1

Keeping the Edge

Managing Defense for the Future

ASHTON B. CARTER

Most advice on national security affairs focuses on the *ends* of our national security and foreign policy: on setting priorities among the almost numberless tasks that could be taken up by the world's leading power. Will China and Russia pose future threats, or can they be cooperatively integrated into the international system? Is preparing to fight two major theater wars still the appropriate organizing principle for overall forces and budgets? Is the defense budget large enough overall? When and how should the United States participate in peacekeeping and conflict prevention?

These are important debates, but equal attention and action should be directed at the *means* to implement policy priorities: the agencies and programs of the executive branch. There is mounting evidence that the national security establishment is deficient not so much in deciding what to do as in having the means to get it done. This book, prepared by a bipartisan Core Group of authors and advisers, therefore takes a different approach: it addresses the organization and management of the national security establishment, and especially the Department of Defense, to *implement* the policies the nation's leaders choose for it, to *manage* the programs they direct, and to *adapt* to a changing world.

When it comes to the means our nation now has to implement security policy, the situation is mixed. Our military is unmatched by any conceivable combination of foes, and will remain so well into the future under a wide range of assumptions about future trends. With its huge and growing economy, the United States can in principle devote economic resources to the pursuit of its foreign interests that are vast

even in comparison to the scale of major world problems. We are constrained mainly by a lack of consensus about our role in the world. The powerful trends shaping the twenty-first century — globalization, commercialization, the information revolution — are so compatible with U.S. culture and interests that much of the world confuses them with "Americanization." Playing such a fundamentally strong international hand is far preferable to playing a weak hand.

But when we consider the state of the foreign affairs instruments of the executive branch of the U.S. government, we find that our cards are much weaker than they should be. Far less recognized than the perplexities of choice among the ends of U.S. strategy is the depletion of means. The military that brought victory in DESERT STORM, peace in the Balkans, and respect from friend and foe since the end of the Cold War is an exception in our government: the "point of the spear" is sharp and hard, but much of the rest of the national security establishment is deficient or broken.

Throughout the national security establishment there are systemic managerial and organizational problems. For example, critical post–Cold War national security missions — counter-proliferation, counter-terrorism and homeland defense, computer network defense, information operations, biowarfare defense, threat reduction and arms control, coalition warfare, peacekeeping and post-peacekeeping civil reconstruction, and preventive defense — are being accomplished in *ad hoc* fashion by unwieldy combinations of departments and agencies designed a half century ago for a different world. Too many of these new missions are institutionally "homeless": nowhere are clear authority, adequate resources, and appropriate accountability brought together in a clear managerial focus. Although it is widely understood and accepted that we need the means to accomplish the homeless missions — even if debate continues about when and how to do so — at this time the government is not well organized or managed to accomplish them when we choose to do so.

Critical underpinnings of quality performance in governmental functions are eroding. Top-flight people refuse to serve at all levels of government, from high political posts to the civilian and uniformed services, because the conditions of public service are often demeaning and frustrating. Quality people already in government are leaving, and those who remain often feel that their potential for creative leadership is stifled. Regulatory systems for auditing and accounting,

contracting for weapons and services, export controls, and security classification and background checks today show all the signs of bureaucratic decline, applying an accumulation of rules rather than logic to their assigned missions. Policymakers attempting to oversee these systems often find themselves lost in the thicket of rules and give up trying to exercise direction over these critical functions, leaving the field to political fringes and interest groups.

The U.S. capability for joint military operations has not yet been affected by the pervasive managerial and organizational problems of the international affairs establishment. But even in the Department of Defense, a disturbing picture emerges if one looks at the "tail" instead of the "tooth." The infrastructure of bases and depots has not been reduced nearly as much as the force itself in the past decade, resulting in a large tail-to-tooth ratio and billions of wasted defense dollars. DOD acquisition personnel are still burdened with the Federal Acquisition Regulations, as thick as a big-city telephone book. Forces that are meant to fight jointly are still equipped, sometimes incompatibly, by the separate services and defense agencies. The research and industrial base upon which the distinctive American way of providing for security relies — with high technology that foes cannot match — is being transformed by the forces of commercialization and globalization, but DOD persists in many old habits regarding research and development (R&D), the industrial base, and acquisition. As a consequence, the U.S. military is not fully exploiting or even staying abreast of the information revolution. It is scarcely even in the game when it comes to biotechnology, whose implications for human conflict may be even more profound than those of information technology. The defense industry upon which the technological edge ultimately depends is suffering from difficulties raising capital and the flight of many of its talented engineers and managers. Trans-Atlantic defense industry cooperation, important for efficiency and NATO cohesion, presents a set of unsolved problems for all allied governments.

Despite these problems of DOD organization and management, the U.S. military is still far better than any other military anywhere in the world. But the government owes the public a military that is not just better than all the others, but one that is as good as the money we are spending can make it. By that standard, we will fall short if the continuing absence of imminent and galvanizing Cold War–scale tradi-

tional military threat causes us to be complacent and to avoid undertaking politically difficult reforms. Eventually these deficiencies will begin to affect the point of the spear itself. For these reasons and more, we must attend to means as well as ends in our national security strategy: to the "threat within" as well as to external threats. President Eisenhower said that the right system does not guarantee success, but the wrong system guarantees failure. A defective system will suck the leadership into its cracks and fissures, wasting their time as they seek to manage dysfunction rather than making critical decisions.

The transition to a new administration provides an opportunity to undertake change to counter the threat within, an opportunity that comes only every four or eight years. Early in a presidential transition, civilian jobs are not yet filled with officials who, once entrenched, might resist a change in their functions. The new administration has not yet settled into a pattern of making do with the system it inherited. Politically, the Congress and the voters are expecting change. Thus the time is right to address these chronic management issues.

Many of the changes we prescribe do not require creating new bureaucracies or eliminating old ones, although sometimes that may be needed. We do not, for example, recommend creation or elimination of cabinet departments or other large-scale structural changes in the executive branch agencies or congressional committees. But management values, incentives, processes, and procedures must change even if the United States keeps the basic organizational structure — the cabinet departments and National Security Council established after World War II, the four armed services, and the constellation of regional and functional Commanders-in-Chief (CINCs) in DOD. Thus our recommendations deal also with processes of analysis, decision, interagency coordination, and execution; with retaining and encouraging quality people, uniformed and civilian; and with incentives, rewards, and accountability.

We recommend evolutionary change where possible. Progressive paths to implementation avoid the kind of turmoil that could disrupt what is working as we try to fix what is not. Evolutionary change can also avoid opposition. Nevertheless, implementing the recommendations in this book will be a formidable task. Government organization and management, unlike policy formulation, is largely the stuff of low politics, not high politics. Resistance comes from inertia and

complacency, from ingrained habits and entrenched interests and bureaucracies. Overcoming this type of resistance is sometimes harder than winning a spirited national debate on a major policy issue. Success will require sustained attention and support from the President and his top national security officials, and close cooperation with Congress, which must lend support and in some cases enact legislation to effect these recommendations.

The historical record of managerial and organizational reform is mixed. The broad outlines of the national security establishment were defined just after World War II and have changed little since. But there have been instances of sweeping and effective change. The All Volunteer Force successfully replaced conscription. The Goldwater-Nichols Act strengthened joint warfighting capabilities and the chain of command, where previously the armed services had sometimes seemed to be planning and waging separate campaigns. But elsewhere change has progressed, if at all, in fits and starts, as in efforts to close unneeded bases, make export controls more effective, and reform the Pentagon's cumbersome acquisition system.

The recommendations in this book reflect three kinds of need for organizational and managerial adaptation. The first need is maintaining the U.S. edge in areas where we are currently unrivaled but where future trends challenge our ability to preserve this lead. Examples include joint warfighting, military technology, application of information technology to national security, a near-monopoly in national intelligence, and keeping quality personnel serving in the armed services. The recommendations we make in these areas are intended to preserve the American edge under the new circumstances of the early twenty-first century.

The second type of recommendations focuses on the new era's demands for new capabilities to address post–Cold War priorities, such as counter-proliferation, counter-terrorism and homeland defense, computer network defense, information warfare, biowarfare defense, coalition warfare, threat reduction and arms control, peacekeeping and post-peacekeeping civil reconstruction, and preventive defense.

The third type of recommendations addresses chronic management problems that have long resisted change: closing unneeded facilities, outsourcing non-military functions to the commercial sector, improv-

ing the quality of DOD's civilian workforce, improving acquisition and logistics practices, and updating export controls and security practices.

Our focus is largely, though not exclusively, on the Department of Defense and the defense function of government. But organizational and managerial problems of the kind this book identifies are at least as severe in other parts of the national security establishment. We therefore believe that comparable remedial efforts are required in the Department of State, the intelligence community, and the Department of Energy.

The rest of this chapter summarizes this volume's key recommendations for action, highlighting the deficiencies in organization and management that prompted the Preventive Defense Project to undertake its study.

Preserving Key Strengths Under New Conditions

The recommendations under this rubric seek to preserve key strengths in the face of changing geopolitical, technological, and market conditions.

TAKING THE NEXT STEP IN JOINTNESS

The so-called Goldwater-Nichols reforms of 1986 were intended to insure that U.S. forces fought "jointly" rather than in separate Army, Navy, and Air Force campaigns. They gave Unified Commanders-in-Chief (CINCs) clear authority for joint operations, a strengthened Chairman of the Joint Chiefs of Staff to advise the President, and required joint assignments for officers to reach flag rank. They assigned organizing, training, and equipping the forces to the separate armed services as their principal mission under Title X of the U.S. Code. While operations are "joint," therefore, forces are still acquired severally.

Goldwater-Nichols has been a great success by almost any measure and account. But it did not answer the question of how joint forces could truly be produced from a non-joint acquisition system.

One option, which we reject, would create a truly joint acquisition process at the expense of the services' Title X authorities. This option would have the theoretical advantage of giving the power to configure and buy joint forces to their ultimate "customer," the warfighting CINCs. However, this option would weaken the services, which are proud, living institutions of which there are far too few in our govern-

ment. It would undermine their proven ability to provide the best land, naval, air, and amphibious forces in the world. In addition, transferring responsibility for requirements, budgets, or acquisition to the joint CINCs would divert their attention from their principal tasks of maintaining alliance and other U.S. military relations in their areas of responsibility, planning for regional contingencies, and commanding operations. The CINCs have no staffs specialized in acquisition. The result of shifting most acquisition authority to the regional CINCs would be to weaken, not strengthen, program execution.

A second option would be to maintain the current system as the best balance between the demonstrated expertise of the services and the need for jointness. But maintaining the status quo is not a true balance because it perpetuates three critical managerial deficiencies that impede true jointness. First, the mechanism to ensure interoperability among forces and systems acquired by the separate services is weak. Second, a purely services-run acquisition system provides no clear mechanism to make difficult trade-offs among service programs and budgets. For example, is a given mission best executed by Army helicopters or by Air Force planes? Such issues are currently either unresolved or left to the most senior DOD leadership at the last minute in the budget cycle. Third, some key capabilities such as reconnaissance, surveillance, and information systems and logistics are inherently joint, and there is no strong voice in the current system for them. These deficiencies are too serious to leave uncorrected.

A third, middle-ground option, described in Chapter 2, offers the best chance for both sustaining the acquisition excellence of the services and giving appropriate voice to joint considerations in the acquisition system. Rather than involving all the CINCs in the acquisition process, the compromise is to give a single CINC — the Joint Forces Command (JFCOM) CINC —the capability as well as the authority to inject joint thinking into the acquisition process on behalf of the Chairman of the Joint Chiefs of Staff and all the other CINCs. This is, in fact, the option being pursued by the Department of Defense, but JFCOM has not yet been given the tools to do the job. Realizing the potential of this option requires four additional steps: first, CINCJFCOM should lead in preparing for the Chairman a broad roadmap, updated annually, for developing truly joint forces. Second, JFCOM should be given the personnel and resources in its Norfolk,

Virginia, headquarters to take on its new acquisition responsibilities. These should include some direct authority over resources devoted to inherently joint capabilities. Third, as the "joint and future forces CINC," the person chosen to be JFCOM commander should be a senior CINC, appointed from among those who have experience as CINCs or service chiefs or vice-chiefs. Fourth, CINCJFCOM should become a member of DOD's key decision-making bodies on acquisition matters: the Joint Requirements Oversight Council (JROC) and the Defense Resources Board (DRB).

EXPLOITING THE INTERNET REVOLUTION

The most important inherently joint military capability resides in command, control, communications, computers, intelligence, reconnaissance, surveillance (C4ISR in the current form of this lengthening acronym). But while the U.S. military is far ahead of any other military in exploiting the information revolution, the pace of commercial technological advance in this field is far faster than DOD's cumbersome requirements and acquisition procedures. Without change in DOD's practices, the information revolution that began in DOD will pass the Department by. This is a pervasive problem, and Chapter 3 recommends attacking it first where it counts most, in joint command and control systems that are used in contingency operations. The time it takes to "glue together" separate service command and control systems is too often incompatible with the required military action, resulting in lost military advantage. We build on the previous recommendation, to strengthen JFCOM's role in joint requirements, by urging that JFCOM undertake a well funded activity to develop a joint command and control system for contingency operations based on continuous exercising and experimentation ("expercising"). A Joint Blueprint Office should develop systems engineering architectural guidelines and lead to the acquisition of a common command and control infrastructure (the Global Information Grid). To accomplish this task, however, JFCOM will require additional resources and dedicated support from scientists and engineers outside the government, in much the way that both for-profit industry and Federally Funded Research and Development Centers (FFRDCs) supported early U.S. air defense and space programs.

A JFCOM activity of this type will make it easier to insert cutting-edge information technology (IT) into joint command and control,

where it is most needed. However, the IT challenge is broader: it pervades DOD systems, yet defense systems no longer occupy the cutting edge in information technology. This place has passed from defense to commercial companies. It was DOD that pioneered the microchip, massive parallel processing, the Internet, software engineering techniques, and other information technologies, but these are now spearheaded by the well-financed commercial e-revolution. In the future, DOD will be a consumer rather than an originator of technology in all but niche areas of this sector.

Given this fact, Chapter 6 recommends steps to keep DOD at the forefront of the IT revolution. It is important for DOD to continue to fund R&D in this field, for three reasons. First, much commercial IT R&D is directed at near-term advances rather than the kinds of breakthroughs that have the most to contribute to national security. There, the government still has a role to play: sponsoring high-risk, high-payoff technology for defense and other national purposes. Second, only by being a participant in the ongoing information revolution can DOD remain a smart buyer of commercial technology. Finally, DOD has unique needs for research and development of new weapons systems, sensors, and other military-specific technology. In addition, DOD procurement practices, which have historically emphasized periodic block upgrades, have become obsolete: commercial practice emphasizes continuous, incremental upgrades and open-system architectures, and DOD's IT buying practices should adopt such practices. Finally, the uniformed and civilian workforces of DOD would benefit from the specification of new career paths for recruitment, training, and retention of technically competent information specialists (a so-called "Cyber Corps").

PRESERVING THE TECHNOLOGICAL EDGE

Information technology is an instance of wider changes in the technology base supporting defense. These changes have serious implications for a core pillar of America's defense strategy: the technological edge on which our "offset strategy" is based. The offset strategy was developed during the Cold War, when the United States decided it could not match the Warsaw Pact tank for tank or soldier for soldier. Instead, superior American technology would "offset" superior opposing numbers. The offset strategy secured deterrence of numerically superior forces and forced the Soviet Union to bankrupt

itself in the pursuit of military technology it could not easily obtain from the West. The fruits of the offset strategy were demonstrated in DESERT STORM, where reconnaissance satellites, stealth aircraft, precision weapons, and other technologies unmatched by any other military made short work of Iraq's Soviet-equipped army. The technological edge on which the offset strategy depends remains the distinctive American way of defense, now applied to new post–Cold War missions.

But a challenge now looms to the preservation of America's technological edge from trends in the industrial and technology base. This base, once largely the creation of Department of Defense spending and almost exclusively American, is commercializing — the technology of central importance to national security increasingly originates in commercial rather than defense companies, without DOD sponsorship and outside its control — and it is also globalizing — leading technology companies are increasingly global rather than purely American in their outlook, ownership, workforce, and markets.

During the Cold War, defense technology originated in a defense technology base that was embedded in defense companies that resided in the United States, and that had DOD as their main market. In the future, defense technology will originate in a commercial technology base embedded in global commercial companies for which defense is but a niche market. In the past, military advantage was conferred by national possession of defense-unique leap-ahead technology that potential opponents could not get. In the future, military advantage will be obtained by adopting mostly commercial technology into defense systems faster than potential opponents who have access to most of the same technology.

Related to commercialization is *marketization* of the defense industry: defense companies must justify themselves to investors by the same standards of profit and cash flow as commercial companies. More and more, market forces are drawing capital away from defense firms and affecting the ability of these companies to be innovative and to attract talented personnel. The total market capitalization of the major defense firms today is about half that of Wal-Mart, just a quarter that of Microsoft. The list of premier U.S. industrial companies that have exited the defense market reads like a Who's Who of industrial America: IBM, Texas Instruments, Ford, Chrysler, GE, Westinghouse, and so on. Meanwhile the "new economy" companies

are wholly absorbed in the pursuit of rapidly growing commercial markets rather than the slowly growing defense market.

Chapter 6 recommends two types of adaptation to help DOD preserve the technological edge in the face of commercialization and globalization. The first requirement is for DOD to align its own practices more closely with the market forces operating both on commercial companies that increasingly supply vital technology for defense and on defense companies that integrate technology into military systems. What is needed is not an "industrial policy" that props up weak defense companies and accentuates the isolation of the defense industry, but an approach that works with, rather than against, market forces, leveraging commercialization to secure the needs of defense. Acquisition and contracting policies that reward industry for delivering value as opposed to monitoring cost, as described in Chapter 7, are an important step in that direction. Chapter 6 describes three additional actions to align market incentives with DOD's needs. First, DOD should reward the defense industry when it follows sound business practices in pursuit of innovation and efficiency, including sharing savings from cost-cutting, facility closings, and other efficiencies between government and industry; allowing higher profits when industry performs successfully in terms of cost, schedule, and performance; expanding use of multi-year contracts with the approval of Congress; and adjusting "progress payment" practices for both contractors and their subcontractors. Second, DOD should encourage second- and third-tier companies serving both defense and commercial marketplaces to remain in the defense business. Third, DOD should encourage robust trans-Atlantic defense industry linkages, which will reinforce alliance solidarity (as described in Chapter 9) and, over the long run, will provide classic free-trade efficiencies to all allied militaries.

The second means to turn commercialization and globalization to DOD's advantage is to assure that the U.S. military remains the world's fastest adapter and adopter of commercial technology into defense systems. Potential opponents will also have access to much state-of-the-art technology since they can purchase it on the open global market. DOD must "run faster" than others, rapidly incorporating new technology from the growing global base into defense systems (and experimenting with concomitant changes in tactics and doctrine), rather than relying almost exclusively on its own spon-

sored R&D as it did during the Cold War. A key step in this direction is to encourage DOD to use commercial buying practices and commercial systems in defense procurement. If DOD persists in its idiosyncratic buying methods and cumbersome contracting procedures, it will always be a generation behind commercial practice, and many commercial companies will refuse to accept defense contracts. DOD must also continue to stimulate R&D on defense problems through direct contracting, prototypes and demonstrations, and especially by making R&D investments by defense companies as profitable as production so companies will have incentives to innovate.

PRESERVING THE INTELLIGENCE EDGE

National intelligence is another long-standing American strength in international affairs, amounting to a virtual monopoly on key security information of importance to the world community, especially in areas such as proliferation, crime, and terrorism. The U.S. national intelligence system was conceived after World War II as a unified effort combining secrets and openly derived information in integrated national analyses; supporting DOD's military operations as well as a broad range of needs from other agencies; and conceiving of engineering, collection, analysis, and dissemination as a single, unified effort. This unity of effort was not always achieved, but the management principle was that of "central intelligence."

Today's environment has some features that challenge this principle. More information and expertise reside outside of government than ever before. Commercial firms now collect information such as satellite imagery previously collected only by government. Military command and control and other governmental management functions are shifting to non-hierarchical models that leave both discretion and the need for intelligence to lower echelons. The pace of warfare and of all international events is quicker. The hierarchical unified system of the past is ill-suited to these changes. But other trends continue to favor the central intelligence model. Technology makes all information, whether signals intelligence, pictures, or open-source information, a common stream of electronic bytes. Wide-bandwidth communications permit rapid and widespread dissemination of information to all echelons simultaneously.

Chapter 4 and Chapter 10 argue that the model of central intelligence can still serve the nation best — indeed, can preserve intelli-

gence as a key national security edge — with adaptations to network support for military operations (also described in Chapter 3), to expand international partnerships to avoid creating competing centers of intelligence expertise elsewhere around the world, to tap into expertise outside of the intelligence community, to manage collection and dissemination of technical intelligence in a common manner, and to embed more analytic capability at lower echelons.

KEEPING QUALITY PEOPLE IN UNIFORM

The All Volunteer Force has been a great success, largely through the DOD's commitment to quality and the continued application of sound management practices. Nevertheless, there are areas where improvements are needed in order to assure equal quality in the future. Military compensation policy has been subject to spasmodic across-the-board pay raises in response to political pressure. Chapter 8 argues that such blanket increases miss an opportunity for more effective management of the overall compensation system to give added incentives to the categories of military personnel we need most and to take account of the labor markets in which the military competes. A similar systemic approach is needed to "quality of life" improvements. Here DOD too often takes the approach of increasing government provision of amenities such as housing, a vestige of the nineteenth-century military practice of providing everything a garrisoned soldier needed through government supply bureaucracies. Today, however, quality of life can often best be assured by giving service members the resources to purchase amenities directly in the local economy.

Another important dimension of military personnel policy treated in Chapter 8 is adapting to demographic change. For example, the military's recruiting policies and career paths tend to force young people to choose between college and military service, yet two-thirds of American high school graduates now attend college. Thus recruiters are limited to a decreasing pool of high-schoolers who do not choose to go to college immediately. Competing in this market will require DOD to make such changes as opening up more career paths for promising enlisted personnel to move to warrant or commissioned status, and making college education compatible with a military career. Other demographic changes will also require adaptation in the personnel policies of DOD: the fact that Hispanics are a grow-

ing fraction of the U.S. population but have lower graduation rates than some other groups, the increase of two-career families, and so on. Personnel policies must go beyond a mixture of outdated bureaucratic procedures and bursts of "political correctness," to manage the human resources of defense to the standards prevalent in large civilian organizations.

Organizing to Accomplish the New Era's New Missions

The second type of recommendations we offer are focused on new missions of the post–Cold War era, which both call for new responses from DOD and, increasingly, cut across departments of the government, requiring a unified interagency approach.

NEW ISSUES THAT CUT ACROSS DEPARTMENTS AND AGENCIES

A key characteristic of the new missions for defense in the post–Cold War era — counter-proliferation, counter-terrorism and homeland defense, computer network defense, information operations, biowarfare defense, threat reduction and arms control, coalition warfare, peacekeeping and post-peacekeeping civil reconstruction, and preventive defense — is that they do not respect the boundaries between agencies and departments of government and between committees of Congress. Our departments and agencies were created in 1947–49 when there were sharper divides between war and peace, domestic and foreign threats, and security and economic issues than there are today. The National Security Council (NSC) is an effective means for policy coordination, but it has little capability for program coordination. For this reason, and because the Office of Management and Budget (OMB) is traditionally not strong in the security field, the White House has little influence in the allocation of resources to deal with a growing number of international problems that are interagency in nature. The current NSC has little ability to construct a government-wide program of technology, acquisition, and institution-building to correspond to its carefully coordinated policy, and few NSC staff have any programmatic experience, while cabinet agencies and congressional committees jealously guard their funding authorities. Yet if we are going to retain the current agency structure and at the same time deal with cross-cutting priority issues such as

proliferation and catastrophic terrorism, we will need to have interagency program coordination at the White House.

A variety of solutions to this problem can be considered: a new "super department" of national security, various "czars" at the White House, a new staff organization for the President, new budget categories, and so on. After carefully considering such options, Chapter 10 opts for retaining the National Security Council structure for policy coordination, but strengthening its capacity for program coordination, in concert with OMB. Under this mechanism, the NSC would devise multi-year, multi-agency program plans for key post–Cold War missions, and the Office of Management and Budget would assure appropriate funding within the agencies.

COUNTER-TERRORISM AND HOMELAND DEFENSE

An important example of the need for program coordination is the creation of a government-wide response to the danger of catastrophic terrorism involving weapons of mass destruction, cyber threats, disruption of critical infrastructures upon which complex modern society depends, or attacks upon the institutions of government themselves. This is an issue that cuts across the boundary between foreign and domestic threats — a boundary deeply carved in American government and cherished by its citizens. The specter of attack on their homeland is a new one in Americans' recent experience. In this century America's wars have been far away. Only after the Soviet Union exploded the atomic bomb in 1949 was a direct external threat of destruction posed to the American homeland. The impact on American thinking and institutions was immediate and profound. A huge and sophisticated strategic nuclear deterrent capable of retaliating against the Soviet homeland was built. Vast programs of continental air and missile defense were inaugurated. Civil defense shelters were built and drills conducted for schoolchildren. Think-tanks such as the RAND Corporation were founded by government to ponder the new security dilemma. Suspected spies and Soviet "sympathizers" were hunted.

It is likely that an incident of catastrophic terrorism on the U.S. homeland would spark concern and effort on a comparable scale. It is easy to see how the concern could escalate to hysteria, and how actions taken in the angry aftermath of a destructive event could be counterproductive and corrosive of civil liberties. The aftermath of

homeland attack is therefore as much to be feared as the attack itself. It is much better if government begins to organize for this future threat *now*, while considered judgments can be made about how best to protect the homeland and how to trade off protection against other social values. Chapters 5 and 10 address this question.

In the past three years, an effort has been made to craft an interagency response to the threat of catastrophic terrorism that bridges all the national security agencies and the law enforcement communities. "Lead agency" responsibilities were assigned to the Department of Justice and the Federal Bureau of Investigation, the Federal Emergency Management Agency, and the State Department to take charge in various circumstances where their historic charters and authorities make a lead role natural and appropriate. This policy was coordinated successfully at the White House, and it appears to be acceptable to all agencies. However, for the most part the agencies assigned lead roles have little existing capability and few or no new resources to carry out their assigned roles, which remain unfunded mandates. DOD, the Department of Energy, and the intelligence community, although they are appropriately not assigned lead roles, have most of the existing capabilities and the best base from which to build new technological and other capabilities. Even taking all the agencies together, current capabilities and plans for responding to such a fearsome event are not adequate. A multi-year, multi-agency program plan to build such a national capability over time is needed, and would provide a prime example of NSC program coordination.

ASYMMETRIC WARFARE, ESPECIALLY BIOWARFARE DEFENSE

Saddam Hussein's military in 1991 was in many ways a miniature version of the Soviet army in its equipment, doctrine, and tactics. This was precisely the type of threat against which the U.S. military and its coalition partners drawn from NATO had been practicing for decades. Faced with the hammer of the U.S. military, Iraq configured itself as a nail. The outcome was never in doubt. Slobodan Milosevic's Serb forces were similarly Soviet-like, as are Kim Jong-Il's North Korean conventional forces. Future opponents, however, observing the lesson of the 1990s, will make no attempt to counter the United States symmetrically. Instead, they will resort to asymmetric means: exploiting vulnerabilities in our elaborate but fragile C4ISR systems; using weapons of mass destruction; or bringing destruction

to the U.S. homeland through catastrophic terrorism. Much of the DOD's spending goes to improving its capability for contending with symmetric foes quickly and with minimal casualties; too little goes to countering asymmetric threats.

Chapter 5 describes some specific steps to prepare better to counter asymmetric threats. In particular, DOD should make strong contributions to the interagency counter-terrorism and counter-proliferation programs recommended above. DOD should also develop a technology base in biowarfare defense (BWD) that is as strong as its base in nuclear proliferation. DOD and DOE have strong laboratories with thousands of personnel skilled in nuclear technology. But the national security community has few experts in the field of biotechnology, neither within its uniformed or civilian ranks nor in its affiliated laboratories and contractors. Biotechnology and pharmaceutical companies frequently decline to participate in BWD programs for fear of being "tainted" by defense work or because of the cumbersome contracting and accounting procedures required by the Pentagon. Yet the biotechnology revolution will have implications for security that will probably exceed those of the nuclear and information revolutions that preceded it. DOD will need to increase funding in the Defense Advanced Research Projects Agency (DARPA), U.S. Army Medical Research Institute of Infectious Disease (USAMRIID), and the Defense Threat Reduction Agency (DTRA) for biotechnology research, but this will not be enough. Government employment practices and the attractive private-sector employment opportunities available to biotechnologists mean DOD has little chance of retaining in-house expertise in this field. A university-affiliated government-owned laboratory (akin to the nuclear laboratories of the DOE) should be founded to give DOD a foothold in the BWD technology field.

ORGANIZE TO DEAL WITH INFORMATION WARFARE

Information technology is not only an enabler of traditional military operations, it is a weapon in its own right. Chapter 3 suggests that DOD needs to organize both offense (computer network attack, or CNA) and defense (CND) to give policy order to this area of importance to future international security. CNA's balkanized and overclassified activities need to be brought together in a functional joint command where the Secretary of Defense and the President can exer-

cise policy oversight. CINCSPACE is the appropriate choice within DOD (supported by the National Security Agency as "force provider"), and CINCSPACE needs to be given the resources to do the job. For CND, the government shares the interests of private banking, e-commerce, and other businesses and of ordinary citizens in privacy and security for networks. A publicly funded but privately operated National Information Assurance Institute should be founded at a major research university, with initial funding from DOD.

BRIDGE THE GAP BETWEEN EUROPEAN AND U.S. MILITARY CAPABILITIES

European nations are far behind the United States in every dimension of modern military proficiency. The process of military reform in Europe will take many years, and it is not practical to "close the gap" between their militaries and ours in its entirety. However, as described in Chapter 9, it should be possible for one NATO Combined Joint Task Force (CJTF) to be equipped and trained to operate at or near U.S. standards and to interoperate fully with U.S. forces. If successful, this capability within NATO, though small, would have significant political effect, would shift some of the burden for small-scale contingencies from the United States to the allies, and would provide a stronger proving ground than European Security and Defense Identity (ESDI) for wider reform of Europe's militaries. The United States should also encourage trans-Atlantic defense industry partnerships.

STRENGTHEN OTHERS' ABILITY TO PERFORM PEACE OPERATIONS

Many Americans would prefer to see the United States attach a lesser priority to peace operations, but such operations must be performed by someone. Chapter 9 recommends a two-part U.S. strategy for dealing with this dilemma. The first part is to strengthen others, including international organizations, to perform certain selected types of peace operations. For example, the United States should appoint a defense advisor to the United Nations. Second, the United States should prepare for a supporting, specialized role emphasizing its areas of comparative advantage relative to other states, international organizations (IOs), and non-governmental organizations (NGOs). Examples would include restoring order in the early period of a peace operation rather than rebuilding institutions of civil society in

the later period, and contributing transport and information systems rather than patrolmen to a policing operation.

IMPROVE THE CONTRIBUTIONS OF DOD'S MILITARY-TO-MILITARY PROGRAMS TO PREVENTIVE DEFENSE

DOD's military-to-military programs begin first and foremost with our key alliances, especially NATO and Japan. But the circle can be widened, as described in Chapter 9, through such programs as the military-to-military activities sponsored by the regional Commanders-in-Chief (CINCs), NATO's Partnership for Peace, and the Department of Defense Regional Centers. In Asia, these programs are a means to "engage" China and, more importantly, provide a U.S.-led mechanism to increase transparency and understanding among militaries in a region without NATO-like security structures. With Russia, military-to-military activities are a means to understand and, at the margin, to influence the attitudes of a key institution in Russia's ongoing revolution. With former Soviet states such as Ukraine and Uzbekistan, these programs are a vital lifeline to the West and provide strategic insurance for them and for the United States against a negative turn in Russia's revolution. These programs are both preventive and protective, and should be fostered.

EXPAND THE SCALE AND SCOPE OF THE NUNN-LUGAR PROGRAM

History has given the United States unique opportunities to reduce the threat of weapons of mass destruction (WMD) through cooperative programs. But Chapter 9 notes that the opportunities available are far more numerous than the current Nunn-Lugar budget can address. New programs are needed in the areas of chemical and biological weapons, assistance to non-Russian states, disposition of fissile materials, and implementation of possible future arms control agreements like START III.

Addressing Long-standing Management Problems

Perhaps most intractable are DOD's long-standing management problems, including management of its civilian personnel, reducing waste due to an excess of infrastructure, bringing government management practices up to the civilian standards characteristic of the

recent economic boom, transforming the logistics system, and developing new ways to protect secrets in a changing world.

A NEW PERSONNEL MANAGEMENT SYSTEM FOR DOD CIVILIANS

The current DOD civil service system is badly in need of reform. It is out of touch with the labor market that supplies its people; it inhibits professional development and innovation by its work force; and it is incapable of responding to the changing needs of the DOD. A new system is needed to attract and retain high quality, innovative people who can implement and manage the new DOD described in this book. Chapter 8 argues that the DOD should manage the new human resources system outside of the civil service system. The new system would be better able to attract the right people because it would have more flexible pay and hiring rules, portable pensions, contracts for limited periods of government service as well as easier entry, exit, and re-entry into the system. It would be more effective because it would include performance-based compensation, interagency rotation, job grade attached to the person rather than the position, and extensive professional training. At the same time it would protect the fundamentals of the civil service system such as the merit system, equal opportunity, and absence of political influence.

REDUCE WASTED INFRASTRUCTURE

Infrastructure — bases, depots, test ranges, and the like — have not been reduced at nearly the rate of the forces since defense budgets peaked in 1985. As recounted in Chapter 7, Congress has ignored the current administration's call for two more rounds of Base Realignment and Closure (BRAC). Orderly, prioritized, and fair reductions require new legislation. The new administration should show its commitment to pursuing these needed economies by introducing a list of base closure candidates and making a commitment to a closure plan that comports with current law. This should drive the key players in both the administration and the Congress to the negotiating table in search of a new BRAC process. At the same time, the new administration should draft a legislative proposal in order to accelerate the inevitably difficult negotiations that will follow.

PURSUE THE REVOLUTION IN BUSINESS AFFAIRS

The current administration is introducing new business process reforms that reflect the principles of the Revolution in Business Affairs (RBA), but progress has been slow. We recommend that the new administration substantially increase the DOD's goals regarding competitive sourcing in order to capture its benefits, including the ability to focus on core competencies, take advantage of private-sector innovation, and obtain large cost savings. The Secretary should declare that the private sector is the preferred provider of goods and services. He should seek relief from the strictures (executive and legislative) of current competitive sourcing rules, and should greatly expand the kinds and types of functions to be assessed for possible outsourcing.

TRANSFORM THE LOGISTICS SYSTEM

Logistics agility is a key to maintaining our fighting edge. The DOD is moving in the right direction in enhancing the performance of its current logistics structures. But the need and promise of fundamental improvements in capability call for more extensive changes. The Secretary of Defense, with support from the President and Congress, should assign the Defense Logistics Agency as another component under the unified command for transportation (TRANSCOM). A National Distribution Center should be established under TRANSCOM, renamed Logistics Command (LOGCOM), and given enhanced staff to ensure that it has the ability to exercise the full range of its responsibilities. The Secretary should also direct CINCLOG to establish standing joint regional logistics commands in direct support of each regional CINC to replace the separate service commands. This should ensure that unity of effort and joint priorities are in place for all military operations, from peace through all stages of hostilities. In order to tailor and reduce the burden of logistics support, OSD should publish and keep current guidelines that set tough standards for size, weight, consumption rates, commonality in support equipment and parts, and other logistics parameters for all deployable pieces of equipment.

PROTECT SECRETS THROUGH AN IMMUNE SYSTEM RATHER THAN A HERMETIC SEAL

The United States must abandon the "hermetic seal" model of denying technology to others by seeking to put an impermeable barrier around the American defense technology base. Globalization and

commercialization trends mean that crucial technology increasingly arises outside this barrier, and cannot be protected in this simple manner. It is also in the U.S. interest to have technology diffuse inward to defense from a globalized, commercialized base, and in these cases the hermetic seal approach would impede DOD from "running faster." Third, the unique sources of military advantage to the United States that will need to be protected will increasingly be systems engineering capability, rather than component or subsystem technologies. The latter will be widely available and increasingly difficult to contain. The U.S. export controls system must focus on unique sources of military advantage rather than technology across the board if it is to be truly effective at slowing the competition. Accompanying this new meaning of "secrets" must be new ways of protecting them. Much technology that is of foreign origin will find its way into U.S. defense systems and must somehow be made trustworthy. Meanwhile new network and compact data storage technologies make "insiders" as dangerous as "outsiders," as is commonly recognized in commercial industry. To deal with all these changes, the export controls and security systems must be capable of identifying and reacting to real security threats rather than applying simplistic and outdated bureaucratic rules. It should operate on analogous principles to the human immune system, which works not by trying to isolate the body from the environment, but by sensing dangers and combating the most dangerous ones selectively.

Chapter 6 recommends steps to make the transition from the hermetic seal to the immune system model. It supports the recent adoption by the U.S. government of a Defense Technology Security Initiative, streamlining and rationalizing export controls administration. It also recommends centralizing all administrative, training, and technical support for export controls licensing (but not policymaking) in a single entity funded jointly by State, Commerce, and Defense; providing the new entity with an automated licensing, intelligence, and enforcement tracking system; and increasing funding for intelligence support to export controls. But more fundamental steps should also be considered, including removing the distinction between munitions and dual-use items for regulatory purposes, widening employment of end-use controls, developing a control approach centered on systems engineering rather than underlying technology, and developing performance metrics common to those used in other

government regulatory systems. In the area of personnel and industrial security policy, the most important steps to implement an immune system approach are to develop policy guidance covering the new threats and ambiguities introduced by technological change: the increased density of storage media (illustrated by the missing hard drives at Los Alamos Laboratory); network security (illustrated by recent widespread computer viruses and the allegations of data transfers by nuclear scientist Wen Ho Lee); and the integrity of software written outside the security boundaries. DOD and other government agencies should also expand their application of commercial techniques of security, privacy, technical monitoring, and human resources management to DOD personnel and industrial security.

Structure of this Volume

This book begins its exploration of ways of keeping the U.S. edge in defense with the "point of the spear," joint military operations. In Chapter 2, John M. Shalikashvili describes the need for evolution in the manner in which readiness, requirements, and logistics — all essential enablers of joint operations — are managed to keep the fighting edge. Chapter 3 by Victor DeMarines deals with two key aspects of the information revolution as it affects national defense: applying new information technology to joint operations, and organizing DOD's response to the fact that information technology is becoming a weapon in its own right. Chapter 4 by Robert Hermann expands the focus on information from warfare to national security as a whole, recommending ways of preserving America's near-monopoly on intelligence critical to international security under post–Cold War conditions. Chapter 5 by Ashton B. Carter and William J. Perry turns from keeping the edge in joint "symmetrical" conflict to developing an edge in asymmetric warfare if potential opponents, faced with a commanding U.S. lead in the former, turn to the latter.

Chapters 6, 7, and 8 deal with key supporting functions upon which success in dealing with future threats — symmetric or asymmetric — ultimately depend. Chapter 6 by Ashton B. Carter argues that the distinctive American technological edge in military affairs rests on a strong industrial and technology base, and urges adaptations to keep the technological edge as this base globalizes and commercializes. Chapter 7 by Michael J. Lippitz, Sean O'Keefe, and John

P. White argues that the business practices of DOD are in many places inefficient and wasteful, and that more resources could be freed for the "point of the spear" if the rest of DOD were better managed. Chapter 8 by David S.C. Chu and John P. White addresses the problem of giving thoughtful management to the most important resource of DOD: the quality of its uniformed and civilian personnel.

Chapters 9 and 10 deal with DOD's linkages to outside organizations with which it must ally to accomplish critical security missions. Chapter 9 by Elizabeth Sherwood-Randall observes that U.S. forces will almost always be operating in concert with allies, other security partners, international organizations, and non-governmental organizations, and that it needs to manage its interfaces with these bodies in a more deliberate manner rather than as an afterthought. Chapter 10 by John M. Deutch, Arnold Kanter, and Brent Scowcroft observes that the key national security challenges in the post–Cold War era cut across Washington's agencies and departments, and that DOD's role and capabilities need to be managed as part of an overall government team under White House direction.

The many recommendations of this book urge change — in many cases fundamental change. Change is never easy, especially in government, where broad consensus is usually a prerequisite. Some recommendations require legislative change, and all require the consent of Congress. Chapter 11 by Judith Miller addresses some of the legal and political considerations involved in implementing this book's recommendations.

Conclusion

The end of the Cold War left the United States with a substantial edge over every other nation in the world in matters of national defense. This volume is dedicated to keeping this edge in the future. While many in the United States and around the world might take the American edge for granted, the group that prepared this volume does not. The challenges to defense organization and management described in these pages are embedded in the practices and traditions of an enormous organization. They are not susceptible to solution by high-level policy decision alone, or by resolution of a policy debate. They are rarely the stuff of national debate. The mandate to make the needed changes we recommend must therefore arise from the natural

insistence by citizens that their government function as well as the rest of the society they see around them, and from their growing awareness that an easy period in which security was inherited is giving way to one in which security will need to be earned. While change will not be easy, the mandate is there if the administration and Congress choose to use it.