PREFACE

The fight for the future makes daily headlines. Its battles are not between the armies of leading states, nor are its weapons the large, expensive tanks, planes, and fleets of regular armed forces. Rather, the combatants come from bomb-making terrorist groups like Osama bin Laden's al-Qaeda, drug smuggling cartels like those in Colombia and Mexico, and militant anarchists like the Black Bloc that ran amok during the Battle of Seattle. Other protagonists are civil-society activists fighting for democracy and human rights—from Burma to the Balkans. What all have in common is that they operate in small, dispersed units that can deploy nimbly—anywhere, anytime. They know how to penetrate and disrupt, as well as elude and evade. All feature network forms of organization, doctrine, strategy, and technology attuned to the information age. And, from the Intifadah to the drug war, they are proving very hard to beat; some may actually be winning. This is the story we tell.

This book also provides a further step in the elaboration of our ideas about how and why the information revolution is affecting the whole spectrum of conflict. Our notion of *cyberwar* (1993) focused on the military domain, and our first study of *netwar*[1] (1996) on irregular modes of conflict, including terror, crime, and militant social activism.[2] The implications of these concepts for organization, doctrine, and technology across the spectrum of conflict were further elaborat-

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

[2] For full citations of these and our other studies, please see the bibliographies for Chapters One and Ten.

ed in our book, *In Athena's Camp* (1997). More recently, we noted that many activists who practice netwar are helping to create a new approach to strategy and diplomacy that we call *noopolitik* (1999). Next, we expanded on our idea that *swarming* (2000) will emerge as a 21st-century doctrine that will encompass and enliven both cyberwar and netwar. Here, we offer new analysis about netwar. The analysis includes case studies about terrorists, criminals, and gangs; social netwars in Burma, Mexico, and Seattle; and closing chapters on some of the technological, organizational, and doctrinal dynamics of netwar.

U.S. policymakers and strategists will be interested in this book. It should also interest analysts in academia and research institutes concerned with how the information revolution is altering the nature of conflict.

This book was prepared for a project on "Networks and Netwars," directed by John Arquilla and David Ronfeldt. The project was sponsored by the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), OASD/C3I, and was conducted within the International Security and Defense Policy Center of RAND's National Defense Research Institute (NDRI). NDRI is a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the unified commands, and the defense agencies.

Comments are invited. We can be reached via email at arquilla@rand.org and ronfeldt@rand.org.