Chapter Two

THE ADVENT OF NETWAR: ANALYTIC BACKGROUND

The information revolution is altering the nature of conflict across the spectrum. There are many reasons for this, but we would call attention to two in particular.[1]

First, the information revolution is favoring and strengthening network forms of organization, while simultaneously making life difficult for old hierarchical forms. The rise of networks—especially "all-channel" networks, in which every node is connected to every other node—means that power is migrating to nonstate actors, who are able to organize into sprawling multiorganizational networks more readily than traditional, hierarchical, state actors can. This means that conflicts will increasingly be waged by "networks," perhaps more than by "hierarchies." It also means that whoever masters the network form stands to gain major advantages.

Second, as the information revolution deepens, conflicts increasingly depend on information and communications matters. More than ever before, conflicts are about "knowledge"—about who knows (or can be kept from knowing) what, when, where, and why. Conflicts will revolve less around the use of raw power than of "soft power" (Nye, 1990; Nye and Owens, 1996), as applied through "information operations" and "perception management"—that is, media-oriented measures that aim to attract rather than coerce and that affect how

[1]While all the co-authors contributed to this chapter, the analytical background is mostly drawn, often verbatim, from Arquilla and Ronfeldt (1996b). For additional discussion of new views of "information" and "power," see Arquilla and Ronfeldt (1996a). Also see Toffler and Toffler (1993).

secure a society, a military, or other actor feels about its knowledge of itself and its adversaries. Psychosocial disruption may become more important than physical destruction.

These propositions cut cross the entire conflict spectrum. Major transformations are thus looming in the nature of adversaries, in the kinds of threats they may pose, and in how conflicts can be waged. Information-age threats are likely to be more diffuse, dispersed, nonlinear, multidimensional, and ambiguous than industrial-age threats. Metaphorically, future conflicts may resemble the Eastern game of go more than the Western game of chess.

As a result, the information-age conflict spectrum increasingly looks like this:

- *Cyberwar*—a concept that refers to information-oriented military warfare (Arquilla and Ronfeldt, 1993, 1997)[2]—is becoming an important entry at the military end of the spectrum, where the language is normally about high-intensity conflicts (HICs) and middle-range conflicts (MRCs).[3]
- *Netwar* (Arquilla and Ronfeldt, 1996b, 1997) figures increasingly at the societal end of the spectrum, where the language is normally about small-scale contingencies (SSCs)—recently known as low-intensity conflict (LIC) and operations other than war (OOTW)—and nonmilitary modes of conflict (and crime).

---

[2]The term *cyberwar* is taking on a life of its own. Arquilla and Ronfeldt (1993) offer the original definition, followed by a more refined one (1997), reflecting a broad perspective as to how the information revolution implies the redesign of military organization, doctrine, and strategy. A cover story in *Time* magazine in 1995 and the book by Campen, Dearth, and Goodden (1996) reflect the original definition, but give it a high-tech flavor. Continuing this trend, Molander, Riddile, and Wilson (1996) narrow it to a synonym for "strategic information warfare" (SIW), mainly meaning attacks on computerized infrastructures for information and communications. But in our view, cyberwar may or may not involve SIW—and it may involve a lot more than SIW. The effort to reduce cyberwar to a high-tech activity neglects the broader dimensions of military organization, doctrine, and strategy, and the ways that they gain importance in the information age. As discussed later, a reductionist view is also affecting the term *netwar*, where it is taken to refer only to war on the Internet—another mistake, in our view.

[3]MRC is also used to refer to major regional conflict. That term is now giving way to major theater war (MTW).

Whereas cyberwar usually pits formal military forces against each other, netwar is more likely to involve nonstate, paramilitary, and irregular forces. Both concepts are consistent with the views of analysts like Martin Van Creveld (1991) who believe that a "transformation of war" is under way. Neither concept is simply about technology; both refer to *comprehensive* approaches to conflict based on the centrality of information—comprehensive in that they combine organizational, doctrinal, strategic, tactical, and technological innovations, for offense and defense.

DEFINITION OF NETWAR

To be more precise, the term *netwar* refers to an emerging mode of conflict (and crime) at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command. Thus, netwar differs from modes of conflict and crime in which the protagonists prefer hierarchical organizations, doctrines, and strategies, as in past efforts to build, for example, centralized movements along Leninist lines. Netwar is about the Middle East's Hamas more than the Palestine Liberation Organization (PLO), Mexico's Zapatistas more than Cuba's Fidelistas, and America's Christian Patriot movement more than the Ku Klux Klan.[4] It is also about the Asian Triads more than the Sicilian Mafia, and Chicago's "Gangsta Disciples" more than the Al Capone Gang.

The term is meant to call attention to the prospect that network-based conflict and crime will become major phenomena in the decades ahead. Various actors across the spectrum of conflict and crime are already evolving in the direction of netwar. This includes familiar adversaries who are modifying their structures and strategies to take advantage of networked designs: e.g., transnational terrorist

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

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, rural militia organizations, and militant single-issue groups in the United States are also developing netwar-like attributes. The netwar spectrum also includes a new generation of revolutionaries, radicals, and activists who are just beginning to create information-age ideologies, in which identities and loyalties may shift from the nation-state to the transnational level of "global civil society." New kinds of actors, such as anarchistic and nihilistic leagues of computer-hacking "cyboteurs," may also partake of netwar.

Many if not most netwar actors will be nonstate, even stateless. Some may be agents of a state, but others may try to turn states into *their* agents. Moreover, a netwar actor may be both subnational and transnational in scope. Odd hybrids and symbioses are likely. Furthermore, some actors (e.g., violent terrorist and criminal organizations) may threaten U.S. and other nations' interests, but other actors (e.g., peaceful NGO activists) may not. Some actors may aim at destruction, but more may aim mainly at disruption. Again, many variations are possible.

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

Caveats About the Role of Technology

Netwar is a result of the rise of network forms of organization, which in turn is a result of the computerized information revolution.[5] To realize its potential, any kind of 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 is afforded by the latest information and communication technologies—cellular telephones, fax machines, electronic mail

[5]For explanation of this point, see Ronfeldt (1996) and Arquilla and Ronfeldt (1996b), not to mention other sources cited in those documents.

(e-mail), World Wide Web (WWW) sites, and computer conferencing. Such technologies are highly advantageous for a netwar actor.

But a couple of caveats are in order. First, the new technologies, however enabling for organizational networking, may not be the only crucial technologies for a netwar actor. Old technologies, like human couriers, and mixes of old and new systems may, in some situations, do the job.

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 key *battles* may occur there, but a *war's* overall conduct and outcome will normally depend mostly on what happens in the "real world"—and this will continue to be, even in information-age conflicts, generally more important than what happens in cyberspace or the infosphere.[6]

Efforts to reduce the netwar concept to being just about Internet-war should be guarded against, along with other efforts to reduce the cyberwar concept to being 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 if not error-prone tendency.[7]

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. As the scholarly literature instructs (e.g., Evan, 1972), networks come in basically three types (or topologies):

---

[6]Paul Kneisel, "Netwar: The Battle Over Rec.Music.White-Power," *ANTIFA INFO-BULLETIN*, Research Supplement, June 12, 1996; unpaginated ascii text available on the Internet. 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*.

[7]See footnote 2, and Arquilla and Ronfeldt (1997, ch. 1).

- the *chain* network, as in a migration or smuggling chain where people, goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes;
- the *star*, hub, or wheel network, as in a franchise or a cartel structure where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other;
- the *all-channel* network, as in a collaborative network of militant peace groups where everybody is connected to everybody else.

See Figure 1. Each node indicated in the diagrams may refer to an individual, a group, an institution, part of a group or institution, or even a state. The nodes may be large or small, tightly or loosely coupled, and 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 may be well defined, or they may be blurred and porous in relation to the outside environment.

Each design is suited to different conditions and purposes, and all three may be found among netwar-related adversaries: e.g., the chain in smuggling operations; the star among criminal syndicates;

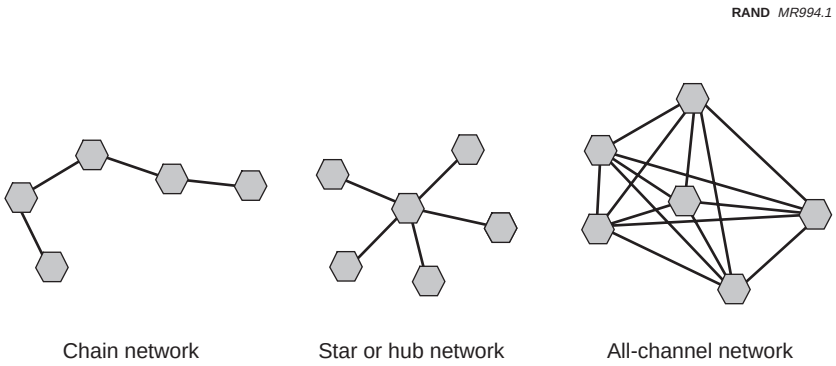

Figure 1—Types of Networks

and the all-channel 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 stars 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. Many combinations and configurations are possible.

Of the three, the all-channel type has been the most difficult to organize and sustain, partly because of the dense communications it may require. But it is the type that gives the network form its new, high potential for collaborative undertakings. It is the type that is gaining new strength from the information revolution. And it is the type that we generally refer to in this study—and in the remainder of this chapter.

Pictorially, then, such a netwar actor resembles a geodesic "Bucky ball" (named for Buckminster Fuller); it does not look like a pyramid.[8] 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 look acephalous (headless) at times, and polycephalous (Hydra-headed) at other times, though not all nodes may be "created equal." In other words, it is a heterarchy, or what may be better termed a "panarchy."

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

[8]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.

principles, shaped through mutual consultation and consensus building, can enable them to be "all of one mind" even though they are dispersed and devoted to different tasks. It can provide a central ideational, strategic, and operational coherence that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that the members do not have to resort to a hierarchy—"they know what they have to do."[9]

The design depends on the network having a capacity—indeed, a well-developed infrastructure—for the dense communication of functional information. This does not mean that all nodes must be in constant communication; that may not make sense for a secretive, conspiratorial actor. But when communication is needed, the network's members must be able to disseminate information promptly and as broadly as desired within the network and to outside audiences.

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.[10]

---

[9]The phrase in quotation marks reflects a doctrinal statement by Beam (1992) about "Leaderless Resistance," which has strongly influenced right-wing white-power groups.

[10]This 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 that are now coming into focus in the analysis of not only social movements but also some terrorist, criminal, ethnonationalist, and fundamentalist organizations.

Swarming, and the Blurring of Offense and Defense

This distinctive, often ad hoc design has unusual strengths, for both offense and defense. On the offense, networks are known for being adaptable, flexible, and versatile vis-à-vis opportunities and challenges. This may be particularly the case where a set of actors can engage in *swarming*. Little analytic attention has been given to swarming, yet it may become the key mode of conflict in the information age, and the cutting edge for this possibility is found among netwar protagonists.[11]

Swarming occurs when the dispersed nodes of a network of small (and perhaps some large) forces can 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."

Swarming may be most effective, and difficult to defend against, where a set of netwar actors do not have to "mass" their forces but can engage in "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 go after any discrete issue area that arises—human rights, democracy, the environment, rural development, and so forth.

In terms of defensive potential, networks tend to be redundant and diverse, making them robust and resilient in the face of adversity. Where they have a capacity for interoperability and shun centralized command and control, network designs can be difficult to crack and defeat as a whole. In particular, they may defy counterleadership targeting. This limits whoever would attack a network—generally, they can find and confront only portions of it. Moreover, the deniability built into a network affords the possibility that it may simply

---

[11]Swarm networks, and the capacity of networks for swarming, are raised by Kelly (1994). For recent thinking about swarming, see Arquilla and Ronfeldt (1997).

absorb a number of attacks on distributed nodes, leading the attacker to believe the network has been harmed when, in fact, it remains viable, and is seeking new opportunities for tactical surprise.

The difficulty of dealing with netwar actors is deepened 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. As we shall discuss, 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, where guerrillas are on the defensive strategically, they may go on the offense tactically; the war of the *mujahideen* in Afghanistan provides a modern example.

Operating in the Cracks

The blurring of offense and defense reflects another feature of netwar: It tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal. This makes it difficult if not nigh impossible for a government to assign to a single agency—e.g., military, police, or intelligence—the responsibility for responding.

As Colonel Richard Szafranski (1994, 1995) illuminates in discussing 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 social netwar tends 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 quite problematic.

Thus, the spread of netwar adds to the challenges facing the nation-state in the information age. Traditionally, ideals of sovereignty and authority are linked to a bureaucratic rationality 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

Against this background, the emerging theory and practice of netwar involves a set of general propositions about the information revolution and its implications for netwar and *counternetwar* (Arquilla and Ronfeldt, 1993, 1996b):[12]

Hierarchies have a difficult time fighting networks. Examples of this exist 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 the robustness of the network form on defense and offense. 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 would defend against netwar will, increasingly, have to adopt organizational designs and strategies like those of their adversaries. This does not

[12]Also see Berger (1998) for additional thinking and analysis about such propositions.

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 upon 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 have advanced at networking (be they criminals, terrorists, or peaceful social activists) 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 Hamas and the Cali cartel illustrate this; so does the Zapatista movement in Mexico.

An implication for governments is that counternetwar may 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, where relevant, 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 terrorists, militias, criminals, or other actors. (For elaboration, see Arquilla and Ronfeldt (1997), ch. 19.)

VARIETIES OF NETWAR

Netwar is a deduced concept—it derives from our thinking about the effects and implications of the information revolution. Once coined, the concept has helped us see 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 terrorists, guerrillas, crimi-

nals, and activists.[13] In noting this, we are not equating terrorists, guerrillas, criminals, or activists with each other—each has different dynamics. Nor do we mean to tarnish social activism, which has many positive aspects for civil society.[14] We are simply calling 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.

Terrorist and Criminal Netwar

Terrorism continues to evolve in the direction of violent netwar (see Arquilla, Ronfeldt, and Zanini, forthcoming). Islamic fundamentalist organizations like Hamas, as well as right-wing militias and extremist groups in the United States that rely on a doctrine of "leaderless resistance" propounded by Aryan nationalist Louis Beam (Beam, 1992; Stern, 1996), consist of groups organized in loosely interconnected, semi-independent cells that have no single commanding hierarchy above them.[15] Hamas exemplifies the shift away from a hierarchically oriented movement based on a "great leader" (like the PLO and Yassir Arafat). Instead, Hamas is characterized by "a loose network of cells without a strict hierarchy or central base." As Israeli General David Agmon has noted, "Hamas is not one organization, but many [which are] connected in a sort of network to other such groups."[16] More to the point, Hamas's organization is "cellular; very loosely structured, with some elements working openly through mosques and social service institutions to recruit members, raise money, organize activities, and distribute propaganda; other elements operate clandestinely, advocating and using violence" (Builta, 1996, pp. 776,

---

[13]These are not the only types of netwar actors; there are others. For example, corporations may also engage in netwars.

[14]See the discussion in Ronfeldt (1996).

[15]The *New York Times* and *Los Angeles Times* insightfully covered this trend among Islamic fundamentalist groups in 1996. See John Kifner, "Alms and Arms: Tactics in a Holy War," *The New York Times,* Friday, March 15, 1996, pp. A-1, A-6, A-7; and John-Thor Dahlburg, "Technology Lets Tentacles of Terrorism Extend Reach," *Los Angeles Times,* Tuesday, August 6, 1996, pp. A-1, A-10, A-11.

[16]Material quoted from Nicolas B. Tatro, "Loose Structure Helps Make Hamas Elusive," *Associated Press,* March 13, 1996.

781). Also, Hamas has numerous "network contacts" to other terrorist groups (e.g., Hizbollah, al-Nahda, Muslim Brotherhood), to nonstate organizations like the U.S. Nation of Islam, and to states (e.g., Iran, Syria).

As for criminal netwar, transnational criminal organizations (TCOs) are gaining strength around the world largely because they are so adept at building networks to take advantage of global interconnections (Sterling, 1994; Williams, 1994). Phil Williams describes these TCOs in words that could also apply to terrorist organizations:

> TCOs are diverse in structure, outlook and membership. What they have in common is that they are highly mobile and adaptable and are able to operate across national borders with great ease. . . . They are able to do this partly because of the conditions identified above and partly because of their emphasis on networks rather than formal organizations. (Williams, 1994, p. 105.)

Social Netwar

Analytically, much the same may be said about social netwar, the focus of this study. Militant social activists, even though their purposes, strategies, and tactics are far removed from those of terrorists and criminals, are increasingly organized into transnational "issue-networks." According to Kathryn Sikkink's work on the rise of human-rights networks:

> An international issue-network comprises a set of organizations, bound by shared values and by dense exchanges of information and services, working internationally on an issue. . . . [I]nternational and domestic NGOs play a central role in all issue-networks. They are the most proactive members of the networks, usually initiating actions and pressuring more powerful actors to take positions. . . . As a result of this exchange of information and services, of flows of funds, and of shared norms and goals, the members of the issue-network work together in a constant but informal, uncoordinated, and nonhierarchical manner. (Sikkink, 1993, pp. 415–417.)

As for doctrine and strategy, human-rights issue-networks operate "by changing the information environment in which state actors work" (Sikkink, 1993, p. 441). While NGO activists may want to shape

the information environment in a distant conflict zone and in the offices of the local government, it may be even more important for them to affect the information environment abroad, notably in Washington, D.C., and in the global media.[17] As Sikkink (1993, pp. 439–440) clarifies, modern issue-networks differ, to some degree, from traditional grass-roots and social movements; issue-networks may have associates, such as international organizations and philanthropic foundations, that are not normally found as part of those traditional movements.[18]

The rise of energetic social netwarriors may thus transform the nature of "strategic public diplomacy." It is traditionally concerned with the interactions of states, as they attempt to manipulate media in pursuit of their foreign policy goals (Manheim, 1994). Now, however, the initiative seems to be shifting to nonstate actors, as they are gaining comparable access to media, are less vulnerable to "targeting" themselves, and, in general, pursue agendas that are more suited to information-oriented issues of equity and human rights as opposed to the *realpolitik*-driven policies of nation-states.

In sum, then, social netwar is characterized by militant activists operating in, and as, SPINs or issue-networks. Social netwars tend to be anti-establishment, but any particular one may be progressive or reactionary, left- or right-wing, mass or sectarian, public or covert, threatening or promising for a society—it all depends. Whatever the case, networks of activist NGOs challenge a government (or rival NGOs) in a public issue area, and the "war" is mainly over "information"—who knows what, when, where, and why. Social netwar aims to affect what an opponent knows, or thinks it knows, not only about a challenger but also about itself and the world around it. More broadly, social netwar aims to shape beliefs and attitudes in the surrounding social milieu. A social netwar is likely to in-

---

[17]These kinds of analytical points by Sikkink and other researchers (e.g., Gerlach, 1987; Thorup, 1991) have finally begun to filter into the writings of policymakers. See Mathews (1997) and Slaughter (1997). For additional citations see Ronfeldt (1996).

[18]There is a definitional gray area here. Some grass-roots movements and social movements, especially what are called "new social movements," are close to being issue-networks, and some may have netwar-like characteristics and capabilities. The point still stands, however, that the literature about grass-roots movements and social movements has been slow to emphasize the rise of network forms of organization, doctrine, strategy, and technology.

volve battles for public opinion and for media access and coverage, at local through global levels. It is also likely to revolve around propaganda campaigns, psychological warfare, and strategic public diplomacy, not just to educate and inform, but to deceive and disinform as well. It resembles a nonmilitary version of "neo-cortical warfare" (Szafranski, 1994, 1995).

In other words, social netwar is more about a doctrinal leader like Subcomandante Marcos than about a lone, wild computer hacker like Kevin Mitnick.

MEXICO—SCENE OF MULTIPLE NETWARS

Mexico is currently the scene of multiple netwars that challenge the stability and the reformability of the Mexican system. For example, the Popular Revolutionary Army (EPR) aims to wage terrorist/guerrilla netwar. It is not entirely clear that the EPR qualifies well as an armed netwar actor, since its design remains obscure to analysis, but it has netwar-like characteristics that we discuss later. As for criminal netwar, Mexico's internetted drug-trafficking cartels are the key culprits. They have evolved aggressively in this direction since the late 1980s, partly in league with Colombian cartels.

The world's leading example of social netwar lies in the decentralized, dispersed cooperation among the myriad Mexican and transnational activist NGOs that support or sympathize with the EZLN and that aim to affect Mexico's policies on human rights, democracy, and other reform issues. That is the subject of this study. Indeed, the points made above about social netwar apply well to the Zapatista movement. It involves myriad issue-networks—for human rights, indigenous rights, etc.—that operate in a nonhierarchical fashion and through shifting coalitions and ad hoc formations. And the Zapatista movement's networks are indeed held together by shared values, dense exchanges of information, and efforts to mount "information operations" against the Mexican government and other actors that the network aims to influence.