SUMMARY

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

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

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

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

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

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

While a network's level of technological sophistication does make a difference—and people do tend to think that netwar depends heavily on technology—the other levels have just as much, if not more, of an effect on the potential power of a given group. One key level is the social basis for cooperation among network members. When social ties are strong, building mutual trust and identity, a network's effectiveness is greatly enhanced. This can be seen most clearly in ethnically based terror, crime, and insurgent groups in which clan ties bind together even the loosest, most dispersed organization.

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

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

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

The most potent netwarriors will not only be highly networked and have a capacity to swarm, they will also be held together by strong social ties, have secure communications technologies, and project a common "story" about why they are together and what they need to do. These will be the most serious adversaries. But even those networks that are weak on some levels (e.g., technological) may pose stiff challenges to their nation-state adversaries. With this in mind, it is necessary to go beyond just diagnosing the nature of the networked nonstate opponent in a given conflict. It will become crucial for governments and their military and law enforcement establishments to begin networking themselves. Perhaps this will become the greatest challenge posed by the rise of netwar.