laden's email was critical in thwarting several of his strikes.[15]

The case of Ramzi Yousef, the World Trade Center bomber, also provides a revealing example of how information-age technology can represent a double-edged sword for terrorists. Yousef's numerous calls to fellow terrorists during his preparation for the strike were registered in phone companies' computer databases, providing law en-

[14]In fact, ambiguous and complex situations are still better tackled through direct communications, because face-to-face interaction is generally faster at resolving outstanding issues and leaves less room for misunderstandings.

[15]"Tracking Bin Laden's E-mail," *Newsweek*, August 21, 2000.

forcement officials with a significant set of leads for investigating terrorists in the Middle East and beyond. Prior to his arrest, Yousef unintentionally offered the FBI another source of information when he lost control of his portable computer in the Philippines. In that laptop, U.S. officials found incriminating data, including plans for future attacks, flight schedules, projected detonation times, and chemical formulae (Reeve, 1999, pp. 39 and 97).

There are other examples of how electronic information belonging to terrorist groups has fallen into the hands of law enforcement personnel. In 1995, Hamas's Abd-al-Rahman Zaydan was arrested and his computer seized—the computer contained a database of Hamas contact information that was used to apprehend other suspects (Soo Hoo, Goodman, and Greenberg, 1997, p. 139). In December 1999, 15 terrorists linked to Osama bin Laden were arrested in Jordan; along with bomb-making materials, rifles, and radio-controlled detonators, a number of computer disks were seized. Intelligence analysts were able to extract information about bomb building and terrorist training camps in Afghanistan.[16] In June 2000, the names of 19 suspects were found on computer disks recovered from a Hizbollah-controlled house (see FBIS, 2000). Finally, several encrypted computer records belonging to the millennialist Aum Shinrikyo cult were retrieved by Japanese authorities after an electronic key was recovered (Denning and Baugh, 1997).

Thus, the organizational benefits associated with greater IT must be traded off against the needs for direct human contact and improved security. This makes it likely that terrorist groups will adopt designs that fall short of fully connected, all-channel networks. Hybrids of hierarchies and networks may better reflect the relative costs and benefits of greater IT reliance—as well as further the group's mission.[17] Another important factor determining the adoption of IT by terrorist groups involves the relative attractiveness of high-tech offensive information operations, to which we turn next.

---

[16]"Terrorist Threats Target Asia," *Jane's Intelligence Review*, Vol. 12, No. 7, July 1, 2000.

[17]In fact, strategy is likely to be an important driver of organizational form and therefore of the density and richness of communications among group members. For instance, any mission calling for quick, dispersed, and simultaneous actions by several nodes could simply not be achieved without some IT support.

NETWAR, TERRORISM, AND OFFENSIVE INFORMATION OPERATIONS[18]

In addition to enabling networked forms of organization, IT can also improve terrorist intelligence collection and analysis, as well as offensive information operations (IO).[19] The acquisition by terrorist groups of an offensive IO capability could represent a significant threat as the world becomes more dependent on information and communications flows.[20] We argue that information-age technology can help terrorists conduct three broad types of offensive IO. First, it can aid them in their perception management and propaganda activities. Next, such technology can be used to attack virtual targets for disruptive purposes. Finally, IT can be used to cause physical destruction.[21]

Perception Management and Propaganda

Given the importance of knowledge and soft power to the conduct of netwar, it is not surprising that networked terrorists have already begun to leverage IT for perception management and propaganda to influence public opinion, recruit new members, and generate funding. Getting a message out and receiving extensive news media exposure are important components of terrorist strategy, which ultimately seeks to undermine the will of an opponent. In addition to such traditional media as television or print, the Internet now offers terrorist

---

[18]The formal Joint Staff and Army definition of information operations is "actions taken to affect adversary information and information systems and defend one's own." See Chairman of the Joint Chiefs of Staff, 1998, 1996a, and 1996b; and Department of the Army, 1997.

[19]For example, IT improves intelligence collection because potential targets can be researched on the Internet. Commercial satellite imagery is now offered by several firms at 1-meter resolution, and in January 2001, the U.S. government granted at least one commercial firm a license to sell 0.5-m imagery. Satellite photos can be used to identify security vulnerabilities in large targets like nuclear reactors. See Koch, 2001.

[20]For more on the importance of information across the spectrum of conflict, see John Arquilla and David Ronfeldt, "Cyberwar Is Coming," in Arquilla and Ronfeldt, 1997, p. 28; also, Arquilla and Ronfeldt, 1993.

[21]The following discussion draws from a variety of terrorist cases, some of which do not necessarily fit the netwar actor description (that is, they may not be networked, as in the case of Aum Shinrikyo). However, we believe they are all indicative of the trends that are starting to shape netwar terrorist offensive operations and that will continue to do so in the coming years.

groups an alternative way to reach out to the public, often with much more direct control over their message.

The news media play an integral part in a terrorist act because they are the conduit for news of the violence to the general population. As Bruce Hoffman has noted, "[t]errorism . . . may be seen as a violent act that is conceived specifically to attract attention and then, through the publicity it generates, to communicate a message" (Hoffman, 1998, p. 131). Terrorists have improved their media management techniques to the point of using "spin doctoring" tactics (Hoffman, 1998, p. 134). In fact, some groups have even acquired their own television and radio stations to take direct control of the reporting of events. Hizbollah, through its television station, has broadcast footage of strikes carried out by its operatives and has a sophisticated media center that regularly—and professionally—briefs foreign journalists. Hizbollah field units have even included specially designated cameramen to record dramatic video footage of Israeli casualties that was then aired in Lebanon and usually rebroadcast by Israeli television. (On these points, see Nacos, 1994.)

The Internet now expands the opportunities for publicity and exposure beyond the traditional limits of television and print media. Before the Internet, a bombing might be accompanied by a phone call or fax to the press by a terrorist claiming responsibility. Now, bombings can be followed—should terrorists so desire—by an immediate press release from their own web sites (at little cost). (For a hypothetical example, see Devost, Houghton, and Pollard, 1997.) The fact that many terrorists now have direct control over the content of their message offers further opportunities for perception management, as well as for image manipulation, special effects, and deception.

An Internet presence could prove advantageous for mobilizing "part-time cyberterrorists"—individuals not directly affiliated with a given terrorist group who nonetheless support its agenda and who use malicious software tools and instructions available at a terrorist web site. This scenario would closely resemble the initiatives taken by both the Israeli and Palestinian governments, which have encouraged private citizens to download computer attack tools and become involved in the conflict surrounding the al-Aqsa Intifadah (more on this below).

It appears that nearly all terrorist groups have a web presence (see Table 2.1 for a selection). As the table indicates, Hizbollah even manages multiple sites—each with a different purpose (for instance, www.hizbollah.org is the site of the central press office, www.moqawama.org describes attacks on Israeli targets, and www.almanar.com.lb contains news and information).

Web sites can also be used to refine or customize recruiting techniques. Recording which types of propaganda receive the most browser hits could help tailor a message for a particular audience. Using some of the same marketing techniques employed by commercial enterprises, terrorist servers could capture information about the users who browse their web sites, and then later contact those who seem most interested. Recruiters may also use more interactive Internet technology to roam online chat rooms and cyber cafes looking for

Table 2.1

Sample of Web Sites Belonging to Militant Islamist Groups

Group Name	Country of Origin	Web Address
Almurabeton	Egypt	www.almurabeton.org
Al-Jama'ah Al-Islamiyyah	Egypt	www.webstorage.com/~azzam/
Hizb Al-Ikhwan Al-Muslimoon (Muslim Brotherhood Movement)	Egypt	www.ummah.org.uk/ikhwan/
Hizbollah	Lebanon	www.hizbollah.org www.moqawama.org/page2/main.htm www.almanar.com.lb http://almashriq.hiof.no/lebanon/300/320/324/324.2/hizballah http://almashriq.hiof.no/lebanon/300/320/324/324.2/hizballah/emdad
Hamas (Harakat Muqama al-Islamiyya)	Palestianian Authority	www.palestine-info.net/hamas/

receptive members of the public, particularly young people. Electronic bulletin boards and user nets can also serve as vehicles for reaching out to potential recruits. Interested computer users around the world can be engaged in long-term "cyber relationships" that could lead to friendship and eventual membership.

Disruptive Attacks

Netwar-oriented terrorists can also use IT to launch disruptive attacks—that is, electronic strikes that temporarily disable, but do not destroy, physical and/or virtual infrastructure. If the ultimate goal of a terrorist is to influence his opponent's will to fight, IO offer additional means to exert influence beyond using simple physical attacks to cause terror. Disruptive attacks include "choking" computer systems through such tools as e-bombs, fax spamming, and hacking techniques to deface web sites. These strikes are usually nonlethal in nature, although they can wreak havoc and cause significant economic damage.

To date, disruptive strikes by terrorists have been relatively few and fairly unsophisticated—but they do seem to be increasing in frequency. For example, in 1996, the Liberation Tigers of Tamil Eelam (LTTE) launched an email bomb attack against Sri Lankan diplomatic missions. Using automated tools, the guerilla organization flooded Sri Lankan embassies with thousands of messages, thus establishing a "virtual blockade."[22] Japanese groups have allegedly attacked the computerized control systems for commuter trains, paralyzing major cities for hours (Devost, Houghton, and Pollard, 1997, p. 67). In 2000, a group of Pakistani hackers who call themselves the Muslim Online Syndicate (MOS) defaced more than 500 web sites in India to protest the conflict in Kashmir (see Hopper, 2000). Finally, Pakistan's Lashkar-e-Taiba claimed to have attacked Indian military web sites in early 2000.[23]

---

[22]See Dorothy Denning's discussion of virtual sit-ins and email bombs in Chapter Eight of this volume.

[23]Jessica Stern, telephone interview with author Michele Zanini, September 2000.

Disruptive rather than destructive actions take place for several reasons. For example, terrorists who rely on the Internet for perception management and communication purposes may prefer not to take "the Net" down, but rather to slow it down selectively. In addition, groups may want to rely on nonlethal cyber strikes to pressure governments without alienating their own constituent audiences. Terrorist groups may also follow the lead of criminal hackers and use the threat of disruptive attacks to blackmail and extort funds from private-sector entities (e.g., the ongoing "cyber jihad" against Israel may come to target commercial enterprises that do business with the Israelis).[24] For instance, in the early 1990s, hackers and criminals blackmailed brokerage houses and banks for several million British pounds. Money can also be stolen from individual users who visit terrorist web sites.[25]

Destructive Attacks

As mentioned earlier, IT-driven information operations can lead to the actual destruction of physical or virtual systems. Malicious viruses and worms can be used to permanently destroy (erase) or corrupt (spoof) data and cause economic damage. In the worst case, these same software tools can be used to cause destructive failure in a critical infrastructure like air traffic control, power, or water systems, which can lead to casualties. Indeed, it is likely that information operations that result in the loss of life may offer the same level of drama as physical attacks with bombs. Also, striking targets through electronic means does not carry the risks associated with using conventional weapons—such as handling explosives or being in close proximity to the target.

---

[24]A survey conducted by the Science Applications International Corp. in 1996 found that 40 major corporations reported losing over $800 million to computer break-ins. This example is cited on several web sites including Don Gotterbarn's web site at www-cs.etsu.edu/gotterbarn/stdntppr.

[25]A related criminal case reveals the potential for this threat. In 1997, a group known as the Chaos Computer Club created an Active X Control, which, when downloaded and run on the user's home computer, could trick the Quicken accounting program into removing money from a user's bank account. See "ActiveX Used as Hacking Tool," CNET News.com, February 7, 1997, http://news.cnet.com/news/0,10000,0-1005-200-316425,00.html.

Offensive IO: Mitigating Factors

The extreme case where the use of IT results in significant human losses has yet to occur. The lack of destructive information attacks is arguably influenced by the relative difficulty of electronically destroying (rather than disrupting) critical infrastructure components—the level of protection of existing infrastructure may be too high for terrorists to overcome with their current IT skill set. In fact, a terrorist organization would first have to overcome significant technical hurdles to develop an electronic attack capability. Concentrating the necessary technical expertise and equipment to damage or destroy targeted information systems is no easy task, given the computer security risks involved. In developing and increasing their reliance on electronic attacks, terrorist organizations may be assuming risks and costs associated with the relative novelty of the technology. Terrorists wishing to expand the scope of their offensive IO activities would have to continue upgrading and researching new technologies to keep up with the countermeasures available to computer security experts and systems administrators. This technology "treadmill" would demand constant attention and the diversion of scarce organizational resources.[26]

Another important determinant in netwar terrorists choosing low-level IT is that such conventional weapons as bombs remain more cost-effective. In fact, most terrorism experts believe that existing groups see their current tactics as sufficient and are not interested in branching into computer network attacks. Since current tactics are simple and successful, there is no built-in demand to innovate: bombing still works.[27] As long as current tactics enable these groups to accomplish their short-term goals and move toward their long-term goals, there will be no strong incentives to change behavior. In addition, the fragility of computer hardware may make a physical attack on these targets more attractive because such an attack is signifi-

[26]These points are also elaborated considerably in unpublished RAND research by Martin Libicki, James Mulvenon, and Zalmay Khalilzad on information warfare.

[27]As one article puts it, "the gun and the bomb continue to be the terrorists' main weapon of choice, as has been the case for more than a century." See Hoffman, Roy, and Benjamin, 2000, p. 163.

cantly less challenging from a technical standpoint than attempting a virtual attack (Soo Hoo, Goodman, and Greenberg, 1997, p. 146).

Disruptive attacks may be easier to carry out, but because of their very nature they do not produce the same kind of visceral and emotional reaction that the loss of human life does. Indeed, some terrorism analysts argue that it is unlikely that terrorist groups will turn to disruptive attacks as the primary tactic. Brian Jenkins points out that IT-enabled disruptive strikes

> do not produce the immediate, visible effects. There is no drama. No lives hang in the balance . . . . Terrorist intentions regarding cyberterrorism are even more problematic. Linking the objectives of actual terrorist groups to scenarios of electronic sabotage that would serve those objectives is conjecture.[28]

In addition, many computer security experts believe that even disruptive attacks remain technologically challenging for most terrorist groups and too undervalued by the media to make them attractive for terrorists (Soo Hoo, Goodman, and Greenberg, 1997, pp. 145–146).

EVALUATING PAST, PRESENT, AND FUTURE TRENDS

Given that information technology brings drawbacks as well as benefits, the terrorist groups examined here have not chosen to rely exclusively on IT to coordinate their operations and execute attacks. The available evidence suggests that netwar terrorists have embraced IT for organizational purposes, especially to facilitate C3, but they have been either unable or unwilling to attempt more ambitious offensive IO. However, the benefits clearly outweigh the risks when it comes to utilizing IT for perception management and propaganda. See Table 2.2 for a summary.

[28]Email correspondence from Brian Jenkins (at RAND) October 2000, who is quoting a forthcoming manuscript by Paul Pillar.

Table 2.2

Benefits and Drawbacks of IT Use for Netwar Terrorists (facilitating and mitigating factors)

IT Use	Facilitating	Mitigating
Organizational	Enables dispersed activities with reasonable secrecy, anonymity	Susceptibility to wire and wireless tapping
	Helps maintain a loose and flexible network	Digitally stored information can be easily retrievable unless well protected
	Lessens need for state sponsorship	Cannot by itself energize a network; common ideology and direct contact still essential
Offensive	Generally lower entry costs	Current bombing techniques already effective
	Eradication of national boundaries	Significant technical hurdles for disruptive and destructive IO
	Physically safer	Unique computer security risks impose recurring costs of "technology treadmill"
	Spillover benefits for recruitment/fundraising	

Future Developments in Information-Age Terrorism

Were the trends described above to persist, one could speculate that future netwar actors will continue to consolidate their IT use primarily for organizational purposes, with some emphasis on perception management on the offensive IO side. Under these conditions, networked terrorists would still rely on such traditional weapons as conventional bombs to cause physical violence. But they will also transmit information on how to build such weapons via CD-ROMs or email, use chat rooms to coordinate their activities, and use web sites to publicize and justify their strikes to a global audience.

The al-Aqsa Intifadah in the West Bank and Gaza highlights how protracted IO campaigns could be waged in conjunction with a campaign of conventional violence. Mirroring the real-world violence that has resulted in hundreds of casualties, a conflict has also been waged in cyberspace over economic and propaganda stakes. Palestinian hackers who support the al-Aqsa Intifadah have been waging a cyberjihad against Israeli government and commercial targets, defacing web sites and conducting DOS attacks. More than 40 Israeli sites have

been hit, including the Tel Aviv Stock Exchange and the Bank of Israel. Israeli hackers have counterattacked, hitting more than 15 different Palestinian targets, including Hizbollah, Hamas, and the Palestinian National Authority. As the disruptive attacks have escalated, individuals and groups have joined both sides, from professional hackers to "script-kiddies" (relative amateurs who rely on off-the-shelf and easy to use tools). (See Lemos, 2000.)

That said, the swift and unpredictable changes associated with technology suggest that other outcomes are possible. The question is, will terrorists have the desire and opportunity to significantly increase their reliance on IT—primarily for offensive purposes—in the future? Several factors could influence such a shift, including the degree to which new technology will serve their main strategic goals in a safe and effective manner.[29] For instance, the introduction of easy-to-use, "unbreakable" encryption programs to support email and file exchange will encourage netwar terrorists to adopt such techniques. Moreover, terrorist access to technologies that can be readily employed without extensive internal development efforts[30]—by group members and part-time "volunteers" or through "hackers for hire"[31]—will be a critical facilitating factor. Equally important, the relative vulnerability of the information infrastructure plays a role in this calculus (more on this below).

These possible developments would likely prompt the evolution of current netwar terrorist groups toward greater reliance on IT for offensive purposes and could also encourage the emergence of new and completely virtual groups that exclusively operate in cyberspace. Each possibility is described briefly below.

---

[29]From a strategic perspective, the more that terrorist groups emphasize swarming doctrines to conduct dispersed and simultaneous operations, the greater the need for a sophisticated IT infrastructure.

[30]One example is Netcat, a free hacking tool made available in 1996. See Soo Hoo, Goodman, and Greenberg, 1997, p. 141.

[31]Rumors persist that people proficient in network attacks are available for hire. Press reports indicate that hacker groups have been approached by anonymous users claiming to be terrorists who have requested help gaining access to government classified information networks such as SIPRNET. For example, one teenage hacker was said to have received a $1,000 check. See McKay, 1998.

The Evolution of Current Groups

As Brian Jackson notes, the introduction of new technologies in an organization follows a complex and often lengthy process. Not only do innovative systems have to be developed or acquired, but organizational actors have to become familiar with new systems and be able to use them effectively (Jackson, unpublished). Given the challenge, terrorist groups are likely to channel their scarce organizational resources to acquire those IT skills that have the greatest leverage for the least amount of cost and effort.

This line of reasoning can help explain terrorists' recent emphasis on using communications technology for organizational purposes: Having access to the Internet and cellular telephones is not overly complicated, and it plays a significant role in enabling dispersed operations, a key goal of netwar groups. This reasoning also suggests that over time terrorist groups might begin to experiment more aggressively with information-age technologies for offensive information operations, as they become more familiar with such innovations. Indeed, some may follow a "migration" pattern as illustrated in Figure 2.1: The knowledge of IT issues gained by relying on technology to fa-

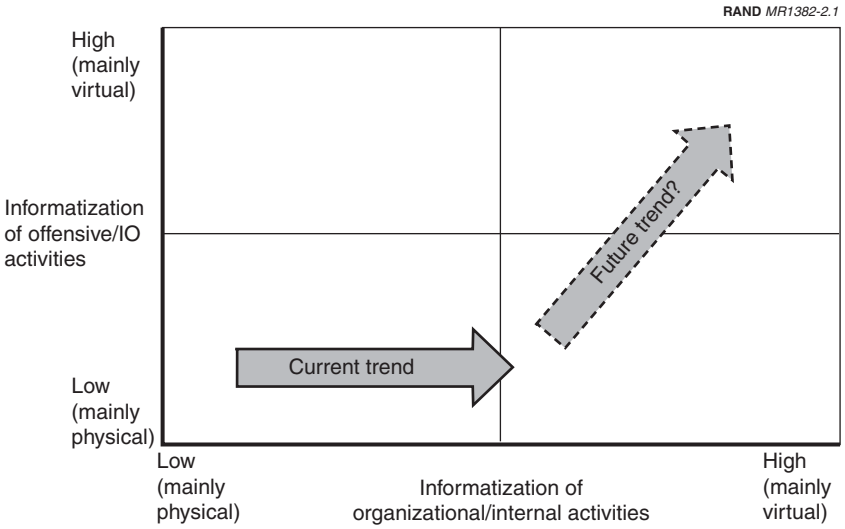

Figure 2.1—Possible Shifts in the Use of Technology

cilitate interactions among group members, or to gain a web presence, might eventually be expanded and harnessed for increasingly offensive uses.

The pace with which current groups move through such a path is also dependent on the degree of cooperation and information exchange among netwar terrorists. Such cooperation has often occurred in the past—for instance, Islamic radicals have organized "terror conferences"(Kushner, 1998, p. 41), while European terrorist groups such as the Irish Republican Army entered into joint ventures with counterparts across the globe to learn from one another and disseminate knowledge (such as designs of booby traps and radio-controlled bombs). (See Wilkinson, 1986, p. 40.) Given the loose and reciprocal nature of ties between actors in networks such as al-Qaeda, it is entirely possible that those with IT skills would be leveraged globally and placed at the disposal of the organization's various members.

Lastly, as leading-edge groups begin to move toward the upper-right quadrant of Figure 2.1, other groups may be tempted to follow suit: Terrorists that hitherto had decided to adopt a low-technology profile for their offensive operations could be emboldened by successful instances of IT attacks by others (Jackson, unpublished).

The Emergence of New Groups

An alternative hypothesis to the notion that existing terrorist groups should be watched for signs of movement toward cyberterror is that qualitative improvements in the informatization of networked terrorists will only be witnessed with the emergence of newer, and more technologically savvy, groups. Just as Hamas and al-Qaeda have overshadowed the PFLP and other Marxist groups formed in the 1960s, new-generation groups may further advance the trend toward networked and IT-reliant organizations. New groups could even be led by individuals who are technically skilled, suggesting the rise of a hybrid breed of "terrorists cum hackers." Like hackers, they would undertake most of their attacks in cyberspace. Like terrorists, they would seek to strike targets by both disruptive and destructive means to further a political or religious agenda.

The possibility that innovation will take place only with the advent of new groups finds support in previous work by such terrorism experts as Hoffman, who describes most groups today as operationally conservative (Hoffman, "Terrorism Trends and Prospects" in Lesser et al., 1999, p. 36). Aside from organizational inertia, current groups may also be hesitant to further rely on IT for offensive purpose because of large, "sunk costs" in traditional tactics, training, and weapon stockpiles. Existing groups wishing to "amortize" such capital cost may be unwilling to direct scarce resources toward the development of new and radically different offensive techniques.

POLICY IMPLICATIONS

The acquisition and use of information-age technology by terrorist groups are far from certain. Indeed, the scenarios painted above are not mutually exclusive. It is conceivable that current groups will acquire new IT skills over time and adopt more-offensive IT strategies. New hacker/terrorist groups may also emerge to compound this problem. Some terrorist networks may even become sophisticated enough to sustain and coordinate offensive campaigns in both the virtual and physical realms.

What is certain, however, is that counterterrorism policy will be able to counter the dangers associated with terrorist IT use only if it becomes attuned to the information age. Counterterrorist policies and tactics could even alter the speed with which terrorists become informatized—groups facing a robust counterterrorism campaign may have less time and resources to acquire new technologies (see Jackson, unpublished). For such reasons, it seems advisable that counterterrorism policymakers and strategists bear in mind the following recommendations.

First, monitor changes in the use of IT by terrorist groups, differentiating between organizational and offensive capabilities. Counterterrorism policies will have to take into account the type of IT capabilities developed by each group, targeting their specific technological vulnerabilities. Evaluating how IT shapes a group's organizational processes and offensive activities will remain a critical component of the threat assessment. Monitoring the shift in capabilities for each type of

IT use and then examining trends in the aggregate can also help forecast future terrorist behavior.

Among the most significant trends to be carefully examined is the possible emergence of a new, and potentially dangerous, breed of terrorists—groups that are highly informatized along both the organizational and offensive axes. In this regard, a number of "signposts" should be identified and tracked. These would include significant increases in the level of technical expertise of known leaders and their subordinates, increases in the frequency of disruptive attacks, increases in the seizures of IT equipment owned by terrorists, the presence—and successful recruiting—of "hackers for hire," and the availability of effective and relatively secure off-the-shelf information technologies (including those that facilitate hacking).

Second, target information flows. Since network designs are inherently information intensive, counterterrorism efforts should target the information flows of netwar groups. Intercepting and monitoring terrorist information exchanges should remain a top priority, and the implementation of "Project Trailblazer" by the National Security Agency—to develop a system that can crack new encryption software, fiber-optic cables, and cellular phone transmissions—represents a useful addition to America's signals intelligence capability (Kitfield, 2000).

Equally important, policymakers should consider going beyond the passive monitoring of information flows and toward the active disruption of such communications. To the degree that erroneous or otherwise misleading information is planted into a network's information flows by what are seemingly credible sources, over time the integrity and relevance of the network itself will be compromised. This in turn could breed distrust and further cripple a group's ability to operate in a dispersed and decentralized fashion—essentially eliminating a netwar group's key competitive advantage.

Increased emphasis on targeting information flows should not exclude nonelectronic efforts to gather intelligence and undermine the network. Indeed, human intelligence will remain an important tool for intercepting (and injecting) information not transmitted through

electronic means of communication.[32] This is an especially pressing concern, given that several intelligence observers have pointed to a lack of U.S. capability in this area.

Third, deter IT-based offensive IO through better infrastructure protection. Changes in the vulnerability of critical infrastructures can significantly alter a terrorist's IT calculus. If such infrastructures, such as those that manage air traffic control, were to become relatively more vulnerable, they might become more attractive as targets: Terrorists could strike at a distance, generating as much—if not more—destruction as would have been caused by the use of traditional weapons. U.S. policy should identify specific vulnerabilities to expected threats and develop security techniques that mitigate each. An analysis of these issues is beyond the scope of the current chapter, but there are numerous studies that explore this process, including RAND's *Securing the U.S. Defense Information Infrastructure: A Proposed Approach* (Anderson et al., 1999). The FBI's National Infrastructure Protection Center and other newly created organizations represent useful steps in this direction. Counterterrorist agencies may also want to consider the option of employing a large number of hackers and leveraging their knowledge for defensive and possibly even retaliatory purposes.

Fourth, beat networked terrorists at their own game: "It takes networks to fight networks." Governments wishing to counter netwar terrorism will need to adopt organizational designs and strategies like those of their adversaries. This does not mean mirroring the opponent, but rather learning to draw on the same design principles of network forms. These principles depend to some extent upon technological innovation, but mainly on a willingness to innovate organizationally and doctrinally and by building new mechanisms for interagency and multijurisdictional cooperation. The Technical Support Working Group (TSWG) is a good example of a nontraditional government interagency group with more than 100 member organizations from at least 13 federal agencies and a growing number of local and state agencies. Its principal aim is to help develop and deploy technologies

[32]After Osama bin Laden noticed that his satellite phone connection was no longer secure, he began to use human couriers to pass information and instructions to his operatives.

to combat terrorism.[33] Another example is the Counter-Intelligence 21 (CI-21) plan, a set of reforms that seek to increase the level of cooperation between counterintelligence personnel at the CIA, FBI, and the Pentagon (Kitfield, 2000). If counterterrorism agencies become ready and willing to rely on networks of outside "ethical hackers" in times of crisis, the need to coordinate beyond the boundaries of government will increase.[34]

Supporters of these initiatives rightly recognize that the information age and the consequent advent of netwar have blurred the boundary between domestic and international threats, as well as between civilian and military threats. This in turn demands greater interagency coordination within the counterterrorism community. As terrorist groups evolve toward loose, ad-hoc networks that form and dissipate unpredictably, so must counterterrorism forces adopt a more flexible approach that crosses bureaucratic boundaries to accomplish the mission at hand. While militaries and governments will never be able to do away with their hierarchies entirely, there is nevertheless much room for them to develop more-robust organizational networks than they currently have—a change that may offset some, if not all, of the advantage now accruing mostly to networked terrorist groups.

BIBLIOGRAPHY

Anderson, Robert H., Phillip M. Feldman, Scott Gerwehr, Brian Houghton, Richard Mesic, John D. Pinder, Jeff Rothenberg, and James Chiesa, *Securing the U.S. Defense Information Infrastructure:*

[33]TSWG received $48 million in fiscal year 2000. Traditional terrorist threats such as bombs still generate the greatest concern, and most of TSWG's budget covers needs such as blast mitigation. See Stanton, 2000, p. 24.

[34]In some cases, hackers may be spontaneously driven to aid law enforcement officials in defending against particularly objectionable crimes. For instance, a group called Ethical Hackers Against Pedophilia has been created to identify and urge punishment of people who publish child pornography on the Internet (see www.ehap.org). The government could take the lead in mobilizing existing ethical hackers in the private sector to help in times of crisis. This would be different from deliberately organizing a virtual militia composed of relatively unsophisticated citizens armed with off-the-shelf hacking tools—something the Israeli government *has* experimented with during the al-Aqsa Intifadah. Given this option's potential to become a double-edged sword—as well as lack of information on its efficacy—more research on this topic is warranted.

A Proposed Approach, Santa Monica, Calif.: RAND, MR-993-OSD/NSA/DARPA, 1999.

Arquilla, John, and David F. Ronfeldt, *The Advent of Netwar,* Santa Monica, Calif.: RAND, MR-789-OSD, 1996.

Arquilla, John, and David F. Ronfeldt, "Cyberwar Is Coming," *Comparative Strategy*, Vol. 12, No. 2, Summer 1993, pp. 141–165. Available as RAND reprint RP-223.

Arquilla, John, and David Ronfeldt , eds., *In Athena's Camp: Preparing for Conflict in the Information Age,* Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997.

Bremer, Paul L. III, et al., *Countering the Changing Threat of International Terrorism,* Washington, D.C.: National Commission on Terrorism, 2000, www.fas.org/irp/threat/commission.html (August 28, 2000).

Burns, Tom, and G. M. Stalker, *The Management of Innovation,* London: Tavistock, 1961.

Cameron, Gavin, "Multi-Track Microproliferation: Lessons from Aum Shinrikyo and Al Qaida," *Studies in Conflict & Terrorism*, Vol. 22, 1999.

Chairman of the Joint Chiefs of Staff, *Doctrine for Joint Psychological Operations*, Joint Pub 3-53, Washington, D.C.: United States Government Printing Office, July 10, 1996a.

Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Command and Control Warfare (C2W)*, Joint Pub 3-13.1, Washington, D.C.: United States Government Printing Office, February 7, 1996b.

Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13, Washington, D.C.: United States Government Printing Office, October 9, 1998.

Denning, Dorothy E., "Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy," 1999, www.nautilus.org/info-policy/workshop/papers/denning.html (January 23, 2001).

Denning, Dorothy E., and William E. Baugh, Jr., *Cases Involving Encryption in Crime and Terrorism*, 1997, www.cs.georgetown.edu/~denning/crypto/cases.html (January 23, 2001).

Denning, Dorothy E., and William E. Baugh, Jr., *Encryption and Evolving Technologies As Tools of Organized Crime and Terrorism,* Washington, D.C.: U.S. Working Group on Organized Crime (WGOC), National Strategy Information Center, 1997.

Department of the Army, *Public Affairs Operations*, Field Manual FM 46-1, Washington, D.C.: United States Government Printing Office, May 30, 1997.

Devost, Matthew G., Brian K. Houghton, and Neal A. Pollard, "Information Terrorism: Can You Trust Your Toaster?" in Robert E. Neilson, ed., *Sun Tzu and Information Warfare*, Washington, D.C.: National Defense University Press, 1997.

Drogin, Bob, "State Dept. Report Cites Growing Reach of Bin Laden," *Los Angeles Times*, May 2, 2000.

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

FBIS, "Arab Afghans Reportedly Transfer Operations to Somalia," *Cairo Al-Arabi*, 10 March 1997b, p. 1, FBIS-TOT-97-073.

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

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

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

FBIS, "Trial of 19 Hizbullah Members Begins in Istanbul," June 2000, FBIS-WEU-2000-0612.

Heydebrand, Wolf V., "New Organizational Forms," *Work and Occupations*, Vol. 16, No. 3, August 1989, pp. 323–357.

Hoffman, Bruce, *Inside Terrorism,* New York: Columbia University Press, 1998.

Hoffman, Bruce, Olivier Roy, and Daniel Benjamin, "America and the New Terrorism: An Exchange," *Survival*, Vol. 42, No. 2, Summer 2000.

Hopper, D. Ian, "Kashmir Conflict Continues to Escalate—Online," *CNN*, March 20, 2000, www.cnn.com (September 5, 2000).

Iuris, Andre Pienaar, "Information Terrorism," in Amelia Humphreys, ed., *Terrorism: A Global Survey: A Special Report for Jane's Intelligence Review and Jane's Sentinel,* Alexandria, Va.: Jane's Information Group, 1997.

Jackson, Brian, unpublished RAND research on technology acquisition by terrorist groups.

Kelley, Jack, "U.S. Acquires Reputed Terrorism Guide," *USA Today*, September 18, 2000.

Kitfield, James, "Covert Counterattack," *National Journal*, September 16, 2000.

Koch, Andrew, "Space Imaging Gets .5m Go Ahead," *Jane's Defence Weekly*, January 10, 2001.

Kurlantzick, Joshua, "Muslim Separatists in Global Network of Terrorist Groups," *Washington Times*, May 2, 2000.

Kushner, H. W., *Terrorism in America: A Structured Approach to Understanding the Terrorist Threat,* Springfield, Ill.: Charles C. Thomas, 1998.

Laqueur, Walter, *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, New York: Oxford University Press, 1996.

Lemos, Robert, "Hacktivism: Mideast Cyberwar Heats Up," *ZDNet News*, November 6, 2000, www.zdnet.com (December 4, 2000).

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Jenkins, *Countering the New Terrorism*, Santa Monica, Calif.: RAND, MR-989-AF, 1999.

McKay, Niall, "Do Terrorists Troll the Net?" *Wired News*, November 1998, www.wired.com (September 15, 2000).

Monge, Peter, and Janet Fulk, "Communication Technology for Global Network Organizations," in Gerardine Desanctis and Janet Fulk, eds., *Shaping Organizational Form: Communication, Connection, and Community*, Thousand Oaks, Calif.: Sage, 1999.

Nacos, Brigitte, *Terrorism and the Media,* New York: Columbia University Press, 1994.

Nohria, Nitin, and Robert Eccles, eds.*, Networks and Organizations*, Boston, Mass.: Harvard Business School Press, 1992.

Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism: 1999,* Washington, D.C.: U.S. Department of State, Publication #10687, 2000.

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

Reeve, Simon, *The New Jackals: Ramzi Yousef, Osama Bin Laden and the Future of Terrorism*, Boston, Mass.: Northeastern University Press, 1999.

Simon, Steven, and Daniel Benjamin, "America and the New Terrorism," *Survival*, Vol. 42, No. 1, Spring 2000.

Soo Hoo, Kevin, Seymour Goodman, and Lawrence Greenberg, "Information Technology and the Terrorist Threat," *Survival*, Vol. 39, No. 3, Autumn 1997, pp. 135–155.

Stanton, John J., "A Typical Pentagon Agency Waging War on Terrorism," *National Defense*, May 2000.

Stern, Jessica, "Pakistan's Jihad Culture," *Foreign Affairs*, November/December 2000, pp. 115–126.

"Terrorist Threats Target Asia," *Jane's Intelligence Review,* Vol. 12, No. 7, July 1, 2000.

Thompson, James D., *Organizations in Action*, New York: McGraw-Hill, 1967.

Whine, Michael, "Islamist Organizations on the Internet," *Terrorism and Political Violence*, Vol. 11, No. 1, Spring 1999.

Wilkinson, P., "Terrorism: International Dimensions," in W. Gutteridge, ed., *Contemporary Terrorism,* New York: Facts on File Publications, 1986.