

Concern recently has grown within the U.S. national security establishment that the natural protection from attack historically afforded by the nation's enviable geographic isolation—long borders with stable neighbors to the north and south and large oceans to the east and west—may be coming to an end.

One reason can be found in a number of unfavorable long-term trends in the nature of the adversaries of the United States and their potential future warfighting strategies. Future U.S. adversaries, recognizing that they are unlikely to prevail in theater war, it is believed, may instead choose to respond asymmetrically by attacking the U.S. homeland.

The unwillingness of the United States to negotiate with terrorists and its willingness to strike sponsors of terrorism have shaped the environment as well. Contemporary terrorist groups increasingly are more interested in killing than extracting political concessions, and the fear of reprisals has led to an increased desire for covert action and plausible deniability among terrorist groups and their sponsors. The emergence of nonstate and transnational groups accordingly has resulted in adversaries who are more difficult to track and deter than nation states are and who are more interested in creating catastrophic events.

Technology also plays an important role. There are increasing fears regarding the proliferation of weapons of mass destruction (WMD). These include concerns about insecure former Soviet nuclear, biological, and chemical (NBC) weapons and materials or—through efforts by so-called “rogue states” and such well-funded groups as

Aum Shinrikyo and Osama bin Laden's organization—the increasing capacity to develop or acquire such weapons. Similarly, the increasing range and payload of available ballistic missile systems has caused concerns about adversaries' future capacity to attack the United States. Finally, technological advances in information and communication technologies have reduced the importance of geography and made possible attacks on information and communication systems and other computer-dependent infrastructures from anywhere on the globe.

These long-term trends also have been punctuated by a number of attacks at home and abroad that have highlighted the vulnerability to terrorism of advanced societies, such as the United States, and have resulted in widescale death and injury:

- The World Trade Center bombing in 1993, in which six were killed and more than 1,000 injured.
- The bombing of the Murrah federal building in Oklahoma City in 1995, in which 168 were killed and 519 were injured.
- The 1995 use of nerve agents by the Aum Shinrikyo group against the Tokyo subway system, in which 12 were killed and more than 5,000 injured.
- The Centennial Park bombing in Atlanta during the 1996 Olympics, which killed one and injured more than 100.
- The bombing in June 1996 of the Al Khobar barracks in Saudi Arabia, in which 19 servicemen died and more than 300 were injured.
- The simultaneous attacks in August 1998 on U.S. embassies in Nairobi and Dar es Salaam by Osama bin Laden's organization in which 301 died, including 12 Americans.

As described in the Report of the National Defense Panel (1997), the Report of the President's Commission on Critical Infrastructure Protection (1997), the Federal Emergency Management Agency's 1997 assessment of federal consequence management capabilities, and the DoD Tiger Team's report on integration of National Guard and Reserve support for responses to WMD attacks (1998), these developments have motivated policy-level attention to the problem

and the identification of numerous shortfalls in the nation's capacity to prevent or mitigate the emerging threats.

The emerging threats and response shortfalls also have led to the allocation of large-scale resources to the prevention and management of the consequences of terrorist attacks against the United States and to serious discussion regarding the parameters of a homeland security (until recently the mission was known as "homeland defense") mission for the Department of Defense (DoD) and U.S. armed forces. This mission would support the national effort to reduce the risks and consequences of future attacks on the United States.

ORGANIZATION OF THIS REPORT

This report seeks to provide an overview of the key policy issues related to homeland security and is organized as follows:

- Chapter Two describes some of the origins of the homeland security mission and provides a definition and taxonomy of tasks.
- Chapter Three provides an analytic framework and methodology for analyzing homeland security options.
- Chapters Four through Seven apply this framework to the four task areas that are the subject of this study: domestic preparedness (Chapter Four), continuity of government (Chapter Five), continuity of military operations (Chapter Six), border and coastal defense (Chapter Seven).
- Chapter Eight provides illustrative planning vignettes that were used to understand potential Army roles in the homeland security task areas.
- Chapter Nine provides an analysis of Army doctrine, organization, training, leadership, materiel, and soldier systems (DOTLMS) for the homeland security task areas.
- Chapter Ten provides conclusions.
- A number of appendixes in this volume provide additional background material. In particular, we draw the readers' attention to

the appendixes on threat campaigns (Appendix A), a notional Weapons of Mass Destruction Civil Support Team (WMD CST) tradeoff analysis (Appendix B), and a consolidated list of performance measures that should be considered for use in meeting the reporting requirements of the Government Performance and Results Act (GPRA).