

As noted in Chapter One, the Zapatista case has been hailed from the beginning as the world's first "postmodern" insurgency or movement. As such, it has generated enormous comment outside as well as inside Mexico, and much of that has involved whether, and how, this case offers an information-age model of social struggle that can be further developed and replicated elsewhere.

That view is not without critics. For example, writing from a rather traditional leftist position, Daniel Nugent (1995) has decried the postmodern label by pointing out that the EZLN remains quite traditional and premodern in many respects:

It is difficult to see how a rebel army of peasants, aware of itself as the product of five hundred years of struggle, that quotes from the Mexican constitution to legitimate its demand that the president of Mexico immediately leave office, that additionally demands work, land, housing, food, health, education, independence, liberty, democracy, justice, and peace for the people of Mexico, can be called a "postmodern political movement." How can the EZLN move beyond the politics of modernity when their vocabulary is so patently modernist and their practical organization so emphatically pre-modern? Their democratic command structure is a slow-moving form of organization—requiring as it does direct consultation and discussion with the base communities in five or six different languages—which is difficult to reconcile with postmodernist digital simultaneity. Do their demands include a modem and VCR in every jacale or adobe hut in Mexico? No. Is their chosen name "The Postmodern Army of Multinational Emancipation" or "Cyber-warriors of the South"? No.

But his points draw sharp dividing lines between what is deemed premodern, modern, or postmodern. The marvel, according to Chris Hables Gray (1997, pp. 5–6), in opening his book *Postmodern War*, is that the Zapatistas represent a hybrid of all three eras, and in a sense to be a hybrid is to be postmodern:

Theirs is a hybrid movement, with the traditional virtues of peasant rebellions augmented by media-savvy spokespeople who use the internet and the tabloid press with the shamelessness of athletic shoe companies. . . . [Marcos] is clearly part of a sophisticated attempt by the Zapatistas to break their political isolation with a strange combination of small unit attacks, national mobilizations, and international appeals. . . . Victory, for Marcos, isn't achieving state power, it is reconfiguring power.

Irrespective of whether the postmodern label is applied, there is no denying that information plays a seminal, decisive role in this movement. As Manuel Castells (1997, p. 79) points out, in an important, wide-ranging discussion about how the information age may affect the nature of social conflict around the world,

The success of the *Zapatistas* was largely due to their communication strategy, to the point that they can be called the *first informational guerrilla movement*. They created a media event in order to diffuse their message, while desperately trying not to be brought into a bloody war. . . . The *Zapatistas'* ability to communicate with the world, and with Mexican society, propelled a local, weak insurgent group to the forefront of world politics.

And his points are not unique to the Zapatistas. As a result of the information revolution, a range of new social movements—Castells also discusses environmental, religious fundamentalist, women's liberation, and American militia movements—are being redefined by the rise of a “networking, decentered form of organization and intervention” (p. 362). What is important about these networks is not just their ability to organize activities, but also to produce their own “cultural codes” and then disseminate them throughout societies:

Because our historical vision has become so used to orderly battalions, colorful banners, and scripted proclamations of social change, we are at a loss when confronted with the subtle pervasiveness of incremental changes of symbols processed through multi-

form networks, away from the halls of power. (Castells, 1997, p. 362.)

The Mexican case is so seminal that Harry Cleaver (1997) speaks of a “Zapatista effect” that may spread contagiously to other societies:

Beyond plunging the political system into crisis in Mexico, the Zapatista struggle has inspired and stimulated a wide variety of grassroots political efforts in many other countries. . . . it is perhaps not exaggerated to speak of a “Zapatista Effect” reverberating through social movements around the world—homologous to, but ultimately much more threatening to the New World Order of neo-liberalism than the “Tequila Effect” that rippled through emerging financial markets in the wake of the Peso Crisis of 1994.

Anti-Maastricht marches in Europe, and the roles played by Zapatista-inspired Italian radicals, are among the examples he cites. But his analytical point is broader than any single example: a new “electronic fabric of struggle” is being constructed, helping to interconnect and inspire activist movements around the world (Cleaver, 1995c, 1998).¹

We should note that there is some intellectual circularity in our presentation here. Most of the writings that we cite and quote from as evidence for the rise of netwar are by authors (e.g., Castells, Cleaver, Hables) who cite and quote from our original work proposing the netwar concept (especially Arquilla and Ronfeldt, 1993, 1996b). However, this circularity does not invalidate our using their writings as evidence for the spread of netwar. Instead, it confirms, as have discussions at the two Intercontinental Encounters organized by the

¹As the final touches were being put on this study, further evidence for this point appeared with news reports that a coalition of transnational civil-society NGOs, including the Council of Canadians and the Malaysia-based Third World Network, making use of the Internet and other media, had “routed” international negotiations that were supposed to lead to a Multilateral Agreement on Investment (MAI). “The success of that networking was clear this week when ministers from the 29 countries in the Organization for Economic Cooperation and Development admitted that the global wave of protest had swamped the deal.” Some of the Canadians involved in this network had previously been active in anti-NAFTA networking. See Madelaine Drohan, “How the Net Killed the MAI: Grassroots Groups Used Their Own Globalization to Derail Deal,” *The Globe and Mail*, April 29, 1998—as posted on the Internet.

Zapatistas, that the "network" meme² is taking hold in intellectual and activist circles and diffusing to new places around the world.

Thus, Chiapas provides the first of what may become a plethora of social networks in the years ahead. Each may have its own characteristics, depending on the country and region in which it occurs. Chiapas, partly because it is an early case, may turn out to be a special case; so we should beware of generalizing from it. Yet it is portentous. To the extent that we can generalize from it, some lessons and implications appear to be as follows.

TOWARD A DEMOGRAPHY OF SOCIAL NETWAR

The Mexican case shows that social netwar is an organizational and technological phenomenon; it depends on the growing presence both of activist NGOs and of all manner of information and communications technologies. As both presences grow around the world—and they are likely to continue growing—the incidence of social netwar is likely to grow. There may well be a synergistic relationship between the rise of the NGOs and the new technologies. As one activist we interviewed stated, "The Net is only useful to the extent that it is able to feed an activist mechanism." Accordingly, the Internet may create a synergy between the producers and the receivers of information, enabling different groups to make contacts and find new allies.

The numbers of NGOs has exploded in the past two decades, and even though many are having funding and other problems, the numbers are likely to keep growing throughout the world. Providing a demographic survey of the data on this lies beyond the limitations of this project. But, to quote from Adrienne Goss (1995), it appears that a global "third sector" is being created—"a massive array of self-governing private organizations, not dedicated to distributing profits

²Dawkins (1989) originated the notion of memes as a postgenetic basis for continued human evolution, in order to convey his point that cultural as well as biological bodies are based on units of "self-replicating patterns of information" (p. 329). In his view (p. 192), "Just as genes propagate themselves in the gene pool by leaping from body to body via sperm or eggs, so memes propagate themselves in the meme pool by leaping from brain to brain via a process which, in the broad sense, can be called imitation." Lynch (1996) discusses how memes spread through "thought contagion."

to shareholders or directors, pursuing public purposes outside the formal apparatus of the state.”³ This amounts to an “associational revolution” among nonstate actors that may prove as significant as the rise of the nation state.⁴

Most NGOs are hungry for the new information technologies, since they realize that communications is one of their key challenges and assets. Some NGOs in fact specialize in transferring the technologies to other NGOs, in order to ensure that their networks expand and become better and easier to use. Of these, the most important remains the Association for Progressive Communications (APC), which, as discussed earlier, is a worldwide partnership of member networks (like Peacenet and Conflictnet) that provides low-cost computer-communication services and information-sharing tools to individuals and NGOs working on social issues. In 1995, the APC had over fifty member networks in sixteen countries, and it provided access to 20,000 activists in 133 countries in fifteen languages (Goss, 1995)—and the numbers have risen since then.

Although netwar does not necessarily require access to the latest generation of information and communication technologies and does not depend specifically on the Internet, clearly some such communications infrastructure is necessary for NGOs to communicate with each other and to get their messages out to broad audiences. While the technologies need not be widely available, they should be sufficiently widespread that NGOs with limited budgets and resources can make consistent use of them. This point reflects our argument that strong local NGOs are essential for the transnational NGOs to network with.⁵

Again, the numbers are going up with respect to peoples’ access to all manner of the new technologies. Nonetheless, it is well known that

³Goss (1995) is selected for quotation because her article was circulated on Chiapas-related lists on the Internet. For a separate, extensive discussion of the notion of a “third sector,” see Rifkin (1995).

⁴Ronfeldt (1996) speaks to these points and offers an extensive bibliography. Recent policy-oriented additions to the literature include Mathews (1997) and Slaughter (1997).

⁵Imagine if the EZLN and local groups had refused to embrace the transnational NGOs and had denounced them as imperialists instead of describing their efforts as vital for peace and reform.

good access to the Internet is available in only a relatively small number of countries, and mostly only among the wealthier, more educated people. Americans are the heaviest users of the Internet, Europeans the second heaviest. In the Third World, Internet access is still spotty, and not particularly good where it does exist—and that applies to large parts of Mexico. In general, the “have-nots” still vastly outnumber the “haves.”⁶ However, Internet connectivity and bandwidth are expanding rapidly around the world. Even relatively “closed” countries like Cuba and Iran have Internet connections now.

Meanwhile, the world is moving rapidly beyond the era of faxes and text-only e-mail. Before long, activists will be able to upload full-motion audio-video files from inexpensive, handheld cameras. Moreover, in the next decade, satellite telephony may become a widespread reality. Activists will be able to upload and download materials from even remote locations, without having to go through a telephone system that may be controlled by a local government. Governments may have no way to prevent this sort of transmission. In short, radical improvements lie ahead for the NGOs’ abilities to communicate and share information, and these improvements may become widely available as costs come down.

EVOLUTION OF ORGANIZATION, DOCTRINE, AND STRATEGY

The Mexican case instructs that militant NGO-based activism is the cutting edge of social netwar, especially where it assumes transnational dimensions. A transnational network structure is taking shape, in which both issue-oriented and infrastructure-building NGOs are important for the development of social netwar. This infrastructure is growing, so that the activism it enables can extend from the locale where issues are generated (e.g., Chiapas) to the distant hallways of policymakers and decisionmakers (including in Washington, D.C.).

⁶Goss (1995), Kedzie (1995), and Swett (1995), not to mention other sources, give extensive statistical details.

The case instructs that netwar depends on the emergence of “swarm networks,”⁷ and that swarming best occurs where dispersed NGOs are internetworked and collaborate in ways that exhibit “collective diversity” and “coordinated anarchy.” The paradoxical tenor of these phrases is intentional. The swarm engages NGOs that have diverse, specialized interests; thus, any issue can be rapidly singled out and attacked by at least elements of the swarm. At the same time, many NGOs can act, and can see themselves acting, as part of a collectivity in which they share convergent ideological and political ideals and similar concepts about nonviolent strategy and tactics. While some NGOs may be more active and influential than others, the collectivity has no central leadership or command structure; it is multiheaded, impossible to decapitate.⁸ A swarm’s behavior may look uncontrolled, even anarchic at times, but it is shaped by extensive consultation and coordination, made feasible by rapid communications among the parties to the swarm.⁹

The Zapatista case hints at the kind of doctrine and strategy that can make social netwar effective for transnational NGOs. Three key principles appear to be: (1) Make civil society the forefront—work to build a “global civil society,” and link it to local NGOs. (2) Make “information” and “information operations” a key weapon—demand freedom of access and information,¹⁰ capture media attention, and use all manner of information and communications technologies. Indeed, in a social netwar where a set of NGO activists challenge a government or another set of activists over a hot public issue, the battle tends to be largely about information—about who knows what, when, where, how, and why. (3) Make “swarming” a distinct objective, and capability, for trying to overwhelm a government or

⁷See Chapter Two for a discussion of network-based swarming. For further elaboration, see Arquilla and Ronfeldt (1997).

⁸However, particular leaders can make a difference. The development of many NGOs is at such an early stage that a leader’s abilities and preferences can make a big difference as to how a specific NGO behaves. Brysk (1992) makes this point well and provides examples.

⁹Of course, there may be significant divisions and factions within a network that affect its overall shape and behavior. Intranetwars may arise that alter or limit the network’s capacity.

¹⁰On efforts to create an international charter on NGOs’ rights to information and communications, see Frederick (1993c), among other sources.

other target actor. Although, as noted above, swarming is a natural outcome of information-age, network-centric conflict, it should be a deliberately developed dimension of doctrine and strategy, not just a happenstance.

Where all this is feasible, netwarriors may be able to put strong pressure on state and market actors, without aspiring to seize power through violence and force of arms. In some instances, this may pose a potential threat to some U.S. interests. But in other cases, like Mexico’s, a social netwar may amount to a challenge rather than a threat—it may even have some positive consequences, especially for spurring social and political reforms. Indeed, in its more positive aspects, the Zapatista netwar has not been bad for Mexico (or for U.S. interests), even though it has heightened uncertainty in Mexico and abroad regarding Mexico’s stability and future prospects.

However, as discussed in Chapter Five, a recent development in the Zapatista case—a call for “electronic civil disobedience”—suggests that the theory and practice of social netwar could go in new directions. A split may even occur, akin to a traditional split on the Left between socialists and anarchists. To date, mainstream netwar activism has gone in the directions described above and elsewhere in this chapter: It has emphasized the creation of complex, multi-organizational networks, which use the new technologies mainly to improve communication and coordination within the network and to exert pressure on government and other actors through electronic protest measures (e.g., via e-mail and fax-writing campaigns). In contrast, a new “electronic civil disobedience” faction is emerging that appears to care less about the organizational network-creating dimensions of doctrine and strategy, favoring aggressive computer-hacking tactics that, though termed “virtual sit-ins,” verge on anarchistic or even nihilistic “cybotage” against sensitive government or corporate Web sites and Internet servers.

FAVORABLE CONDITIONS FOR SOCIAL NETWAR

The Zapatista movement substantiates the growth of “global civil society” and has helped to catalyze it, showing it can reach from the global down to the local level and influence the policies of states. This netwar has affected not just Chiapas and Mexico; it is galvaniz-

ing a new presence in world politics that challenges the primacy of the nation-state in some issue areas.

The Zapatista case indicates some conditions that should be present for a transnational social netwar to emerge and spread. Evidently, as in the case of Mexico, a society should be relatively open (or opening up), including in regard to freedom of association and information. It should be in flux and under political, economic, and other strains that are generating divisive public debates. This may be especially the case in societies where old clannish and hierarchical structures are being challenged by, and adapting with difficulty to, new market and civil-society forces.¹¹

The society should have local NGOs to which the transnational NGOs can link. The society should be in a region where the infrastructure for social activism is growing, in both organizational and technological terms. The activists should have diverse communication systems at their disposal for purposes of rapid all-channel consultation, coordination, and mobilization. The transnational NGOs and their networks should have sufficient reach that they can not only arouse public opinion, but also lobby in Washington and other capitals where policy decisions are made.

A target government should care about its international image, and be sensitive to its disruption.¹² The more a government cares about presenting to the world an image that it is, or is becoming, a modern democracy and wants to attract foreign investors, the more vulnerable it may be to a netwar that jeopardizes its image. A pariah state, like Iraq, that does not care much about its image in Washington or European capitals will be less vulnerable to social netwar, and less hesitant to crush activists who try to create one. (Perhaps a susceptibility to social netwar is a sign of modernity.)

Social netwar thrives on having audiences outside the conflict zone. Audiences should be aroused not only in the target society but also in distant, influential foreign capitals. Social netwar may be most effective where activists in a target society can appeal to strong, liberal, democratic audiences abroad whose own civil-society actors can

¹¹For clarification and elaboration, see Appendix B.

¹²Sikkink (1993) addresses this point well.

take up the cause and lobby for changes in their government’s policies toward the nation at issue. Getting the message from the conflict zone to such audiences abroad may be facilitated by the fact that this is the direction in which the Internet and other global media generally tend to convey information.

Indeed, a major part of social netwar is about activists’ efforts to get their story into the global media, so that it reaches and arouses foreign publics and governments. Conditions should be such that a “CNN effect” can occur that amplifies the theatrical information operations of netwarriors. The local and international press should have access to and be captivated by the story. The mainstream press may not be part of a social netwar, in that it (usually) does not have an explicit agenda and does not form part of the NGO networks. Nonetheless, the presence of journalists may contribute importantly to a netwar by providing, very quickly, a broader audience than usual for NGO activities. A symbiotic dynamic may thus develop between the activists and the media (in which the journalists may claim that they are the ones who deserve credit for calling a conflict to the world’s attention, but the larger dynamic is about the activists using the media to accomplish this). Furthermore, the media’s presence may alter the local power equations vis-à-vis information—a local government may lose the luxury of controlling who knows what about a conflict, and its options may decrease accordingly. As international attention grows, a hard-line approach, for example, may be less feasible for a government.

Finally, the issues should be amenable to social activism. Some are easier than others for NGOs to take up. The more statecentric an issue area—the case, for example, with issues like military reform—the more difficult they may be for NGOs to address. Much may depend on whether there are international bodies concerned with the issues. As Brysk (1992) has observed, an indigenous people may face the following kinds of issues: being killed (a human-rights issue), poverty (a development issue), land theft (which becomes a migration issue), deforestation (an environmental issue), and land-use conflicts (which may be a market issue). In this situation,

the rational response of a social movement is to launch simultaneous appeals in all appropriate venues—and over time, to concentrate on those issue areas governed by accessible and responsive

international regimes. In general, information-processing regimes such as human rights and ecology are more accessible to NGOs than state-centric arrangements for trade or arms control.¹³

In other words, the situation in a target society should be such that a diversity of NGOs exist and can mount different attacks on different issues, adapting flexibly to the circumstances. In the process, the message—the story and its symbolism—may get modified and broadened beyond its original meaning in the conflict zone, in order to appeal better to audiences abroad.

Because such conditions are not present everywhere—they apply less to Myanmar than to Mexico—some societies will provide more susceptible environments than others for social netwar. Where the conditions are ripe, the Mexican case implies that social netwar may put a liberalizing authoritarian regime on the defensive and, to some extent, spur new steps toward democratization. Moreover, some foreign capitals will provide more susceptible external targets than others for social netwar. The conditions identified above indicate that social netwar will be most effective where a conflict can be “exported” in order to arouse activists and policymakers in the capitals of a foreign power. This is much more likely to be the case with the United States than, for example, with a power like Japan, where transnational social activism is relatively weak and can even be ignored.

Thus, social netwar can be an agent of change that may have both positive and negative effects—it may represent “good news” as well as “bad news” for U.S. interests. Social netwar is also in its infancy as a mode of conflict; governments are just beginning to learn about it. Mexico is one of the first countries to experience it, but it is far from the last. The significance and effectiveness of social netwar are likely to grow around the world. In some cases, the United States may even want to foment one, or at least be positioned to benefit from its effects—or the United States may want to preempt a netwar that might start against a key ally (e.g., Saudi Arabia).

¹³Brysk (1992), p. 23. Also see Brysk (1998, forthcoming) for further discussion.

CHALLENGES TO AUTHORITARIAN SYSTEMS

A major proposition in the literature about the implications of the information revolution is that it compels closed systems to open up, and thus will prove damaging to totalitarian and authoritarian regimes. This proposition emerged particularly during the administration of President Ronald Reagan, when Secretary of State George Shultz, writing in 1985, before the revolutions of 1989 in Eastern Europe, forecast that

the free flow of information is inherently compatible with our political system and values. The communist states, in contrast, fear this information revolution perhaps more than they fear Western military strength. . . . Totalitarian societies face a dilemma: either they try to stifle these technologies and thereby fall farther behind in the new industrial revolution, or else they permit these technologies and see their totalitarian control inevitably eroded. (Shultz, 1985, p. 716.)

If the Soviet regime adopted the new technologies, Shultz and others (e.g., Stonier, 1983) predicted that its leaders would have to liberalize their economic and political systems. Subsequent events in Eastern Europe, China, and to a lesser extent Latin America provided evidence for the democratizing effects of the information revolution. Since then, researchers (e.g., Builder and Bankes, 1990; Kedzie, 1995) have increasingly argued that the diffusion of the new technologies will speed the collapse of closed regimes and favor the rise of open ones.

One recent Pentagon-based analysis focuses on the Internet. According to Charles Swett (1995), authoritarian governments are threatened by the freedom of information that it represents:

The Internet is the censor's biggest challenge and the tyrant's worst nightmare . . . Unbeknown to their governments, people in China, Iraq and Iran, among other countries, are freely communicating with people all over the world.

As a result, "Authoritarian countries are hesitating before allowing their people access to this technology," because the Internet poses a "significant long-term strategic threat to authoritarian regimes" which they will be ineffective in countering (Swett, 1995).

The other side of the picture is that guerrillas and other antiestablishment groups are making increasing use of the new communications technologies. While systematic evidence for this is lacking, anecdotal evidence abounds. According to one journalist, for example,

Today, every group from the Irish Republican Army to Hamas and Peru's Shining Path has taken its struggles to the Internet, and in the process they have radically altered the nature of guerrilla action and civic protest around the world. Net surfers can now learn everything about the revolutionary struggles in Mexico and Peru, and even how to construct a pipe bomb. (Vincent, 1996.)

That authoritarian regimes are at a strong disadvantage is not a sure bet over the near term, however. Some such regimes—for example, China, Cuba, and Myanmar (Burma)—have managed to control access to the new technologies and to the Internet, without incurring high political or social costs at home or setbacks in foreign trade and investment. This does not disprove the proposition that the information revolution will eventually compel closed systems to become open, but it indicates that the process will be uneven, situational, and long term in perhaps many cases.

The Zapatista case generally substantiates these points, since it is partly a case of a liberalizing authoritarian regime being affected by activists using the Internet and other media. Our point, however, is not so much about the information *technology* revolution in general or the Internet per se. Our point is more about the organizational dimensions of the information revolution: Whether a netwar can topple a particular dictatorship will depend on the situation; but in general, many authoritarian regimes are likely to prove vulnerable to social netwar, viewed as a combined organizational, doctrinal, and technological phenomenon.

For example, the scenes of future social netwars could include such countries as Cuba, Nigeria, Russia, and Saudi Arabia. In Cuba, the prospects for social netwar are growing. Castro's government has begun to open the economy, but persists in political and social repression. Meanwhile, grass-roots groups, which are very few in number, are trying to open space for themselves inside Cuba and to connect to outside NGOs, including through faxes and e-mail

(Gonzalez and Ronfeldt, 1994; Press, 1996). Aspects of netwar have existed for decades in U.S.-Cuban relations, as in the U.S. broadcasting and Cuba's jamming of Television Martí and Radio Martí, as well as in the activities of pro- and anti-Castro groups in the United States. What could emerge before long are the conditions for a full-fledged social netwar, if Cuba becomes more open than is presently the case.

In Saudi Arabia, the ruling family keeps tight control, including through heavy surveillance and security measures. But an underground exists, and people's access to modern telecommunications is improving as a result of new connections to the Internet and plans for AT&T to upgrade the cellular telephone grid. Thus, opportunities may grow for an indigenous dissident movement to emerge and gain links to outside fundamentalist and even secular democratic forces. At the same time, the more Saudi Arabia's telecommunications systems become connected to the outside world, the higher the costs of repression and control may become for the ruling regime. Note, for example, that even a sleek information-age autocracy like Singapore's cannot prevent the rise of stealthy activists using faxes and e-mail (though so far they have not had much effect on weakening the regime there).

Even a country as closed as Myanmar (Burma) may be vulnerable to social netwar. "Free Burma" exile groups have organized into a network and have created an e-mail circuit and Web pages to promote the downfall of the military junta and support internal pro-democracy activists. With the motto, "When spiders unite, they can tie down a lion," the network has successfully pressured some foreign corporations to stop doing business there. According to one report, "the junta seems to be worried, despite the fact that nobody outside the government in Myanmar has access to the Internet."¹⁴ To control dissidents, the junta has outlawed the unauthorized possession of computers that have networking capability as well as the use of computers to transmit information on such topics as state security, the economy, and national culture.¹⁵

¹⁴From "Arachnophilia," *The Economist*, August 10, 1996, p. 28.

¹⁵From a note taken from the *Financial Times*, October 5, 1996, as posted on the Internet. Also see Danitz and Strobel (1998, forthcoming).

Of course, authoritarian regimes will not respond lightly to the emergence of social netwars. In their efforts at counternetwar, they may try to monitor, harass, arrest, and expel both domestic and foreign activists; regulate the formation and behavior of NGOs through administrative and judicial methods; and even create “dummy” NGOs or GONGOs¹⁶ to hijack an agenda. Furthermore, they may try to control the means of communication—by restricting access to the Internet, seizing unauthorized pieces of technology, pressuring journalists about what to report, or other measures. They may also try to provoke intranetwars by sowing dissent among the NGOs. And they may try to wage misinformation and disinformation campaigns to embarrass or confuse the netwarriors. Some, though certainly not all, of this is evident from the Mexican case.

Opposing authoritarian regimes in some nations may not be the only objective of netwarriors. In the years ahead, the possibility should not be overlooked that a major new global peace and disarmament movement may eventually arise from a grand alliance among diverse NGOs and other civil-society actors attuned to netwar.¹⁷ They may increasingly have the organizational, doctrinal, technological, and social elements to oppose recalcitrant governments, as well as to operate in tandem with supranational organizations and national governments that may favor and support such a movement.

Social netwar is fundamentally antiestablishment. It may be used by leftists, or rightists, or anyone else with an antiestablishment agenda. It is more likely to be used against states, rather than by states.

¹⁶See page 35, footnote 16.

¹⁷This prediction, which appeared in the December 1996 draft of this study (and earlier in Arquilla and Ronfeldt, 1996b), has since come partially true, with the rise of the worldwide movement to ban land mines. Because of it, a social netwar has won a Nobel prize.

IMPLICATIONS FOR THE U.S. ARMY AND MILITARY STRATEGY¹⁸

Why should this matter to the U.S. Army? In large part, it matters because the world is changing in ways that may be more likely to present social netwars than traditional insurgencies in many nation-states that are allies of, or otherwise of interest to, the United States. By analyzing the Mexican case, we may better understand the patterns that may arise in other contexts, and the innovations that may become advisable for responding to them. Mexico provides a preliminary case study not only of social netwar, but also of some options for counternetwar.

This case confirms the major propositions about networks-versus-hierarchies posited in Chapter Two. The Zapatista networks have performed impressively against the Mexican hierarchies. The latter, in turn, have responded with interagency cooperation and tactical decentralization, as the emerging theory of netwar suggests. In addition, this case shows that information operations are an important, innovative aspect of information-age conflict. The fight over "information" has made the Zapatista conflict less violent than it might otherwise have been. But it has also made the conflict more public, disruptive, protracted, and difficult to isolate; it has had more generalized effects than if it had been contained as a localized insurgency. Thus, although the Mexican military has performed reasonably well militarily against the EZLN, has decentralized its organization, created new small units, improved its communications and mobility, and acquired new material and budgetary resources in the process, it has been bedeviled by many aspects of this new approach to conflict. The army in particular has seen its combat operations deterred and its image impugned to an unusual degree.

The Mexican case suggests that the U.S. Army should continue to improve its understanding of the growing roles of NGOs in environments affected by SSCs.¹⁹ Is social netwar, where activist NGOs operate in tandem with an insurgent army, really a new phe-

¹⁸Many points in this and the next subsection are reiterated from previously published work by Arquilla and Ronfeldt (1996a, 1996b, 1997). For additional insights, see Berger (1998).

¹⁹RAND research by Jennifer Taw is inquiring into this matter in other cases.

nomenon? Or is it just more of the same, with a heavier emphasis on psychological operations and public relations? Does social netwar mean that a local military, not to mention the U.S. military as an ally, has to respond quite differently? Our study suggests that the answer to such questions is “yes,” largely because of the protagonists’ emphasis on information operations. More than likely, the local military (and the government) will find it needs to develop its own information strategies to deal with the NGOs.

Where feasible, it may be increasingly advisable to improve U.S. and allied skills for communication and even coordination with NGOs that can affect the course and conduct of a netwar. The Mexican case suggests that the U.S. Army may be increasingly called upon to provide “knowledge assistance” to allies for public and press relations, psychological operations, and the restructuring of command, control, communications, and intelligence (C3I) functions in response to netwars. Respect for human rights, and possibly for the looming matter of “information and communications rights,” may play no small part in this.

Furthermore, this case indicates the importance of monitoring and analyzing what is transpiring in cyberspace, where information operations may be conducted out of much public sight. Some work (e.g., Swett, 1995) has been done on this, but much more is needed. As noted earlier, netwars are waged mainly in real life, but what occurs in the infosphere—particularly “on the Net”—may have significant bearing on the course and consequences of a conflict.²⁰ It took Mexican officials a while to realize the role of the Internet in the Zapatista netwar.

By conventional measures, the EZLN has never had much of an order of battle—just an odd mixture of weapons, and only a few sizable combat formations. Yet, by emphasizing information operations, it has done quite well. This accords with points made in another study (Arquilla and Ronfeldt, 1996a): A new generation of assessment methodologies may be needed, including to determine a protagonist’s “information order of battle” and the intentions, capabilities, and vulnerabilities related to it—in short, for doing a new kind of net

²⁰See page 11, footnote 6.

assessment. It may turn out that a new language and a new set of metrics must be devised. New centers and schools are already being established for the U.S. military to help address such challenges. The question might also be addressed as to what an “information war room” would look like.

As we in the United States grapple to define our own concepts of information, we should keep an eye on how they are being defined in other societies and cultures that are trying to take advantage of the information revolution. To some extent, the U.S. government should aim to identify operational concepts that may serve as the basis for alliances and other forms of cooperation, where relevant. But we should also enhance our knowledge of others in order to develop early warning of potential adversaries, including nonstate adversaries, who may invent information concepts that are unusually difficult for us to counter. This may be especially the case with psychological and cultural aspects of warfare.

CONCLUDING COMMENT

In sum, the Mexican case confirms, and portends, that netwars may be a natural next mode of conflict (and crime). The advent of netwar is a result of the rise of network forms of organization, which in turn is a result of the information revolution. Not all conflicts will involve netwar—many traditional modes of conflict and crime will persist—but netwar is already ascendant.

A few propositions (taken from Arquilla and Ronfeldt, 1996b) that we would reiterate in conclusion, all confirmed by the Mexican case, are as follows:

- Organization, and knowing how to organize, have always been a source of power, independently of the resources and skills available in an organization. Today, the network form is fast becoming a new source of power—as hierarchy has been for ages. It is especially a source of power for actors who previously had to operate in isolation from each other, and who could not or would not opt to coalesce into a hierarchical design where they would lose their independence and autonomy.

- Power is migrating to actors who are skilled at developing networks, and at operating in a world of networks. Actors positioned to take advantage of networking are being strengthened faster than are actors embedded in old hierarchical structures that constrain networking. This does not favor actors on any end of an ideological or political spectrum—it favors whoever can best master network design elements.
- At present, nonstate transnational actors appear to be ahead of government actors at using, and at being able to use, this form of organization and related doctrines and strategies. It takes skill to use them well, but the ease of entry and the deniability afforded by network designs imply an increasing “amateurization” of militant activism, terrorism, and crime (Hoffman, 1994). It is increasingly easy for protagonists to construct sprawling networks that have a high capacity for stealthy operations by individuals or groups, as well as for rapid swarming en masse.

Information—as a function of the technological and organizational innovations stemming from the information revolution—is now said to be a “force multiplier” (notably during the Gulf War, to the benefit of U.S. forces). Yet the more important point is that information, along with the attendant rise of the network form, is a “force modifier.” Taking advantage of the information age is bound to require modifications in how forces are organized and deployed for offensive and defensive moves, perhaps especially where the objective is more about disruption than destruction.

More to the point, “information strategy” is emerging as a new tool of statecraft. U.S. officials are accustomed to emphasizing economic, political, and military strategies and instruments for urging foreign governments and societies to develop in liberal democratic directions. Yet, global civil-society NGOs whose focus is informational more than economic, political, or military may prove more potent as information-age instruments of policy and strategy, especially to pursue goals like “democratic enlargement.” Chris Kedzie’s (1995) work on the positive correlation between political democracy and communications connectivity provides a basis for proposing that information be treated and developed as a distinct new dimension of policy and strategy (see Arquilla and Ronfeldt, 1996a, 1997, and forthcoming).

Understanding the network form is important for understanding the advent of netwar—why and how the world is giving rise to a new mode of conflict. More research lies ahead to improve our ability to study this form, its levels of analysis (e.g., the organizational, doctrinal, technological, and social levels), and its emerging implications for society and security in the information age. Better theories and methodologies are needed on how networks function and how best to analyze them. The age—and the study—of networks and netwars is barely beginning.