What Is "Netwar"—Revisited

- Proposition: The more an actor uses network forms of organization, doctrine, strategy and communications to engage in conflict or crime, the more it is a netwar actor

- Implication: There are degrees and varieties of netwar actors

To reiterate: In ideal form, a netwar actor exists in (or as) a network of small, diverse units—perhaps even as cells. They are dispersed but also interconnected. The network will likely be amorphous and a cephalous—it will have no precise heart or head, although not all nodes may be "created equal." As discussed below, the network may have a chain, star, or better yet, an all-channel design, though hybridization and multilayering are likely. For example, an all-channel network might send out a chain to fulfill some mission or to connect with an allied network. Colombian and Mexican drug gangs seem to interconnect in this fashion. Older criminal organizations, like the Mafia, appear to use star networks more frequently than all-channel formations, although linking via chains also occurs.

In addition to these structural elements, the netwar actor has behavioral dynamics that enhance both operational effectiveness and survivability. This type of actor has a great capacity for self-reorganization, allowing for adaptation to varied environments and challenges, and for the versatility needed to pursue a wide range of activi-
ties. These behavioral traits contribute to the robustness of the archetypal netwar actor when under attack, and also allow for smooth transitions from defense to offense. Indeed, the loose, somewhat dispersed attack formation of the network, discussed earlier, also serves as the principal alignment for defense.

Our basic proposition is that the more an actor uses network forms of organization, doctrine, strategy, and communications to engage in conflict or crime, the more it is a netwar actor. By implication, there are various types of netwar actors.

What specific forms will netwar take? Who may be the state and nonstate adversaries? What threats and challenges may they pose to U.S. interests, or to life in the international system? Preliminary answers are presented in this chapter. The variety of actors discussed include ethnic, nationalist, and separatist movements; criminal organizations; terrorists and other violent revolutionaries; cyberspace saboteurs; and militant social activist groups. This is not meant to provide a formal typology of the varieties of netwar actors, nor a detailed analysis of them, nor an analysis of literature about them—it is just a presentation that emerges readily from our inquiry into what is going on in the world.

As discussed below, a netwar actor’s design, and its strength, may be analyzed at four levels: organizational, doctrinal, technological, and social. The discussion in this section often highlights one level or another in describing a particular type of netwar actor. But we do not attempt, at this stage of our research, to examine systematically each variety in terms of all four levels.

The cases examined in this chapter fall along a spectrum, ranging from conflicts that have substantial (though not predominantly) military components, to those that hardly look like war at all, in the traditional sense. As to actors, we focus principally upon nonstate groups and organizations, since these constitute the majority of current netwar actors. However, some states may transform themselves to wage netwar. Indeed, they may come to resemble, in essential ways, the networked nonstate actors that will likely constitute the typical “netwarriors” of the future. For the present, though, states involved in netwar tend to work through nonstate proxies (e.g., some Middle Eastern states’ sponsorship of a wide variety of small groups that engage in terrorist activities).
### Basic Types and Levels of Networks

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chain (Smugglers)</td>
<td></td>
</tr>
<tr>
<td>Star or Hub (Drug cartel)</td>
<td></td>
</tr>
<tr>
<td>All-channel (Peace network)</td>
<td></td>
</tr>
</tbody>
</table>

- Different types suit different purposes and situations
- **All-channel** type gives network form its high potential
- Mixes of all three may be present in a netwar actor

As the scholarly literature instructs, networks come in basically three types (or topologies):

- The *chain* network, as in a migration or job-search chain where people, goods, or information move along a line of contacts that are separated from each other, 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 SPIN-like collaborative network of militant peace groups in which everyone is connected to everyone else.

Each node indicated in the diagrams may refer to an individual, a group, an institution, part of a group or institution, or even a nation-state. Each design is suited to different conditions and purposes. Of the three, the all-channel network is the most difficult to organize and sustain, partly because of the dense communications it may require. But it is also the type that gives the network form its new, high potential for collaborative undertakings. And it is the type that we generally refer to in this study.

All these types may be found among netwar-related adversaries, e.g., the chain among smuggling operations, the star among criminal syndicates, and the all-channel among militant groups that are highly internetworked 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 different combinations and configurations are possible.
Basic Types and Levels of Networks (cont.)

- **Strength depends on functioning well across four levels**
  - _Organizational:_ little hierarchy and high autonomy
  - _Doctrinal:_ reasons to collaborate
  - _Technological:_ dense communications
  - _Social:_ personal ties to ensure loyalty and trust

- **Each level’s characteristics may affect other levels**

So far, we have not found an established academic methodology to follow for analyzing the networks that appear among netwar actors, although the literature identifies many factors and attributes to consider. What makes sense to us is to examine the design and operation (or form and function) of a network—be it a chain, star, all-channel, or hybrid—in terms of four levels of analysis:

- **Organizational level**—To what extent is an actor, or set of actors, organized as a network? What type is it? This is the top level—really, the starting point—for assessing the extent to which an actor, or set of actors, is designed for netwar. Our earlier discussion of netwar design elements (see prior chart with that title) points out many considerations that should be taken into account. Among other things, assessment at this level may include inquiring whether and how members may act autonomously, but also whether and how hierarchical dynamics that preclude autonomy may be mixed in with the network dynamics.

- **Doctrinal level**—Why have the members assumed a network form? Is it deliberate? Fortuitous? What doctrines, ideologies, interests, and other reasons or motivations exist for their using and remaining in this form? This level of analysis is important for explaining what keeps a network together and enables the members to operate strategically and tactically without necessarily having a central command or leadership. The doctrine should reflect a commitment to collaborate and to remain in a network form (i.e., not change to a hierarchy). However, despite a generally shared world view, the network may include members who vary as to the priority of specific ends and the selection of means.

- **Technological level**—What is the pattern of, and the capacity for, dense information and communications flows? What technologies support this? How well do
they suit the organizational design? This level may involve a mix of new and old, high- and low-tech capabilities; but in general it is the new technologies that are making the new forms of organization and doctrine feasible. The higher the bandwidth, and the more advanced the means of transmission, reception, storage, and retrieval, the better the prospects for network-style communications and thus organization. Design elements and capabilities at this level may significantly affect the organizational and doctrinal levels.

- **Social level**—How well, and in what ways, are the members personally known and connected to each other? This is the classic level of social network analysis, where strong personal ties, often ones that rest on kinship, ethnicity, friendship, or bonding experiences, help ensure high degrees of personal trust and loyalty. To function well, networks seem to require higher degrees of interpersonal trust than do other forms of organization, like hierarchies. This traditional level remains important in the information age.

The strength of a network, perhaps especially of the all-channel design, depends on functioning well across all four levels. The strongest networks will be those in which the organizational level is supported by a pervasive doctrine or ideology attuned to the overall design and in which all this is layered atop advanced telecommunications and has traditional networks of personal and social ties at the base. Each level, and the overall design, may benefit from redundancy and diversity. Each level’s characteristics are thus likely to affect the other levels.

In a well-developed network, the network itself may be considered more influential and important than any member (a dynamic that may help constrain any single member from dominating the network). The all-channel network may offer particular advantages in situations where the members aim to preserve their autonomy and independence and to avoid hierarchical controls, yet they also have agendas that are interdependent and benefit from coordination. Such a network may become most durable—it may even have a central coordinating office—when its members develop strategic, collective interests in being part of the network that may at times override their individual interests, and when they prefer to remain in this form rather than coalesce into a hierarchical institution as the network gains power and influence.
Netwar Actors Are Mostly Nonstate

- Nonstate varieties (subnational and transnational)
  - Pre- or proto-state: ethnonationalists or separatists
  - Market-oriented: criminal and commercial predators
  - State-oriented and often antistate: militant NGOs or revolutionary movements
- Some actors may be agents of a state
  - Some proliferation or smuggling networks
  - Some fundamentalist networks
- Symbiotic hybrids are likely, too

Most netwar actors who engage in offensive operations will be nonstate and/or stateless, at least in the near future. They will be sub- as well as transnational. However, as the low costs and risks and likely high gains from netwar are demonstrated, more and more states may realize the value of adopting this approach to conflict in the information age. Indeed, some netwarriors are already serving as agents of a state, as is a common practice in the Middle East.

Hybrids are likely to emerge. In some instances, states may sponsor, but not necessarily direct, nonstate netwar actors. In other instances, nonstate actors may sponsor states. These sorts of developments will enhance the effectiveness of both the networks and the states with which they link up, posing a formidable task for state actors waging defensive netwar.

One type of nonstate actor exists mainly within the nation-state, often as a subnational ethnic or separatist movement. Another type functions more in the interstices between states and includes transnational criminals and revolutionaries, and sometimes also militant NGOs whose activities erode nationalism. Of course, there are exceptions to this. For example, the Kurds, quintessential ethnic separatists, are located across the territories of several states. But these exceptions highlight a general rule that ethnonationalists and separatists operate within state boundaries, while criminals often operate across them. Both types, however, often harbor powerful, dangerous anti-state sentiments and aims.

A troubling aspect of the interplay between state and nonstate actors in netwar revolves around the possibility that, instead of the emergence of symbiotic relationships, nonstate actors may often oppose, or prey upon, states. In Colombia, transnational criminal networks, principally the drug cartels, have been hammering...
away at state political, legal, and social institutions for decades, to the point at which the foundations of the state may be fatally undermined. Another case has arisen in the wake of the dissolution of the Soviet Union, where the Russian successor state finds itself besieged by powerful criminal networks that have, in many ways, come to drive and dominate the nascent market structures struggling to survive and empower the state.

Finally, we also see a third path for nonstate netwar actors: Instead of developing symbiotic relationships with states or intentionally preying upon them, networked organizations may use nation-states' territories as arenas for their competition with rival networks. The consequences for the states subjected to such activities will be conditioned by the course and outcome of the particular netwar in question. For example, Zambia has, for at least the past 20 years, been a principal battleground between transnational ivory poaching interests and the Wildlife Fund, which seeks to protect the dwindling African elephant population. The poachers have sought to "capture" various political, legal, and military institutions, while the conservationists have striven to foster local political reforms and to provide economic alternatives to the exploitation of elephants. Gibson's (1995) examination of this case points out that the poachers have undermined the state, while the conservationists have engaged, in many respects, in state-building. The outcome, as of this writing, remains uncertain, as the competing interests appear to be in equipoise.

In short, the current landscape of netwar is dominated by nonstate actors. However, their interactions with states are almost continuous, having effects that range from beneficial to pernicious. A key question revolves around the possibility that states might come to realize the strengths of networked forms of organization, and develop them for the explicit purpose of combating networked nonstate criminal, terrorist, or revolutionary organizations.
During the Cold War, indigenous conflicts were often sublimated to the demands of the superpower rivals. Now, the international system seems to be returning to traditional polycentric, regionalized patterns of conflict. Thus ethnonationalism, religious revivalism, and separatism are fostering a resurgence of unruliness, with the principal actors generally operating at the sub- or transnational levels. Indeed, of the 35 wars ongoing in 1995, only 3 (in the Balkans, Kashmir, and the Western Sahara) featured major interstate elements. The rest are internal wars (Brassey’s, 1995). In these, the combatants have mostly tribal organizational structures, onto which many appear to have grafted various aspects of information-age network designs. Because of this, these ethnic, nationalist, and separatist (ENS) conflicts represent an important variety of netwar, and a potentially fruitful study of netwar.

ENS protagonists are generally unlike nation-state actors. The former, and their organizations, are held together mainly by ethnic kinship ties. While many have a nominal “chief,” there is, in reality, a dearth of formal, professional institutions; conduct is guided largely by premodern ethnic and religious traditions. Thus, we have the interesting phenomenon of netwar actors who graft N-type designs onto T-type structures, and who have little interest in building modern institutions and markets.

ENS organizations have proven well-suited to irregular warfare (and often to crime as well). Indeed, many exist in a state of almost perpetual conflict. When not fighting against a local government or outside power, their internal disputes often lead to internecine strife. (In anthropological terms, they oscillate between “fission” and “fission.”) Thus, near-constant warfighting hone their skills and contributes to the development of ever more efficient network structures, making them formidable adversaries.
The recent American experience in Somalia exemplifies the difficulty of dealing with ENS adversaries; and at least one thoughtful study has focused on the need to understand the networked, organizational dimensions of the opponent in these sorts of conflicts (Allard, 1995). The long-standing resilience and intractability of the Serbs in the current Balkan War provide further evidence of the robustness of this kind of adversary, as the United Nations and NATO have learned that they must deal, beyond “chiefs” like Radovan Karadzic or Ratko Mladic, with countless clan members to whose demands the nominal leaders must be attentive, if not subservient. The current Russian trials in Chechnya reflect a similar struggle against a networked, clan-based opponent that can withstand enormous damage and yet continue the fight. This case approaches the netwar ideal; the Chechen insurgents eschew traditional military structures in favor of cell-like “task groups” capable of an unusual degree of autonomous action.

Traditional warfighting approaches will continue to have little ability to defeat such adversaries. Those who wish to counter ENS opponents may have to adopt doctrines and organizational structures that resemble the insurgent networks they confront.

A recent example, still worthy of careful study even though it predates the current rash of ethnonationalist conflicts, involves the Viet Cong campaigns in the early years of the Vietnam War. Organized in cells and networks, these insurgents came close to toppling the regime in Saigon, which was propped up only by American intervention. U.S. forces, though quite effective militarily, employed an ill-suited “big unit” approach to fighting an opponent almost invulnerable to traditional military pressure (Summers, 1982; Krepinevich, 1992). The Viet Cong insurgency against the South Vietnamese and American forces highlights the robustness of the network when under attack by hierarchically oriented adversaries.
**Shots Heard 'Round the World**

<table>
<thead>
<tr>
<th>• Paul Revere and the Minutemen</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Cohesion via &quot;Committees of Correspondence&quot;</td>
</tr>
<tr>
<td>– Decentralized command and communications</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• Mohamed Aidid and his clansmen</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Warlord command and kinship ties</td>
</tr>
<tr>
<td>– Mix of low- and hi-tech communications</td>
</tr>
</tbody>
</table>

Consider the situation that the British colonists in North America faced in the mid-18th century, when the first major wars against the Indians flared. The immediate response of the British (and the settlers, including George Washington) was to send a traditional European-style field army off to the wilderness to pacify it. The result was the slaughter of General Braddock and his forces, followed by a newfound willingness to innovate. This led to much "irregularization" of colonial forces (Rogers' Rangers, etc.), and a great deal of tactical decentralization by the Crown commanders. In the end, this institutional redesign played as much a role in winning the French and Indian Wars as any of General Wolfe's heroics on the Plains of Abraham (Parkman, 1884).

The irregular politico-military organizational structures that served the British colonists so well during the French and Indian War formed the basis of the militias that would start the fight for independence from Britain. Militia nodes soon covered the land, linked together, network-style, by the Committees of Correspondence. Although each cell was quite small, and most were geographically dispersed, strong communications links allowed for rapid mobilization and deployment. During the initial battles at Lexington and Concord, for example, this form of organization and its communications infrastructure allowed the rebels to engage in unrelenting "swarm" attacks against veteran British regulars, inflicting a costly, humiliating defeat on them.

After these opening battles, the rebels sped to write up their accounts of the skirmishes, dispatching them on the first available packet ship to Europe. They seized the initiative to win the information and propaganda war in Europe. The British, by engaging in procedurally proper after-action reporting—and being in little hurry to relay the debacle to military superiors, the Crown, and the British public—were thus
confronted with the fact that the rebels’ view of the fighting had been circulating for weeks in Europe before official government reports became available (Fischer, 1994; Galvin, 1989).

Recently, Somali clan leader Mohammed Farrah Aidid used an internetted structure similar to that employed by the Minutemen, and mixed low- and high-technology instruments in his communications infrastructure. This gave him and his forces considerable defensive robustness and allowed them to monitor the movements of U.S. Rangers sufficiently closely to permit a shift to the tactical offensive that helped unravel U.S. policy. Indeed, the swarming tactics used by the Somalis during their long firefight with Task Force Ranger are reminiscent of the command and control of the Minutemen in the battles of Lexington and Concord.

Further, it must be observed that Aidid was extremely aware of the importance of directing the flow of information about this action away from the fact that his fighters suffered grievous losses. Instead, he successfully kept the focus on the issue of U.S. casualties, which directly affected the resolve of the American public and political leadership in sustaining its campaign against him.
Clannish structures dominated by ethnic concerns appear among some contemporary white supremacist groups in the United States. A doctrine of “leaderless resistance” elaborated by one extremist leader, Louis Beam, shows—disturbingly, but with great relevance for understanding netwar in the information age—the importance of doctrine for organization and behavior. This particular doctrine downplays hierarchy in favor of a network of “phantom cells.” It reveals a belief that the more an extreme right-wing movement conforms to networked organizational designs, the more robust it will be defensively, and the more flexible offensively.

Utilizing the Leaderless Resistance concept, all individuals and groups operate independently of each other, and never report to a central headquarters or single leader for direction or instruction. Participants in a program of Leaderless Resistance through Phantom Cell or individual action must know exactly what they are doing, and exactly how to do it.

Since the entire purpose of Leaderless Resistance is to defeat state tyranny . . . all members of phantom cells or individuals will tend to react to objective events in the same way through usual tactics of resistance. Organs of information distribution such as newspapers, leaflets, computers, etc., which are widely available to all, keep each person informed of events, allowing for a planned response that will take many variations. No one need issue an order to anyone (Beam, 1992).

Beam’s doctrine calls for four types of cells: (1) command, (2) combat, (3) support, and (4) communiqué. Each cell consists of about eight “minutemen” and has its own leader. This allows for a specialization of function and tight security precautions.

Similar doctrinal instructions reportedly appear in a manual used by U.S. militias that, while not necessarily white supremacist, have objectives and worry about threats that call for a secretive, decentralized cell structure:
The fundamental rule guiding the organization of the free militia is generalized principles and planning but decentralized tactics and action.

What is meant by this key statement is that the whole militia must be committed to the same cause and coordinated in their joint defense of a community. Thus, there must be allegiance to a higher command. But specific tactics should be left up to the individual elements so that compromise of a part does not compromise the whole. Furthermore, all training and combat actions should be up to the smaller elements, again so that isolation or decapitation does not render the smaller units inept.

The way a balance between these competing concerns is achieved in the free militia is to organize all elements into “cells” (Field Manual Section 1: Principles Justifying the Arming and Organizing of a Militia, Wisconsin: The Free Militia, 1994, p. 78).

These are important tenets for netwar; they show the importance of the doctrinal level for analyzing netwar actors and are consistent with the concept of SPINs mentioned earlier. Although the quotations are drawn from writings about U.S. right-wing groups, they hark back to the U.S. Committees of Correspondence, and to European anarchist doctrines. Overall, they reflect a looser approach to decision-making and operations than traditionally found in right- and left-wing movements—compare, for example, to Mao Zedong’s doctrine that “command must be centralized for strategic purposes and decentralized for tactical purposes.” (See Burghardt, 1995a, and 1995b, from which the quotations are taken; and Stern, 1996.)
Transnational Criminal Organizations (TCOs) Are a Major Dimension of Netwar

- TCOs are developing powerful, sophisticated hybrids of all-channel, star, and chain networks
  - Build on ancient clannish traditions
  - Excel at exploiting immigration and globalization
  - Form dark alliances—partnerships that penetrate legitimate structures
  - Versatile and adaptable, both offensive and defensive

"They are able to do this partly because . . . of their emphasis on networks rather than formal organizations" (Williams, 1994).

Transnational criminal organizations (TCOs), though eminently modern, have a long history, dating at least from the pirate networks that ravaged Mediterranean trade during the first Caesar’s day. The Muslim Cult of the Assassins was organized similarly, operating over a wide territorial base. Finally, the Italian Mafia, the Chinese Tongs, and the Japanese Yakuza have clear roots in the Middle Ages.

The ability of TCOs to prosper in international systems dominated first by empires and later by states lies in their tight kinship ties and loosely knit networked structures. That they have long practice in coping with hostile environments implies their likely continued success in an increasingly interconnected world in which the dominant political entities (states) are growing ever more “soft-edged.”

TCOs, as Phil Williams has pointed out, are a burgeoning problem in the information age, in large part because they are extremely well-suited, organizationally, to operate in an era marked by greater interconnectivity:

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).

TCOs are developing sophisticated hybrids of all-channel, star, and chain networks that build on long traditions of clannish networking. They excel at exploiting trends that enhance interconnectivity. They are versatile and adaptable and have a proclivity to form odd alliances and partnerships that can penetrate legitimate political structures.
TCOs have developed alarming offensive as well as defensive capabilities. Criminal predations in Colombia provide a clear example of the creation of a virtual "kleptocracy," where legitimate institutions must continually fight for their autonomy. This war is waged by criminal networks in loose alliances (cartels) that draw resources from their international operations. Colombia has little ability, alone, to combat transnationalized opponents. Even the recent captures of cartel leaders have had only modest effects, because the cartels are organized in mixed all-channel, chain, and star networks, which are not easily susceptible to counterleadership targeting.

The threat of states besieged by TCOs is not unique to Colombia. Russia faces a similarly stern challenge from a variety of criminal enterprises, of which the Chechen Mafia is only one. Italy has recently learned of sophisticated penetrations of its institutions by the Sicilian and American mafias (e.g., the indictment of former Prime Minister Giulio Andreotti for colluding with the Mafia). Perhaps more troubling is evidence that, as states often form alliances, TCOs are entering into dark pacts, carving out spheres of influence and making common cause wherever possible, as the late Claire Sterling noted (1994). States, loath to cede any sovereignty, have great difficulty coping with such enterprises, though the recent establishment of Europol shows some willingness to relax sovereignty in return for enhanced crime-fighting capabilities.

Criminals often use methods of "epistemological warfare" as they insert themselves deeply into the fabric of societies, embrace nationalism, act like "Robin Hoods," and corrupt their governments' foreign and domestic policies. Examples abound in Colombia, Italy, Mexico, and Russia.

Some states use criminals to pursue national goals. China sponsors both intellectual and maritime piracy. The former invigorates the economy, its competitiveness, and trade balance. Sea piracy (e.g., of oil tankers) abets Chinese efforts to exert hegemony over the Spratly Islands. Harassment by pirates presumably makes other governments succumb to Chinese claims that its presence is needed to control the threat. The example of the East Asian pirates is not unlike the curious relationship of the Royal Navy and the Barbary Pirates in the early 19th century. Britain fostered their depredations against ships of other, competing nations (including the United States). This drove much international trade onto British flag vessels and had profound effects on the costs of goods in many countries.
Criminal netwar appears in the arms and drug trades, trafficking in illegal immigrants and merchandise, and money laundering. States with acute TCO problems include China, Colombia, Italy, Japan, Mexico, Nigeria, and Russia. In the post-Cold War era, TCOs benefit from the unsettled nature of the international system and from the strains that so many states are suffering. Uncertainty about alliances and about security guaranties fosters a thriving demand for arms, including weapons of mass destruction, and TCOs have tried to fill the role of supplier. Increasingly, competitive economic relations put a premium on intellectual property, another area into which TCOs have moved. Economic dislocation and internal conflict have induced masses of people to emigrate by any means, providing yet another opportunity for illicit activity. The drug trade remains a key activity, though these other “profit centers” suggest that TCOs, like successful corporate ventures, can diversify into many areas in which they have comparative advantages.

While TCOs often sought to coexist with states in the past, their new activities have increasingly corrosive effects on state power, signaling the possibility of serious clashes with states (Anderson, 1989; Clutterbuck, 1990). This implies two plausible TCO strategies. First, the TCO might choose to cooperate with one or a few state “hosts,” becoming an unusual basis and agent of state power. The other strategy would pursue a more confrontational approach, fending off state control, or, in some instances, establishing an informal “shadow state” to co-opt the host.

Our look at TCO operations and interactions suggests that both strategies have enjoyed substantial success. In terms of collaboration with a host state, China stands out as a preeminent example. Despite official calls for an end to corrupt practices and ties to organized crime, there is abundant evidence of a substantial symbiosis, particularly in areas relating to illegal immigration and to industrial espionage.
(Bresler, 1981). The Chinese diaspora offers fertile ground for the establishment of ties to Chinese TCOs, suggesting that, as concern grows about China's emerging great-power status, there should also be a growing awareness of its tremendous potential for netwar, not least in terms of its use of TCOs.

Another, albeit lesser, case is the collaboration of the Nigerian government with various TCOs. As in China's case, the Nigerian state is not imperiled but has a principal-agent relationship with the TCOs. Similar issues may also be raised about Mexico, where drug traffickers have built a full range of operations. But in this case, the available evidence suggests that the TCOs may be trying to "capture" parts of the Mexican government. Russia appears to have a similarly fractious relationship with the many TCOs plying their trades on Russian territory, and the Japanese Yakuza can be seen as engaging in similar efforts, though in this case their targets are industrial concerns (Vaksberg, 1992; Kaplan and Dubro, 1986).

In two cases, TCOs have mounted sustained assaults on the foundations of statehood: in Colombia and Italy. In the former case, these activities have come perilously close to causing the "failure" of the state itself. In the Italian case, Mafia predations have helped to divide Italy between the increasingly impoverished South, where organized crime's power is greatest, and the prosperous North, which has thus far been reasonably well-defended.

As these cases indicate, TCOs have a great strategic and tactical flexibility that results partly from their networked natures. Thus far, governments have had mixed results dealing with them. Part of the problem is that hierarchical institutions are often ill-suited to grapple with networked opponents. To adapt, governments have begun to adopt internal reforms, so that "stove-piped" bureaucratic approaches to law enforcement give way to interagency (i.e., network-like) approaches. Governments may also have to be willing, externally, to relax sovereignty enough to foster the rise of transnational crime-fighting mechanisms that are capable of the same nimbleness of maneuver across borders as exhibited by the TCOs. The next chart provides an example of just this sort of development.
Southeast Asian Piracy: Instructive Case of Criminal Netwar and Counternetwar

- Resurgence is serious (echoes of 19th century)
  - Pirates developed multinodal structures
  - Attacks posed financial and environmental risks
- State-by-state responses failed
  - Joint efforts inhibited
  - Pirates circumvented countermeasures
- Network-style innovations are working
  - Intermilitary information sharing
  - Relaxation of state sovereignty

The recent resurgence of piracy in Southeast Asia\(^1\) provides a valuable case for examining netwar and counternetwar strategies and operations. This resurgence, which echoes the activities of the Penang and other Southeast Asian pirates of the 19th century, has posed serious financial and environmental risks. In addition to the values of commercial ships and their cargoes in general, the pirates have focused on attacking oil tankers. Sometimes, fearing interception, the pirates have abandoned their raids, leaving tanker crews bound and gagged while their ships run without piloting, sometimes for hours, in the narrow Strait of Malacca. Back in the 19th century, the Royal Navy faced few political or legal constraints and could deal summarily with such pirates. Today, these waters are divided among a number of states, all of whose sovereignty claims must be respected. The pirates, who have developed multinodal structures and sometimes engage in loose principal-agent relations with regional states, have taken full advantage of their balky, hierarchical adversaries.

Initially, those states whose territorial waters were the scenes of piracy (Indonesia, Malaysia, Singapore, and the Philippines) attempted to resolve the problem independently of each other. These efforts failed miserably during the late 1980s and early 1990s, because the pirates learned to move in and out of territorial waters, much as American gangsters of the 1920s and 1930s were able to avoid local and state police by crossing state lines.

With incidents of piracy rising at a precipitous rate (about 20 percent per year), local states decided to share additional intelligence and went so far as to engage in cooperative interdiction efforts. More-decentralized command and control systems

---

\(^1\)Facts and figures used herein derive from the *Violence at Sea Database* (1995).
emerged, allowing for rapid responses. Even some relaxation of state sovereignty occurred. Military and police elements, within and between these countries, began to coordinate more directly and continuously. Within a year, piratical incidents in Southeast Asia fell by 50 percent. In 1994, no acts of piracy occurred in the Strait of Malacca. The networked response to dealing with the pirates was working, in the wake of the failure of traditional state-by-state responses to the problem.

This is a fine example of network-style innovations working to combat an age-old problem that once again threatened the freedom of the seas. Success came through both intermilitary (and police) information sharing and the relaxation of state sovereignty. Interestingly, the pirates appear to have picked up their operations and moved them to the vicinity of the Spratly Islands, an area riven by conflicting sovereignty claims. There is some evidence, though it is not conclusive, that China is tolerating these pirates. In any case, the 40 percent increase in pirate attacks in this area suggests that, where international and interorganizational cooperation are lacking, such depredations may flourish.

Finally, it is crucial to note that these pirates, though tied into a tradition as old as history, have shown great interest in and sensitivity to the tools and organizational concepts of the information age. Thus, they frequently locate buyers for their contraband (including oil) on the “spot market,” and sometimes create new identities for seized ships and their cargoes. These “phantom ships,” which are real, are occasionally used as the basis for creating fictitious doubles, which are then insured, “lost at sea,” and submitted to claims for insurance reimbursement. Surely, the Cilician pirates from Roman days, or the Barbary corsairs, would nod in proud wonder at such activities. To cope with pirate networks that support the phantom ship business, a whole new set of intelligence and operational skills will be needed.
Revolutionary and terrorist groups have been players in world politics since at least the days of the Zealots, who tried to free Palestine from Roman rule two thousand years ago. Lewis Gann’s (1971) rich history of these groups documents that they have had a common tendency toward centralized leadership and hierarchical control. In the 20th century, Leninist views about the importance of centralized control, no doubt growing out of the centralized Bolsheviks’ success in 1917 Russia, have culminated in the *foco* theory of guerrilla warfare expounded by Fidel Castro and Ernesto “Che” Guevara (Goren, 1984). However, centralized leadership, which worked well in a militarily defeated, war-weary Russia, may, under most other conditions, make revolutionary and terrorist organizations vulnerable to counterleadership targeting, a tactic often used against them, and one that continues to cripple those that maintain hierarchical structures. Thus, *Sendero Luminoso* in Peru suffered severely when its charismatic leader, Abimael Guzmán, was captured, and the Islamic Brotherhood was put virtually out of business when its commander was assassinated in late 1995 in Malta.

Now, perhaps partly in response to the increasing vulnerability if not obsolescence of Leninist and Fidelista designs in a world defined by U.S. preponderance, many revolutionary and terrorist organizations are adopting networked command structures that are segmented and polycephalous (i.e., having a number of commanders who are positioned at various nodes but who are able to exert strategic control over the whole network). This new approach to their organization harks back to the SPIN design (see p. 10 above) that is increasingly found among netwar actors.

Historically, efforts to counter terrorists and revolutionaries have centered either on the establishment of preclusive security procedures to protect vulnerable places and people, or on the infiltration of these radical groups. Preclusive security has never
resulted in "leak-proof" point defenses, as even the most vigorous programs (e.g., Israel's) indicate. Infiltration has also had a problematic record, because the terrorists' networks limit the damage that an infiltrator can inflict prior to exposure. Moreover, many years may be required to move into a position of authority, with advancement contingent upon the commission of acts of terrorism. Thus, in addition to the matter of temporal constraint, the infiltration option runs up against Western normative inhibitions about committing terrorist acts as part of combating terrorism (see Rivers, 1986).

The evolution of terrorism (and criminal organizations, militias, etc.) has been from cells arranged and controlled hierarchically (Laquer, 1979) to networks of cells, with a new mix of civilian and military elements. For example, the PLO has highly centralized decisionmaking around a common doctrine and dominant leader (Yasir Arafat). In contrast, Hamas has devolved much decisionmaking authority to local cells, eschewing a "cult of the leader" (Cobban, 1984).

Aum Shinrikyo, the Japanese religious cult responsible for the recent series of chemical attacks throughout Japan, may provide an example of a new, hybrid type of organization. It is hierarchical, in the sense that the leader (now under arrest) embodied the doctrine of the cult, providing its overarching sense of vision and mission. Operationally and tactically, however, the organization appears to have been quite decentralized. Nevertheless, because of the centralization of its strategic and doctrinal dimensions, the cult was still susceptible to serious damage as a result of the loss of its leader. Thus, a key implication for counternetwar may be to continue to focus operations against any remaining hierarchical elements in the terrorist or revolutionary organization's institutional design.

Finally, the dilemmas posed by these changes in terrorist organizations imply that governments might be well advised to adopt an information-based counternetwar to combat terrorism. When protecting persons or places or infiltrating terrorist groups seems problematic, then detecting, monitoring, tracking, and anticipating terrorist moves, particularly those of semi-autonomous cells, will prove of paramount importance. This issue is discussed further in the doctrine and strategy portion of this study.
Cyberspace is an increasingly attractive venue for terrorism and sabotage. The list of actors who may be drawn to cyber-terror or "cybotage" is long and includes anarchists, nihilists, and anarcho-syndicalists, at one end of a spectrum, and societal misfits, disaffected scientists, disgruntled employees (or ex-employees) and hackers at the other. Many such actors today operate primarily as loners (e.g., Kevin Mitnick) or in juvenile leagues (e.g., the Legion of Doom). This will likely remain the case to some extent, perhaps because this phenomenon is still in a formative stage (Hafner and Markoff, 1991). But meanwhile, more sophisticated, better organized actors are emerging, including "cyber mercenaries" and information warfare specialists who may be developed from within or recruited into the ranks of terrorist or revolutionary organizations or cults (e.g., the Church of Scientology has apparently recruited or developed a cadre of netwarriors to deal with dissidents and apostates).

Cyberspace offers opportunities for such actors to inflict costly, disruptive damage, but without inflicting the physical and human destruction that so often arouses the ire of victims, or that may even alienate the affections of the terrorists' sponsors or constituencies. Unlike blowing up planes or killing hostages, disrupting the flow of information can inflict enough pain to convey the symbolic message so central to terrorism, while avoiding the more unsavory aspects of traditional destructive terrorism.

A reason for terrorists to move into cyberspace is to cause disruptions that have widely diffuse effects. Previously, terrorist attacks tended to cause serious physical damage in limited spaces (though the repercussions through the media may have been global). The easing of spatial limitations on the direct effects of acts of terror should prove quite attractive. Finally, terrorists will find, no doubt, fertile ground for recruits willing to engage in acts of "cybotage."
Of course, one cannot overlook the possibility that terrorists themselves will see merit in becoming as adept at computer hacking as they try to be at killing (Reich, 1990). An ability to threaten the national information infrastructure (NII) and C3I systems gives terrorists another way to command media attention, thereby affecting the primary means by which Americans inform themselves about the world. Such a prospect poses the opportunity to make great gains, while controlling risks and doing little violence to innocent people. Indeed, for some terrorists, netwar may provide the best of all worlds.

Compared with other types of netwar, this type is one of the easiest about which to be alarmist at this stage in the information revolution—but it is also the type whose implications for netwar are among the most uncertain. It is relatively easy to concoct havoc-wreaking scenarios (Collins and Lapierre, 1979; Hundley and Anderson, 1996; Kupperman and Kamen, 1989; Schwartau, 1994). Yet, it is unclear whether these scenarios are realistic. This is reminiscent of extreme terrorism scenarios of the 1970s and 1980s, in which the United States may be momentarily brought to its knees—but, so far, such scenarios have not unfolded, in part because they presume both ends and means that, in fact, lie beyond the reach of terrorists and should continue to do so as defenses form and spread.

Often when we have presented the concept of netwar, audiences have presumed the term denotes primarily the types of actors discussed on this chart: cyberterrorists, cyboteurs, and various societal misfits who have the skills of hackers. While these actors sometimes fit the pattern of netwar, this is not always the case. It is particularly not the case for the lone hacker who is simply engaging in vandalism in cyberspace. It is more the case where such actors have links to, or are members of, an organized network that has clear goals and missions, and cohesive doctrines for effecting them. Indeed, the significance of cyberterrorists and cyboteurs for netwar may depend upon their “fit” into the other types of actors discussed here (e.g., those having to do with ethnonationalist struggles, criminal enterprises, or militant civil-society conflicts). Lone hacker Kevin Mitnick is far less a netwarrior than the Zapatistas' Subcomandante Marcos.
Social struggles form another arena where netwar is on the rise. Since the 1970s, the world has entered an era of “new social movements”—of information-age activism based on associations among NGOs concerned with modern and postmodern issues such as the environment, human rights, immigration, indigenous peoples, cyberspace, etc. When such struggles turn militant, there is usually evidence of “social netwar.”

We see this, for example, in the domestic U.S. conflicts about abortion and environmental issues (e.g., see Chase, 1995), and at the global level in the campaigns of human-rights organizations against dictatorial regimes. Elements of social netwar appear in efforts by Chinese students abroad to aid their companions in Tiananmen Square, in alliances among American and European “skinhead” groups, and in the global campaign by Greenpeace and its allies to try to compel the French government to halt nuclear testing in the Pacific. While these particular examples do not represent clear victories by nonstate against state actors, they help define a trend and indicate that governments are going to need great agility and adaptability to cope with threats and challenges from social netwarriors in the coming decades. Yet, it is far from clear that NGOs will be able, as a rule, to erode state power.

Our comments focus on the rise of netwar-related forms of organization, doctrine, strategy, and communications to support transnational activism. Social netwar at this level is conducted largely through vigilant swarming. And to this end, a global

---

2 Bibliography on this phenomenon is still sparse. Sources, in addition to those cited earlier regarding the rise of civil society, include Boulding (1988); Brecher, Childs, and Cutler (1993); such academic volumes on “new social movements” as Laraha, Johnston, and Gusfield (1994), and Morris and McClurg (1992); and a special issue of Social Research, Vol. 52, No. 4 (Winter 1985).
network structure is being built up. It consists of issue-oriented groups (such as Doctors Without Borders) and infrastructure-building organizations (such as Global Exchange) that can mount a campaign around any issue. This structure has no central leadership or ideology, although some activists and political tendencies may be stronger than others. Instead, it is characterized by what we call "collective diversity" and "coordinated anarchy"—once a focus arises (e.g., Mexico), activist NGOs that find any connection to their specialty (e.g., peace, sustainable development, etc.) may join the swarm and choose autonomously but consultatively in which actions to participate. Building a communications infrastructure (like the APC networks—see pp. 23–24) that enables rapid mobilization is very important to this structure.

Doctrine and strategy for transnational social netwar remain nascent, but some outlines have emerged. Briefly, as we have noted elsewhere, they involve making civil society the vanguard—and constructing a "global civil society" that can connect to local NGOs, and that can counter state and market actors. They also include "information" as the decisive weapon. Indeed, in a social netwar in which a set of NGO activists challenge a government or another set of activists over a hot public issue, the battle is largely about "information"—about who knows what, when, and where. A social netwar involves seeking total intelligence or "topsight" (Gelernter, 1991) about one's own and the opponent's situation, while keeping that opponent in the dark about oneself and, if possible, about its own situation. It involves affecting what an opponent knows, or thinks it knows, not only about its challenger but also about itself and the world around it. Among other things, this may mean trying to shape images, beliefs, and attitudes in the social milieu in which both are operating. A social netwar is thus likely to bring demands for freedom of information and battles for public opinion and media access and coverage to local and global levels. It may include propaganda and psychological warfare, not only to inform but also to disinform. It may well resemble a nonmilitary version of Szafranski's (1994, 1995) notion of "neo-cortical warfare."

Many varieties of netwar—e.g., criminal and terrorist—that we discuss in this document threaten U.S. interests. We do not mean to imply that social netwar also generally poses a threat. Indeed, as noted below, social netwar may sometimes benefit U.S. interests. Our point is that transnational NGO activists are on the cutting edge of developing new network forms of organization, doctrine, and strategy—and whoever wants to understand netwar dynamics would be well advised to study their innovative models.
Mexico Provides Major Example of Transnational Social Netwar

- Subnational and transnational actors link to confront state lagging at democratization and development
  - Zapatistas nearly trigger counterinsurgency
  - Influx of transnational activist NGOs restrains government and alters context of struggle
- New model of conflict tested by “netwarriors”
  “Chiapas . . . is a place where there has not been a shot fired in the last 15 months. The shots lasted 10 days, and ever since the war has been a war of ink, of written word, a war on the Internet”
  — Mexico’s Foreign Minister Jose Angel Gurria, April 1995
- Mixed results (counternetwar also under way)

In Mexico, a mix of subnational and transnational actors have mounted a social netwar against a state lagging at democratization. The netwar appears in the decentralized collaboration among the numerous, diverse Mexican and transnational (mostly U.S. and Canadian) activists who side with the Zapatista National Liberation Army (EZLN), and who aim to affect government policies on human rights, democracy, and other major reform issues. Mexico, which generated the first successful social revolution of the 20th century, is now the scene of a prototype for social netwar in the 21st century.

The Zapatistas are insurgents—in some eyes, the first post-Communist, postmodern insurgents. But the dynamics that make their insurgency so different—notably, the strategic links to activist NGOs—move them out of an “insurgency” into a “netwar” framework. Without the influx of foreign NGO activists, which began hours after the EZLN’s insurrection on New Year’s Day 1994, the dynamics in Chiapas might have deteriorated into a conventional insurgency and counterinsurgency—and the small, poorly equipped EZLN might not have done well. Transnational NGO activism, not the novel insurgency per se, is what changed the framework.

The EZLN’s artful “Subcomandante Marcos” says that a new model of social conflict and transformation is being tested. He and his cohorts have eschewed Leninist, Maoist, and Fidelista models that call for an army or a party to seize power as the vanguard of revolution. Instead, their agenda (e.g., political democracy and regional autonomy) is more reformist than revolutionary (Castañeda, 1995). They deny that they want state power (though they aim to change the state). According to Marcos, “It is civil society that must transform Mexico—we are only a small part of that civil society, the armed part. . . .” The activation of civil society—not the expansion of an insurgent army—is the key feature of their doctrine.
NGO activists—some call themselves “netwarriors”—realize that they are developing a new model of conflict (e.g., Cleaver, 1994). For many, nonviolent but compelling action is crucial; and to this end, they need rapid, far-reaching communications, and freedom of information and travel. Much of their netwar has been waged in the media—in both old media like newspapers, magazines, and television, and new media like faxes, e-mail and computer billboard and conferencing systems. Since word of the insurrection first spread, the activists have made heavy use of the Internet (and systems like Peacenet) to disseminate news, mobilize support, and coordinate actions. Each side has waged public-relations battles to affect public perceptions of the other. Thus, in April 1995, Foreign Minister Jose Angel Gurria could comment that

Chiapas... is a place where there has not been a shot fired in the last fifteen months... The shots lasted ten days, and ever since the war has been a war of ink, of written word, a war on the Internet.

This social netwar has been partially effective. It helped compel President Carlos Salinas in January 1994, and President Ernesto Zedillo in February 1995, to halt army operations and turn to political negotiations in Chiapas. It has added to the national pressures on Mexico’s rulers to enact political reforms, take human rights more seriously, accept the rise of civil society, and heed the needs of indigenous peoples. It may also be obliging the Mexican army to adopt institutional changes. In such respects, this netwar has not been bad for Mexico (or for some U.S. interests), even though it has heightened uncertainty about Mexico’s stability.

This netwar, and the government’s efforts at counternetwar, are far from over. Although the EZLN amounts to a figurative “army-in-being” that poses more a symbolic than a real threat of violence, the Zapatistas and their civil-society allies have effectively challenged and disrupted the Mexican system. The high visibility of the episodic peace negotiations in Chiapas, the unusual national poll known as the National Consultation, and the mixed results of the National Democratic Conventions sponsored by the EZLN attest to this. More to the point, the netwarriors evidently have a capacity to keep up the pressure, as just indicated by the creation of a nonmilitary FZLN (Zapatista National Liberation Front), whose aims include rallying nationwide support among marginalized indigenous peoples, and pressing for reforms independently of political parties.
Implications Extend Far Beyond Mexico

- Conditions for social netwar to be effective
  - Society should be partly open, under strain, and have local counterparts for transnational NGOs
  - Society should be in region where activists have transnational communications infrastructure

- Netwar may prove potent for affecting some nations
  - Disrupting authoritarian regimes
  - Spurring democratic reforms

- Future cases:
  - Cuba, Nigeria, Russia, or Saudi Arabia?
  - New global peace and disarmament movement?

This Mexican prototype has implications that extend beyond Mexico, for it indicates conditions that should be present for a transnational social netwar to develop. As in the case of Mexico, a society should be relatively open (or opening up), particularly as regards freedom of information. It should be in flux and under political, economic, and other strains that are generating public debate; this may be the case especially where traditional clannish and hierarchical structures are challenged by, and adapting with difficulty to, new market and civil-society forces. The society should also have local NGOs that transnational NGOs can link to—more to the point, the society should be in a region where the transnational infrastructure for social activism is growing in both organizational and technological terms.

Because such conditions are not present everywhere—e.g., they apply far less to Myanmar than to Mexico—social netwar may affect some nations more than others. Where the conditions are ripe, the Mexican case implies that social netwar may work to disrupt authoritarian regimes and compel them to make democratic changes. Social netwar is in its infancy as a mode of conflict, and governments are just beginning to learn about it, but its importance and effectiveness are likely to grow around the world.

The scenes of future social netwars could include such countries as Cuba, Nigeria, Russia, and Saudi Arabia, to mention a few possibilities. In Cuba, the prospects for social netwar are increasing. Castro’s government has begun to open up the economy but persists in political and social repression. Meanwhile, grassroots groups are trying to open space for activities within Cuba and gain connections to outside NGOs, including through faxes and e-mail (Gonzalez and Ronfeldt, 1994). Aspects of netwar have been present for decades in U.S.-Cuban relations, notably in the U.S. broadcasting and Cuban jamming of Radio Martí, as well as in the activities of pro-
and anti-Castro groups in the United States. What may be emerging now are the conditions for a full-fledged social netwar.

In Saudi Arabia, the ruling family retains tight control of the country, 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, the opportunities may improve for an indigenous dissident movement to develop that has 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’s, the higher the costs of repression and control will become for the ruling regime. Note, for example, that even a deliberately information-age autocracy like Singapore’s cannot prevent the rise of stealthy activists using faxes, e-mail, computer networks, etc.

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 who are attuned to the doctrinal elements of netwar. They will increasingly have the organizational, technological, and social infrastructures to fight against recalcitrant governments, as well as to operate in tandem with governments and supranational bodies that may favor the movement.

U.S. officials and analysts are accustomed to viewing economic actors and policies as potential instruments for urging foreign governments to move in liberal democratic directions. Transnational civil-society actors whose focus is more informational than economic may prove even more potent as information-age instruments of policy (e.g., “democratic enlargement”). Indeed, many networked NGOs are as transnational as corporations—and they can move faster, too. Chris Kedzie’s (1995) work on the positive correlation between political democracy and communications connectivity provides a basis for urging that policymakers begin to treat information as a new dimension of policy and strategy (see Arquilla and Ronfeldt, 1996).
A World Crisscrossed by Netwars

- Some adversaries may be global, attempting to affect world order
  - Radical Islamic or other fundamentalist movements or states
  - Interneted criminal enterprises
  - Information-age NGO activists or ideological movements
- Other protagonists may be regional or local
  - Most ethnonationalist movements
  - Local grievance groups, reform movements, and insurgents
- Vertical and horizontal interactions and linkages
  - Global actors may exploit local groups
  - Local groups may connect to local, transnational groups

We have shown that network forms of organization (and hybrids with other forms) are spreading among a broad array of actors, strengthening them in ways that present new and continuing difficulties for those who want to control or defeat them. Again, many of these types of actors have deep historical roots, but largely because of the information revolution, they are gaining organizational vibrance, a sense of mission, and an improved robustness against countermeasures.

Some of the types discussed operate in isolation, but often there are cross-linkages. Chechen ethnonationalists, for example, are fighting for the autonomy of their region from Russia; at the same time, Chechens are deeply involved in what is known as the Russian mafia, which has nodes throughout the former Soviet Union, in eastern and central Europe, and even toeholds on both coasts of the United States. Interestingly, Dzokhar Dudayev, the Chechen rebel leader, attempted to deter the recent Russian incursion into Chechnya by threatening an escalation of the conflict throughout Russia, utilizing “forward-based” nodes of the Chechen mafia network as jumping off points for a punitive netwar.

Netwar protagonists will likely range from those that have global agendas and capabilities, to those that are regional or local in orientation, to those that oscillate between global and local agendas. Islamic revivalists seem to fit all these patterns—sometimes they focus on influencing events in specific countries (e.g., in Egypt and Algeria); at other times their endeavors have a regional focus (e.g., Middle Eastern-sponsored efforts in the Levant, former Soviet Central Asia, and the Persian Gulf); and, finally, there are occasions when Islamists try to affect the tone of world politics. An example of this last phenomenon can be seen in the expansive terrorist planning of Sheik Rahman, whose campaign of terror sought to deter American involvement in “managing” the affairs of the international system.
In addition to its attractiveness to terrorists, netwar will likely become a mode of conflict of choice for a multitude of state and nonstate actors. This choice, or tendency, may be fostered by the very preponderance of American power in the post–Cold War world. Simply put, the lopsided victory over Saddam Hussein may have proved that trying to imitate the power possessed by the United States is too difficult. Instead, challenging American preeminence in unconventional ways, such as are afforded by a netwar doctrine, is indicated.

In the future, many adversaries will be transnational, even global, and will have the potential to affect (and perhaps threaten) political and economic aspects of the world system. Such actors may include (in addition to the aforementioned radical Islamic fundamentalist movements and the states that support them): internetted transnational criminal enterprises and information-age social and ideological movements. Other actors may be regional or local, principally including most ethnnonationalist movements along with local grievance groups and other insurgents.

There will likely be both vertical and horizontal interactions among them. At the vertical level, global actors may exploit local grievance groups for their own purposes, or vice versa. The Zapatista movement, for example, could be viewed as a local grievance group that has linked up with global human-rights and other activist NGOs in a netwar against the Mexican government.

Another possibility, this time at the horizontal level, is that local groups may connect to other local groups, or global actors to other globals. In waging defensive netwar, it will be useful to understand the nature of the opponent’s structural alliances. Coping with a violent local insurgency may be complicated if it has reached out to nonviolent civil society actors for support. The Mexican government is learning this in Chiapas.

Because of the likely profusion of netwars, it may be advisable to begin tracking and cataloging them in all their varieties and locations. This could be undertaken along the lines of annual reports similar to ones that already exist about more traditional modes of conflict (e.g., the volumes by Brassey’s and by the Stockholm International Peace Research Institute).
The United States in the Age of Netwar

- The United States will benefit from new epoch
  - Consolidation of power at global level
  - Diffusion of power in and to regions
  - Potential new allies among NGOs
- The United States will face new vulnerabilities and risks
  - Openness, power, and restructuring invite challengers
  - The United States may be besieged by multiple netwars
  - U.S. allies may also be besieged
- The United States is vulnerable whether it is isolationist or globalist

The United States should benefit mightily from the information age. It is moving toward a consolidation of power at the global level; at the same time, it stands to benefit from a diffusion of power in and to actors at the regional level who may be beholden to the United States. As noted earlier, U.S. power and presence around the world should also benefit from the proliferation of potential new allies among NGOs, and from the usage of “information” as a fourth dimension of grand strategy.

Yet, the age of netwar will pose threats, risks, and vulnerabilities for the United States, perhaps more so than for any other advanced society. U.S. openness, one of its greatest assets, becomes a double-edged sword; its very openness as well as its superpower status in an era of restructuring is bound to invite challengers.

As a result, U.S. government and society should expect to be besieged by multiple netwars: leftist and rightist, domestic and foreign, social and criminal, etc. Moreover, U.S. allies may also be besieged, not only in Europe but also in parts of the Middle East and Latin America. We may have to be selective about which netwars to fight, and about which adversaries can most affect our society and security.

U.S. foreign policy, and debates about U.S. foreign policy, tend to oscillate between isolationist and globalist options, with protagonists arguing that the choice can have major effects on our vulnerabilities. Yet, the argument should not be overlooked that the United States will remain vulnerable to netwar whether it opts for isolationist or globalist foreign policies. U.S. society is too interdependent, too interconnected, with the rest of the world for policy orientation at this level to make a major difference, even though once made, the choice may affect the specific mix of vulnerabilities.
Many points we make here are reminiscent of points long made about U.S. vulnerability to international terrorism. Indeed, there may be embedded tendencies in some quarters to react to netwar in terms of antiterrorism models. Those models may be instructive—some terrorist organizations are designed for violent netwar—but they cannot be definitive. Netwar is a broader and a different mode of conflict.