This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.
Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense

James C. Mulvenon, Murray Scot Tanner, Michael S. Chase, David Frelinger, David C. Gompert, Martin C. Libicki, Kevin L. Pollpeter

Prepared for the Office of the Secretary of Defense
Approved for public release; distribution unlimited
The research described in this report was prepared for the Office of the Secretary of Defense (OSD). The research was conducted in the RAND National Defense Research Institute, a federally funded research and development center sponsored by the OSD, the Joint Staff, the Unified Combatant Commands, the Department of the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract DASW01-01-C-0004.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN 0-8330-3768-4

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2006 RAND Corporation

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2006 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org
Chinese strategists have avidly consumed U.S. Department of Defense (DoD) writings over the past 10 years and have keenly observed changes in U.S. national strategy and military transformation. Commentary by People’s Liberation Army (PLA) experts on Operation Iraqi Freedom suggests that Beijing believes the Pentagon’s efforts at achieving a Revolution in Military Affairs are not just succeeding, but accelerating. Yet the concomitant acceleration of the pace of Chinese military modernization also suggests that the Chinese are not dissuaded by U.S. military prowess, but instead are driven by a range of strategic and military motivations to continue their efforts apace. This report examines the constraints, facilitators, and potential options for Chinese responses to U.S. transformation efforts and offers possible U.S. counterresponses.

**Constraints and Facilitators of Counter-Transformation Strategies**

China’s response to U.S. military transformation will be shaped by Beijing’s key national security goals (political stability, national reunification, comprehensive national power, and rapid economic development) and the political and economic context within which the goals are pursued. Beijing’s responses will be constrained by major political, social, economic, and international challenges as well as China’s available package of financial and technological resources.
Defense modernization in particular must compete with several enormous, growing demands on budgetary and economic resources in a “decelerating growth” economy. Budget deficits have risen substantially since the late 1990s, and government banks are badly overextended by nonperforming loans to insolvent state factories. Rising social unrest will also heighten “national security” resource competition. Moreover, increased funding for higher education and infrastructure will be essential for defense modernization to succeed. As a result, regardless of their intrinsic strategic merit, the response options that enjoy the greatest political advantages will be those that require lower budgetary demands and start-up costs, draw upon existing technological packages, and simultaneously serve other national security goals such as internal stability and regime security.

**Chinese Counter-Transformation Options**

This report examines four notional Chinese response options to U.S. military transformation. Each is used as a heuristic to illustrate potentially threatening developments. Although these options are discussed in isolation, developments in China suggest that all or portions of each strategy are being pursued in earnest, and some combination of the options will likely characterize the final configuration.¹

**Option One: Conventional Modernization “Plus”**

The first potential strategy is characterized by the use of conventional weapons, including space weapons, submarines, and antiship cruise missiles, to conduct anti-access operations and to strike at perceived U.S. vulnerabilities or high-value targets whose degradation, denial, or destruction could decisively influence the campaign. Of the analyzed options, this strategy is the most feasible because it relies on proven technologies that can be developed or purchased; however, it

¹ The use of nuclear weapons is not discussed in detail given China’s lack of counterforce capabilities, but electromagnetic pulse bursts and conventional missile strikes are analyzed in Option Three.
is vulnerable to U.S. network-centric warfare (NCW) efforts. Signposts of Chinese efforts in this direction include increased and coordinated blue-water training by the Navy, over-water training by air units, development of long-range unmanned aerial vehicles, and development or purchase of counter-space technologies. The PLA’s concentration on the use of conventional weapons against U.S. vulnerabilities indicates that the U.S. military must prepare for the PLA to seize the initiative, requiring increased attention to defensive training and technologies such as antisubmarine warfare and passive and active air base defenses.

Option Two: Subversion, Sabotage, and Information Operations

The second potential response option is based on a belief among Chinese strategists that information operations can successfully attack the two critical centers of gravity in a Taiwan scenario: the will of the Taiwanese people and U.S. military intervention. Beijing’s strategy to manipulate the national psychology of the populace and leadership on Taiwan involves the full spectrum of information operations, including psychological operations, special operations, computer network operations, and intelligence operations. The goal of these efforts is to shake the widely perceived psychological fragility of the populace, causing the government to prematurely capitulate to political negotiations with the mainland. Signposts of growing PLA interest in these strategies include evidence of physical and virtual probing of Taiwanese infrastructure, greater use of regional media to send psychological-operation messages to Taiwan, and more frequent compromises of Taiwan intelligence networks on the mainland. The primary implication for the United States is that the Taiwanese side may buckle quickly, perhaps even before U.S. forces arrive, and thus any operational planning should prepare for the United States to fight alone or with only limited and possibly compromised assistance from Taiwan forces.

In terms of using information operations to affect U.S. military intervention, the use of computer network attack (CNA) to degrade or even delay a deployment of forces to Taiwan offers an attractive asymmetric strategy. Some Chinese have concluded from studies of
Desert Storm and Operation Iraqi Freedom that logistics and mobilization are a weakness of U.S. operations, particularly given their dependence on precisely coordinated transportation, communications, and logistics networks, many of which are sensitive but unclassified networks like the NIPRNET (Non-Secure Internet Protocol Router Network). PLA writings suggest that a successful CNA against these systems could have a detrimental impact on U.S. logistics support to operations and delay U.S. intervention long enough to allow the information operations and other coercion against Taiwan to have the desired effect. The advantages of this strategy are twofold: (1) it is available to the PLA in the near term, and (2) it has a reasonable level of deniability. The primary signpost of preparation for this strategy is increased evidence of probing against the NIPRNET from China-origin networks, although the nature of CNA makes attribution highly challenging. The principal implication for U.S. forces is to recognize the vulnerability of logistics and other deployment systems and to train and exercise publicly without use of the networks to diminish their value (perceived and actual) as a target.

**Option Three: Missile-Centric Strategies**
The third potential response is a missile-centric force that would seek to present an overwhelming short-range missile threat to Taiwan, improve China’s offensive capabilities against U.S. bases in the Asia-Pacific, and give the PLA the capability to launch conventional strikes against U.S. strategic targets with conventionally armed ballistic and cruise missiles. This approach allows the Chinese to bring the fight to the full-strategic depth of the United States by attacking weak points in the enemy rear, denies the U.S. military the ability to use regional bases (Guam, for example) as sanctuaries, changes the dynamics in the early stages of a conflict, and provides an effective response to strategic attacks by American conventional forces. If the Chinese were to produce a missile-centric force designed as a counter-transformational capability, the signposts that might provide hints as to the direction of development, deployment and employment issues would include: declaratory statements, doctrinal developments, shifts in resource allocation, research and development interests, deployment
patterns and numbers, testing, and exercises. Building an effective deep attack capability is challenging from a technical standpoint, especially if the United States attempts to develop alternate strategies or force employment concepts to operate while under attack. In the end, however, the United States will be obliged to develop an approach for dealing with the threat and will need to consider a range of responses that could entail limiting its own actions, altering the basic strategy for conflict to render irrelevant the capabilities of the missile forces, employing a host of protective measures throughout its full strategic depth, or employing escalation dominance.

**Option Four: Chinese Network-Centric Warfare**
The fourth potential response is a Chinese version of NCW, which is likely to reflect China’s strengths in operational security, operational control, surprise/stratagems, massed artillery, and rocketry. To this end, the Chinese are therefore unlikely to duplicate U.S. air power or develop doctrine on untethered operations. The major operational challenge for China vis-à-vis the United States is defeating U.S. air power, notably finding and targeting carrier battle groups (land-based air power can be countered by massed missile attacks on air bases). Massed sensors and weapons may be one way to solve this problem, but weaknesses in systems integration, logistics, and concerns over operational control of remote devices with autonomous intelligence may impede pursuit of this strategy. Signposts of a Chinese effort to develop network-centric strategies include a ramp-up in percentage of expenditures devoted to C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance), writings by PLA strategists and doctrinal experts espousing the idea, greater interest and resources directed toward exploiting the information technology manufacturing base, the use of smaller units in training and exercises that seem from the outside to be unusually well coordinated, and the use and coordination of an unusual number of flying objects over a large battlefield. The challenges of correctly identifying and classifying a Chinese network-centric modernization are significant, including the difficulty of signals intelligence collection against modern, encrypted, and largely fiber-optic communications.
systems and the smaller, component-based nature of network-centric systems.

**Implications for DoD Planning, Force Transformation, and China Analysis**

**Implications for DoD Planning and Force Transformation**
Unlike U.S. adversaries’ plans in U.S. military conflicts following the end of the Cold War, China’s plans have called for its forces to conduct offensive operations to seize the initiative in any Taiwan scenario, with the goal of delivering a “decisive blow” to both Taiwan and any foreign military intervention on Taiwan’s behalf. As a result, DoD planning may need to focus more on defensive measures, particularly those related to protecting U.S. forward basing, satellites, information systems, and expeditionary assets, such as aircraft carriers. These efforts go well beyond simply a validation of the need for missile defense, requiring a significant reorientation of force posture, deployments, technology acquisition, and training.

What if the Chinese adopt NCW? If they do, how should the United States respond? Regardless of whether they adopt our brand of NCW, it is likely that they will enhance their investment in sensors and precision weapons. The upshot of that development is straightforward. If our NCW makes the battlefield visible to us, theirs is likely to make the battlefield visible to them. In particular, that means our own forces will be more visible to them and thus more likely to be targets. The more visible the battlefield, and the more that visibility is tantamount to destruction, the more difficult it will be to go to war with platforms. The U.S. response to that may be to accelerate certain aspects of its own NCW evolution—toward deploying sensors and weapons from a distance, or if it must operate closely, to do so either with a reduced signature (i.e., stealth) or with so much signature as to be disorienting. In either case, exposure times must be short. Both sides, China and the United States, may pursue the informatization of warfare to its logical conclusion. Victory, if not inherent in the balance of forces or unique attributes of geography,
falls to whoever has the best combination of surprise, error control, fortune, and highly trained people. Ironically, a confrontation between two technologically advanced, network-centric militaries will likely reduce the importance of technology in favor of people and their ability to make rapid but accurate decisions with incomplete or overwhelming amounts of information. In such a contest, volunteer military personnel drawn from an open, educated society like that of the United States would appear to have the advantage over a stove-piped military embedded in an authoritarian state, but the blinding pace of social, cultural, and technological change in China strongly suggests that this conclusion will not always remain true.

Implications for China Analysis
The centrality of Taiwan for China’s leaders makes it highly unlikely that U.S. transformation would dissuade China from devoting resources to development of capabilities it regards as essential to deter or prevent Taiwan from moving further toward formal independence (although China may be dissuaded from broader competition for military influence in the Asia-Pacific). As a result, new approaches are needed to acquire information on Chinese responses to U.S. transformation that will facilitate analysis of Chinese capabilities and intentions. Efforts require that priority be given to the recruitment and training of subject-matter experts with advanced language qualifications.