PART I. NEW CHALLENGES FOR DEFENSE

INTRODUCTION TO PART I

Defense planning during the Cold War was dominated by the threat from the Soviet Union. It was, in that sense, threat based. It also was, to a great extent, symmetrical, based on force-on-force calculations for U.S. and Soviet armored forces, fighter jets, and the like. In these circumstances, the U.S. planning structure within the Pentagon became increasingly centralized, seeking to maximize the benefits from various investments in ways to better cope with the Soviet threat.

All the practices that made considerable sense during the Cold War badly need to be rethought now. Soviet strategy may have been more creative than it was usually given credit for, but it was relatively slow moving. By contrast, today's threats—and still more tomorrow's—are many and very uncertain. While none may be in a class with the Soviet threat, the attacks of September 11, 2001, drove home how lethal even "lesser" threats can be. Moreover, U.S. military power has given rise to a paradox: the United States is so dominant in its ability to fight a conventional armored war that it is not likely to have to fight such a war. Realizing the futility of a conventional face-off with the United States, would-be adversaries will instead aim to confront the United States where it is weak or can be surprised—posing what are called *asymmetric* threats. Terrorism, the strategy of the weak against the strong, is quintessentially an asymmetric strategy.

This change from a fairly predictable, symmetrical threat to the myriad unpredictable, asymmetrical threats possible has profound effects for defense planning. It impels a shift from threat-based planning to capabilities-based planning and suggests that a "portfolio" approach to these capabilities—i.e., trying to build breadth and flexibility in the hope that capabilities can be brought to bear across a spectrum of unpredictable threats—would be the most useful type. It also presses the United States to draw on advantages where it has them, particularly in harnessing information technology to identify threats, link shooters tightly to sensors, and manage a flexible, fast-moving campaign. And it hints at the value of decentralizing Pentagon management so as to encourage the innovation needed to produce a real "revolution in military affairs" (RMA).

In the first chapter here, "Decisionmaking for Defense," David S.C. Chu and Nurith Berstein argue that any military organization must ask itself four questions: what forces should be fielded, how should they be trained, how should they be equipped, and what tempo of operations should they maintain? The two questions on force structure and equipment are likely to dominate in the next decade. The debates over the size and structure of military forces that were not fully joined in the 1990s will have to be faced squarely, particularly in light of strains placed on the current force by the pace of operations, all the more so with the war on terrorism. Moreover, the urgent need to recapitalize the present generation of equipment places this issue near, perhaps atop, the agenda. In this regard, a central issue is the degree to which new investment should shift from modernizing existing capabilities to procuring quite different capabilities, ones geared to a different vision of what future military forces might look like. The more decisionmakers lean toward a new vision, the greater the challenge they will pose to how "legacy" systems—including some still under development—are treated. Such fundamental issues are never settled once and for all or even for very long.

In Chapter Two, "Responding to Asymmetric Threats," Bruce Bennett explains why U.S. conventional military superiority has forced adversaries to pursue asymmetric strategies—i.e., those designed to attack such vulnerabilities as U.S. and allied will, host nation support, and basing infrastructure. Potential adversaries have developed weapons of mass destruction (WMD), information warfare, and simple countermeasures such as sea mines as part of their asymmetric threats, and they use camouflage, concealment, and deception to hide their capabilities and strategies. Part of the danger of asymmetric threats stems from the surprise they can achieve, which undercuts U.S. response preparation, leaving the United States at a disadvantage. Asymmetric threats can affect U.S. and allied forces, civilians, and interests in diverse ways that are difficult and expensive to counter. The threat of retaliation, alone, is insufficient to deter their use in at least some cases. What is needed is an integrated defense effort that includes three elements: understanding the threats, protecting against them, and threat management. Understanding the threats is key to addressing them, protection is necessary to reduce any gains the adversary may be seeking, and threat management seeks to deter the spread of such threats and discourage the development of new ones. The United States must institutionalize its response efforts within its own military; it must also internationalize them, coordinating with allies to provide a common defense.

Chapter Three, “What Information Architecture for Defense?” by Martin Libicki, is a plea for planners to recognize the choices, deliberate or not, that underlie enterprise-level information technology systems and thereby shape how they are used. One office networking system may be much like another, but the Pentagon’s requirements for information will vary depending on whether it is planning for a strategic campaign (putting a premium on analytic skills to determine enemy strengths and weaknesses), a conventional campaign (with its need for mass force coordination), modern high-technology warfare (which requires that targets be found and prosecuted in real time), or a low-intensity conflict (which requires that warfighters be enabled with subtle but detailed portraits of their environment). Information architectures may be described by how they collect, present, display, circulate, maintain, secure, standardize, and integrate information. Each of these eight dimensions involves choices that the Pentagon must make if it is to make best use of U.S. advantages in information technology.