JANUARY 1996

Strategic War . . . in Cyberspace

National security is becoming progressively more dependent on and identified with assets related to the "information revolution." As part of this revolution, both defense and civilian activities are becoming more heavily dependent on computers and communications, and a variety of key information systems are becoming more densely and extensively interlinked. With the many benefits of the information revolution have also come vulnerabilities. Civilian data encryption and system protection are rudimentary. Talented computer hackers in distant countries may be able to gain access to large portions of the information infrastructure underlying both U.S. economic well-being and defense logistics and communications. Current or potential adversaries may also gain access through foreign suppliers to the software encoded in U.S. transportation and other infrastructure systems. We could thus one day see actions equivalent to strategic attack on targets of national value within the U.S. homeland and on essential national security components and capabilities. In short, there will exist the capability for *strategic information warfare.*

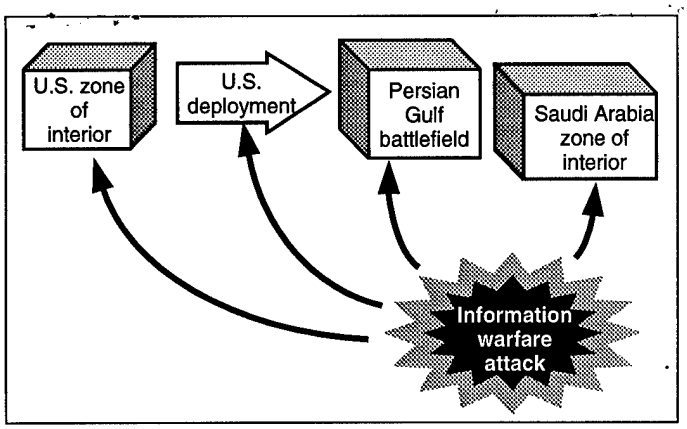
Recognizing this possibility, in January 1995 the Secretary of Defense established an Information Warfare Executive Board to facilitate "the development and achievement of national information warfare goals." RAND was asked to provide an analytic framework and exercise for identifying defensive information warfare issues, exploring their consequences, and highlighting starting points for policy development. Among those points emanating from the exercise were the following:

- Establish within the Executive Office of the President a focal point for federal leadership in support of a coordinated response to the information warfare threat.
- Assess the vulnerability of key elements of current U.S. national security and national military strategy to strategic information warfare.
- Explore the feasibility of developing a minimum essential information infrastructure, permitting effective overseas force deployments and keeping the nation functioning even in the face of a sophisticated information warfare attack.

The exercise leading to these conclusions was conducted by a RAND team led by Roger Molander and is described in *Strategic Information Warfare: A New Face of War.* It was run three times with participation by senior members of the national security community and representatives from U.S. government domestic agencies and the telecommunications and information system industries. The exercise confronted participants with a challenging hypothetical political-military crisis in the year 2000. In this crisis, a conventional Iranian military threat and an internal threat to Saudi Arabia are made more acute by critical information and communication system failures in the U.S. homeland and elsewhere. These failures appear to result from both strategic information warfare conducted from outside the United States and from the actions of domestic anti-interventionist groups.

The exercise scenario thus highlighted from the start a fundamental aspect of strategic information warfare: There is no "front line." Though defense planners are used to thinking of information-related attacks in terms of such actions as jamming in-theater military communications, strategic targets in the United States may prove just as vulnerable. So also may targets in allied "zones of interior" and in the systems supporting U.S. force deployment. As a result, the attention of exercise participants quickly broadened to include four distinct theaters of operation, as shown in the figure.

Strategic information warfare challenges conventional approaches to defense as a result of various defining and closely coupled characteristics:



The Changing Face of War: Four Strategic Information Warfare Theaters of Operation

- **Low entry cost.** In contrast to the strategic nuclear environment of the cold war, a strategic information attack on the United States might be made without access to large financial resources or state sponsorship. The "weapons" could be software "logic bombs" or computer worms and viruses, the "delivery systems," cellular telephones and the Internet.
- **Blurred traditional boundaries.** In cyberspace, the boundaries between nations and private-sector organizations are porous, rendering distinctions between war and crime, and between public and private interests, less meaningful. International activist organizations may function largely over the Internet and provide (perhaps unintentional) cover for information warriors within their ranks.
- **Expanded role for perception management.** New information-based techniques may substantially increase the power of deception and image manipulation activities. Disinformation may make it difficult for the U.S. government to build political support for actions needed to ensure national security.
- **Lack of strategic intelligence.** Vulnerabilities to strategic information warfare are poorly understood. The identities of potential adversaries may be unknown, and classical intelligence collection and analysis methods may not apply. New methods of analysis and interorganizational relations may have to be developed.
- **Difficulty of tactical warning and attack assessment.** There will be formidable problems in distinguishing between strategic information warfare attacks and other kinds of activities and events, such as espionage, accidents, system failures, and hacker pranks. An inability to make such distinctions could lead to very cautious military responses to regional challenges such as those hypothesized in the exercise.
- **Difficulty of building and sustaining coalitions.** Coalition responses could be at risk to the weakest information links binding the alliance. An inability to protect partners from information warfare attacks could jeopardize the United States' ability to form and sustain coalitions.
- **Vulnerability of the U.S. homeland.** The U.S. economy and society rely increasingly on a high-performance networked information infrastructure for everything from air travel and electric-power provision to management of citizens' financial accounts. A new set of lucrative strategic targets thus presents itself to potential information warriors.

These characteristics were elucidated over the course of the exercise, which was based on a methodology RAND had developed previously for exploring counterproliferation and related intelligence issues. The output of the exercise was a set of initiatives intended to minimize the likelihood of a crisis of the type portrayed or, failing that, minimize its consequences. These recommendations, presented near the beginning of this brief, reflect both the potential gravity of the threat as viewed by the exercise participants and their desire not to overreact to what is now largely a hypothetical problem. It is possible, after all, that the evolving information infrastructure will be equipped with adequate protections as its commercial developers respond to local vulnerabilities and concerns. However, the tendency of the exercise participants was to view information infrastructure vulnerabilities and the potential for strategic information warfare far more seriously the more they learned about the subject and debated its implications.

RAND research briefs summarize research that has been more fully documented elsewhere. This research brief describes work done for the National Defense Research Institute; it is documented in Strategic Information Warfare: A New Face of War, *by Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, MR-661-OSD, 1995, 125 pp., $15.00, ISBN: 0-8330-2352-7, available from RAND Distribution Services (Telephone: 310-451-7002; FAX: 310-451-6915; or Internet: order@rand.org). Abstracts of all RAND documents may be viewed on the World Wide Web (http://www.rand.org). Publications are distributed to the trade by National Book Network. RAND is a nonprofit institution that helps improve public policy through research and analysis; its publications do not necessarily reflect the opinions or policies of its research sponsors.*

RAND

1700 Main Street, P.O. Box 2138, Santa Monica, California 90407-2138 • Telephone 310-393-0411 • FAX 310-393-4818
2100 M St., N.W., Washington, D.C. 20037-1270 • Telephone 202-296-5000 • FAX 202-296-7960