5

Countering Asymmetric Threats

ASHTON B. CARTER AND WILLIAM J. PERRY

WITH DAVID AIDEKMAN

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.

The hammer that struck Iraq in Desert Storm was the result of the second post–World War II "revolution in military affairs" (RMA), to use a now-popular phrase. The first revolution began during World War II and centered on the atomic bomb and the ballistic missile for strategic bombardment. The second RMA, dubbed the "offset strategy" because it was begun in the 1970s to offset Soviet numerical superiority in conventional tactical forces, centered on air superiority, dominant intelligence and communications, and precision weapons.[1]

Today the RMA continues, and organizing to exploit it has been the subject of the preceding chapters. The tasks of implementing jointness in procurement, exploiting the information revolution, and improving intelligence support to national security, treated in Chapters 2, 3, and 4, are essential to keeping the U.S. military unmatched by any other military in the world.

[1] For a description of the origins and content of the offset strategy, and its role in DESERT STORM, see William J. Perry, "Desert Storm and Deterrence," *Foreign Affairs*, Vol. 70, No. 4 (Fall 1991).

But we must also bear in mind that in mounting future threats to U.S. national security, opponents are not likely to make the same mistake as Saddam Hussein. Rather than take on the unmatched U.S. military with a symmetric conventional military force, they will seek asymmetric means to chase away or scare away the United States from protecting its interests. They will seek vulnerabilities in the technologically sophisticated, information-intensive, fully joint "system-of-systems" of the offset strategy whose development was described in the preceding chapters. They will employ weapons of mass destruction: chemical, biological, or nuclear. Rather than waiting for the United States to project power to a distant battleground; they will seek to bring destruction to the U.S. homeland.

As the previous chapters indicate, much of the U.S. defense effort is devoted to the projection overseas of sophisticated conventional military power. Proficiency in such symmetric warfare is necessary, but it is far from sufficient. A dedicated effort must also be mounted to counter asymmetric threats. Organizing that effort is the subject of this chapter.

Asymmetric threats are divided into three categories. First, there are vulnerabilities in the complex but fragile information technology (IT)–based systems-of-systems. Such threats as jamming communications that carry targeting information or the Global Positioning System navigation and timing signal, attacking reconnaissance satellites, or erecting decoy missiles to frustrate reconnaissance-strike systems are examples of challenges to the RMA for which countermeasures must be devised. The RMA military must be made more robust as it is made ever more sophisticated.

A second category of asymmetric threat is the potential use of weapons of mass destruction (WMD) — on the battlefield, at ports and airfields where U.S. power projection is taking place, or on the territory of allies the U.S. is trying to defend. This threat requires counter-proliferation capabilities such as protective suits and detectors, with accompanying tactics and doctrine for their effective use.

Third is the disturbing prospect that opponents will attempt to threaten the U.S. homeland with terrorism on a war-like scale. Catastrophic terrorism might result from the use of weapons of mass destruction, especially biological weapons; from attack upon the critical infrastructures upon which fragile modern society depends, including power, transport, communications, and finance; or from attack upon the persons and institutions of the federal government. The specter of attack on our homeland is a relatively new one; in this century, America's wars have been far away. The country is favored by geography, with oceans to the east and west, and friendly neighbors to the south and north. But globalization and technological change undercut the protection historically afforded by favorable geography.

In this century, it was only when the Soviet Union exploded the atomic bomb in 1949 that a direct external threat of destruction was 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.

In the coming years, an incident of catastrophic terrorism on the U.S. homeland would be likely to 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 corrosive of civil liberties as well as counterproductive. Because the aftermath of homeland attack could be as fearsome as the attack itself, our government should begin to organize for this future threat now, while considered judgments can be made about how best to protect the homeland and how to reconcile protection with our democratic values. The Department of Defense will, of course, play a role in homeland defense. Capabilities it possesses for battlefield use will find application in the event of homeland attack. But there are also limits to the role the military should play in providing domestic security. It is better for all if this role is defined in advance.

Countermeasures to Asymmetric Warfare

The history of warfare has always been a struggle between measures and countermeasures, and so it will be with asymmetric warfare. During the 1970s and 1980s, the U.S. offset strategy incorporated modern information technology in its weapons to offset the numerical superiority of the military forces of the Soviet Union. This strategy has come to be known as the Revolution in Military Affairs (RMA).

After the effectiveness of the new RMA weapons was convincingly demonstrated in DESERT STORM, nations potentially hostile to the United States began to seek "offsets to the offset strategy," i.e., countermeasures to America's RMA weapons. Since they are not able to copy U.S. weapons (indeed, even our technically advanced allies have been slow to do so), they are led to the development of asymmetric warfare techniques. More specifically, they seek to develop systems that can disrupt the information networks that serve the RMA weapons; their objective is to give the United States pause before it uses its superiority in conventional weapons. The Defense Department must, therefore, take steps to reduce the vulnerability of its RMA systems to these asymmetric measures.

There are many technical approaches to reducing the vulnerability of communication networks, including modification of circuits to make them more jam-resistant; designing protective shielding for circuits and cables; configuring critical networks with redundant nodes so that the loss of one node is not catastrophic; designing transmitters with frequency-hopping or frequency-spreading capabilities to make the intercept and jamming of these signals more difficult; and the use of radio frequencies in the high microwave band and with narrow beam widths to make them less accessible to potential jamming systems. A detailed discussion of how to reduce vulnerability to jamming and disruption would fill many volumes. The point to be made here is that although vulnerability reduction techniques are well known, they are generally expensive and difficult to implement, and often require changes in operating procedures. From this we draw important conclusions regarding future DOD programs.

First, countermeasures must be seen by the Defense Department to be a serious threat; otherwise, the actions necessary to reduce vulnerability, which are not easy or cheap, will not be taken. Second, many of the techniques for vulnerability reduction are best done when the communication network is designed or installed; therefore the commitment to reduce vulnerability needs to be made before the threat of countermeasures has been manifested by an actual attack on the network. And finally, reducing vulnerability is not just a matter of equipment design; most importantly, it affects tactics, doctrine, and training, all of which should be developed with explicit consideration of countermeasures. All of this is lacking in today's military, which has been lulled into a false sense of complacency. This complacency has arisen because Saddam Hussein's military forces were so taken by surprise by the effectiveness of RMA weapons that they were not able to mount an effective countermeasure program. But since then, Iraq and many other nations have learned the lessons of DESERT STORM and are seeking ways to counter the RMA. In the meantime, America's military forces have come to depend more and more on RMA, and therefore on the reliable operation of their information networks, but have done little to reduce their vulnerability to asymmetric attack.

We believe that this deficiency is so serious that it calls for dramatic changes in the way the U.S. military forces train. Robust countermeasures should become a required part of military exercises; at present they are often excluded because they "disrupt" the exercise, but of course this is exactly the point of having them. An even better approach, and the one we recommend, would require a significant modification to the major national training ranges such as those at Nellis Air Force Base and Fort Irwin. Special facilities should be added to these ranges that allow the robust application of countermeasures during exercises and the "scoring" of their effectiveness. The "Red Teams" that are resident at these ranges should develop countermeasure tactics as a part of every exercise, and the team being tested should be scored on how it responds to the countermeasures. This would serve to illuminate, first of all, the inadequacy of our present approach to countermeasures. More importantly, it would train American troops how to deal with countermeasures as best they can with present equipment and tactics. What is essential, however, is that it would lead to the development of improved tactics and doctrine, and to the establishment of requirements for the development of information networks with inherent resistance to countermeasures.

Counter-proliferation

In recognition of the fact that potential opponents in regional conflict might not play by the same rules as Saddam Hussein did in DESERT STORM, the U.S. Department of Defense launched a Counterproliferation Initiative in 1993. The objective was to integrate preparations to counter weapons of mass destruction into U.S. capabilities for power projection and joint operations. A great deal of progress has been made since 1993, including the creation of a Counter-proliferation Council chaired by the Deputy Secretary of Defense and the establishment of the Defense Threat Reduction Agency (DTRA) to bring together a number of WMD-related technology and field operations efforts. However, DOD's technology and systems acquisition capabilities are still fragmented, and WMD preparations are still incompletely integrated into planning for joint operations. These efforts will require the continuing attention of the Secretary of Defense.

The greatest deficiency in counter-proliferation, as in other cross-cutting issues described in Chapter 10, lies in interagency program coordination, however. An interagency program planning mechanism is needed for counter-proliferation, similar to the one described below (under "Homeland Defense") for countering catastrophic terrorism.

A second challenge for counter-proliferation is the improvement of our international cooperative efforts. One such effort is the Nunn-Lugar program, which should be expanded in scale and scope as detailed in Chapter 9. Cooperation with key allies and friends is also important: even if U.S. forces are adequately protected, allied forces and allied populations near a war zone cannot be left vulnerable to WMD attack. The new administration should, therefore, support and sustain the NATO Senior Defense Group on Proliferation and the bilateral counter-proliferation "Working Groups" with the United Kingdom, the Republic of Korea, Japan, Israel, and the Gulf Cooperation Council.

A third urgent need for U.S. counter-proliferation efforts is development of a technology base in biowarfare defense (BWD) that is as strong as our base in nuclear non-proliferation. The United States has strong DOD and DOE laboratories with thousands of personnel skilled in nuclear technology, but few experts in the field of biotechnology, neither within DOD's 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 (a problem discussed further in Chapter 6). Yet the implications of the biotechnology revolution for security will probably exceed those of the nuclear and information revolutions. DOD must do more than increase funding in the Defense Advanced Research Projects Agency (DARPA), the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID), and DTRA for biotechnology research, although this is also necessary. A university-affiliated government-funded laboratory (akin to the nuclear laboratories of the DOE) will need to be founded to give DOD a foothold in the BWD technology field, and to compete for talent despite the drawbacks of government employment practices and the attractive employment opportunities available to biotechnologists in the private sector.

Homeland Defense

New technology means that smaller and smaller groups of people, well below the scale of nation-states, will be able to inflict war-scale violence. This poses a fundamental long-term problem for global society. Appropriate and effective counters to this danger are likely to take a long time for the United States government and others around the world to devise. The question is where and how to begin.

When to begin should not be in question: the time is clearly "now." Even though an instance of catastrophic terrorism has not yet occurred, such an event seems inevitable. Not only is mass destructive power becoming more available, but society is becoming more vulnerable through the complexity, interdependence, and global reach of its supporting infrastructures. Some groups that turn to terrorism are motivated by vengeful and messianic rather than political agendas, inclining them to drastic acts that more "mainstream" terrorist groups would regard as excessive or counterproductive. The United States may be a prime target, precisely because its conventional power is so great that asymmetric means such as catastrophic terrorism might seem the only method available to those who would challenge U.S. policies by violent means.

The aftermath of the first event of catastrophic terrorism would be the wrong time to take preventive action. In an atmosphere of fear and hysteria, we are unlikely to achieve the delicate balancing among competing social objectives that such an effort requires. Because the effort involves protecting the homeland rather than foreign interests, and because terrorist groups might well include or even be composed entirely of U.S. citizens, this problem straddles the divide between the agencies in our government that are dedicated to fighting domestic crime and protecting civil rights and those that are devoted to countering foreign threats. The required effort will also involve agencies of the government that are not normally involved in security issues, such as the Department of Health and Human Services and the

Department of Agriculture. Preparations must extend well beyond the federal government to the state and local government bodies that respond to emergencies and provide essential services. Protecting critical national infrastructure must also involve the private-sector providers of these infrastructures.

A cross-cutting issue such as catastrophic terrorism therefore calls for an unusually broad concert of government departments. In recent years, the U.S. government has begun to put this concert together. This effort has been organized by the White House National Security Council and the existing departments and agencies, rather than by designating a single existing agency as "lead agency" or by creating a new "department of domestic security." Progress has been made in parceling out "lead agency" and "supporting" assignments, and setting policy on "who's in charge" in a given circumstance involving catastrophic terrorism. These assignments are consistent with the historical roles and other duties of the existing cabinet departments, with due regard for other social values such as civil rights. For example, lead federal agency responsibility for responding to imminent threat of catastrophic terrorism (called "crisis management") was assigned to the domestic law enforcement agencies, the Department of Justice, and the Federal Bureau of Investigation, rather than to national security agencies such as the DOD or the Central Intelligence Agency.

This arrangement is appropriate and can work, but its current capability falls far short of what is needed to counter catastrophic terrorism. In many cases the agencies assigned lead roles have few or no capabilities for carrying them out and little funding, technology, or institutional base to build new capability. The result is a host of unfunded mandates. Other agencies, of which DOD is the prime example, are assigned only supporting roles, but have preponderant capability because of their other missions, including, in DOD's case, counter-proliferation, force protection, and defense information network protection. The result of this management plan is that if an incident of catastrophic terrorism occurred in coming years, the federal government agencies would arrive on the scene with an orderly system of command and control but with capabilities that are inadequate: a "come-as-you-are" party.

We have finished the period of assigning roles, and now it is time to begin an era of capability building. Now that the National Security Council (NSC) has coordinated interagency policy for catastrophic terrorism, it must begin to coordinate interagency programs. We need a national program covering technology, doctrine and techniques, law and regulation, research into the underlying causes of catastrophic terrorism, and institution-building. This program should cover all phases of the "life cycle" of catastrophic terrorism: intelligence, prevention and deterrence, warning, protection, crisis management, damage mitigation and cleanup (called "consequence management"), forensics and attribution as the basis for prosecution or retaliation, and "lessons learned" to prevent future events.

The NSC has not performed this type of program design and coordination in its recent history (for more on this point, see Chapter 10), as it is mainly a mechanism for policy coordination, not program coordination. It has little clout in determining agency budget allocations or internal management, while the Office of Management and Budget (OMB) does not play a very strong role in interagency budget coordination among the national security agencies compared to its role in domestic policy matters. NSC staff are typically selected for their foreign policy and international experience rather than experience managing large operating agencies or technical programs. In this weak NSC program coordination system, program decisions coordinated at the NSC are easily ignored by departments or overturned by congressional committees that have even weaker mechanisms than the executive branch for coordinating cross-cutting activities.

The problem of program design, planning, and coordination is common to many post–Cold War new missions that are cross-cutting and where new capabilities are required. As discussed further in Chapter 10, this problem can be addressed within the existing NSC and departmental structure through a strengthened White House mechanism. Specifically, we recommend a new NSC arm, headed at the level of a Deputy National Security Adviser, with a small staff experienced in program and budget management. This entity would have the charter to draw up a coordinated program plan for catastrophic terrorism, counter-proliferation, peacekeeping support, and other cross-cutting issues on behalf of the President. OMB would play an essential role in this new arrangement, ensuring that agencies reflect the President's cross-cutting program plan in their budget priorities and in their internal organization and management. In comparable efforts in the past, an active role by the Vice President, the only official besides the President who stands above the cabinet secretaries, has also proved valuable.

DOD's role in the national program for homeland defense is appropriately not a lead one. But DOD should play a strong supporting role, especially in the interagency program to build capability. Much of the needed effort can be an offshoot of DOD's existing missions of counter-proliferation, force protection, and protection of its own information networks.[2] For example, as DOD seeks information dominance through the application of network technology as described in Chapter 3, it will become increasingly important that its information systems remain secure. Through the National Security Agency and other DOD components, the Department must conduct a strong program to develop and deploy security technology such as public-key cryptography, and techniques such as requiring two cleared persons to perform key network control functions (akin to the "two-man rule" long in force for personnel who handle nuclear weapons). Due to DOD's sheer size, this effort will dwarf any comparable effort that other agencies can mount, and it should therefore be conducted as the core of a national effort. For example, DOD could take the lead in funding a National Information Assurance Institute, a government-funded but private organization dedicated to developing best-practice information assurance techniques and technology in partnership with the private sector.[3]

Conclusion

The very strengths of the U.S. military could also create vulnerabilities unless we begin, now, to recognize them and to plan appropriate protections and countermeasures.

[2] The ingredients of a DOD program to contribute to the national effort against catastrophic terrorism were detailed in Ashton B. Carter and William J. Perry, *Preventive Defense: A New Security Strategy for America* (Washington, D.C.: The Brookings Institution, 1999).

[3] The National Information Assurance Institute concept was described in Carter and Perry, *Preventive Defense*, pp. 164–165.