Chapter Two

RESPONDING TO ASYMMETRIC THREATS

Bruce W. Bennett

As Chapter One indicates, Cold War planning dealt largely with "symmetric" threats—strength-on-strength planning vis-à-vis the Warsaw Pact, especially in central Europe. Warfighters find it easiest to address such threats, ones they understand thanks to the Cold War experience. But America's ability to prevail handily against symmetric threats has forced U.S. adversaries to pursue asymmetric threats. In one sense, strategies often include asymmetric components in that they seek to exploit the other side's vulnerabilities, but the Cold War's image of two broadly similar superpowers obscured that fact.

The 1997 Quadrennial Defense Review (QDR) identified asymmetric threats, or "challenges," as a major issue for the U.S. military.[1] Previous RAND work[2] defined asymmetric threats as those that attack vulnerabilities not appreciated by the target or that capitalize on the target's limited preparation against the threat. These threats usually rely on concepts of operation (CONOPs) that differ from the target's and/or from those of recent history.[3] The U.S. military understands

[1]William S. Cohen, *Report of the Quadrennial Defense Review*, Department of Defense, May 1997, in particular pp. 4 and 49–51, but also pp. vii, 12, 13, 19, 41, and 43.

[2]Bruce W. Bennett, Christopher P. Twomey, and Gregory F. Treverton, *What Are Asymmetric Strategies?*, DB-246-OSD, RAND, 1999.

[3]Additionally, asymmetric threats can serve political or strategic objectives not shared by the victim. For example, in 1941, U.S. economic sanctions against Japan were intended to coerce Japan into stopping its aggression in East Asia. But the Japanese, having different strategic objectives, responded with an asymmetric strategy: a strike against Pearl Harbor that sought to neutralize the U.S. Pacific Fleet and thereby to convince the United States to disengage from East Asia.

its own strengths and tends to focus on them even when it does not see comparable preparations by a prospective adversary, assuming that warfare will be largely symmetric in character. This failure to adequately recognize asymmetric threats is neither new nor unique to the U.S. military.[4] However, given that asymmetric threats are now the greatest threats to the U.S. military and U.S. society (as the terrorist attacks of September 11, 2001, drove home), the subject requires particular attention in U.S. military planning.

This chapter characterizes asymmetric threats and outlines steps the U.S. military needs to take to counter them. It starts with a general introduction to asymmetric threats, explaining why and how they would be wielded. It also addresses the importance of adversary surprise and anonymity, as well as the nature of challenge and response cycles. It then focuses on threats based on chemical and biological weapons, which are a significant element of the current threats to the United States and its allies.

FROM THE COLD WAR TO THE PRESENT

The two principal arenas for Cold War military confrontation with the Soviet Union—the NATO Central Front on the inter-German/Czech border, and strategic nuclear conflict—were perceived by the United States as symmetric confrontations, creating a culture of expectation for strength-on-strength combat. Yet even these Soviet threats included many elements that were asymmetric. On the Central Front, armor faced armor in a contest of maneuver, and both sides depended on artillery, aircraft, and naval forces. U.S./NATO strategy eventually focused on developing technologically superior weapons to provide an asymmetric advantage for NATO. Meanwhile, the Soviets relied on quantity and strong CONOPs, including the heavy use of special forces and chemical and biological weapons (CBW); artillery disruption leading to breakthroughs, especially against the weaker forces of some NATO allies; and penetration concepts, such as operational maneuver groups.[5]

---

[4]Comparable historical concepts have included the writings of Sun Tzu, maneuver warfare, and centers of gravity.

[5]An operational maneuver group was a corps-sized heavy maneuver force designed to penetrate an operational breakthrough (the collapse of at least part of a NATO corps

Despite the efforts of some military specialists, however, the extent of asymmetry in the Soviet threat was not well comprehended in the United States.

Each side's strategic nuclear forces consisted of a triad: intercontinental ballistic missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and bombers. Many in the United States argued that stability was maintained by the assured ability to destroy opposing urban/industrial areas even after suffering a first strike against strategic weapons. The United States planned a nuclear response to a major Soviet conventional force breakthrough in NATO, and proposed a doctrine of limited nuclear operations to control the escalation from such nuclear weapons use. After the Cold War, the United States learned that the Soviets had taken asymmetric approaches to many of these U.S. concepts and did not accept the primacy of assured destruction. For example, the Soviets created vast production capacities for and stockpiles of such biological weapons (BW) as anthrax and smallpox and planned to use them against the United States.[6]

This perception of symmetry led many U.S. analysts to conclude that quantitative measures of military hardware, units, and warfighters were the key metrics for evaluating the military capabilities of the United States and the Soviet Union. Analysts compared the numbers of U.S./NATO tanks, artillery pieces, combat divisions, military manpower, and fighter aircraft to Soviet/Warsaw Pact equivalents.[7] Strategic analysts counted ICBMs, SLBMs, bombers, and warheads, and assessed mixed quantitative/qualitative measures such as equivalent megatons and countermilitary potential.[8] Analysts and de-

---

sector) and overrun targets behind the front, including headquarters, airfields, major storage depots, and even political targets. The hope was that by so doing, these groups would expedite the strategic collapse of NATO's defenses.

[6]See Kenneth Alibek, "Biological Weapons," presented to the USAF Air War College, November 1, 1999. It refers to Soviet storage of anthrax in excess of 100 tons, with an annual production capacity of thousands of tons; it also says that the Soviets had stockpiles of plague and smallpox that were each roughly 20 tons.

[7]See, for example, *NATO and the Warsaw Pact: Force Comparisons,* NATO Information Service, 1984; and William P. Mako, *U.S. Ground Forces and the Defense of Central Europe*, The Brookings Institute, 1983.

[8]See, for example, Paul Nitze, "Considerations Bearing on the Merits of the SALT II Agreements as Signed at Vienna, *The Congressional Record—Senate*, July 20, 1979, pp.

cisionmakers talked in terms of a "military balance," as if roughly equal force quantities were stable and greater quantities conferred military advantage.[9] In practice, most comparisons concluded that because the Soviet Union had more military equipment, personnel, and units, it held a military advantage, though there were some uncertainties even about these quantities. These comparisons were largely strength-on-strength comparisons and thus tended to ignore other key characteristics and relative vulnerabilities—the essence of asymmetric threats.[10] In addition, these analyses seldom considered whether U.S. and allied forces could perform their missions or meet their operational requirements.

Today, military leaders and analysts, trained during the Cold War, are tempted to apply similar methods in discussing U.S. conventional and nuclear superiority over potential adversary states.[11] Figure 2.1 shows how U.S. conventional and nuclear capabilities overwhelm the conventional capability of most prospective adversaries,[12] especially the "rogue states," such as Iraq, North Korea, and Libya. And the addition of weapons of mass destruction (WMD) by these rogue states is not seen as providing sufficient "strength" to offset U.S. ca-

---

S10070–10082; and Robert L. Leggett, "Two Legs Do Not a Centipede Make," *Armed Forces Journal International*, February 1975, pp. 30–32. A critique of these methods is contained in Bruce W. Bennett, *Assessing the Capabilities of Strategic Nuclear Forces: The Limits of Current Methods,* N-1441-NA, RAND, June 1980.

[9]See, for example, arguments on the Conventional Forces in Europe (CFE) negotiations in James R. Thomson and Nanette C. Gantz, *Conventional Arms Control Revisited: Objectives in the New Phase*, N-2697-AF, RAND, December 1987.

[10]These comparisons acted as if the relative quality of military personnel or command-and-control or intelligence or even (in many cases) hardware quality did not matter in the overall assessment. The Soviets included qualitative force multipliers in their assessments, as discussed in Allan S. Rehm and Joan F. Sloan, *Operational Level Norms,* SAI-84-041-FSRC, SAIC, April 24, 1984, especially Section 3.

[11]Most military analysis is still fixed on repelling ground force invasions. Neither the diversity of other U.S. military engagements nor the differences in each side's vulnerabilities and force requirements get much attention. Although such threats as ballistic missiles are recognized, conflicts that entail their use per se (rather than as ancillaries to an invasion) are downplayed.

[12]The United States explicitly wishes to avoid becoming an adversary of the world's other great powers. "The United States is committed to expanding its network of friendships and alliances with the aim that eventually all of the world's great powers will willingly cooperate with it to safeguard freedom and preserve peace" (Donald H. Rumsfeld, *Guidance and Terms of Reference for the 2001 Quadrennial Defense Review*, June 22, 2001, p. 1).

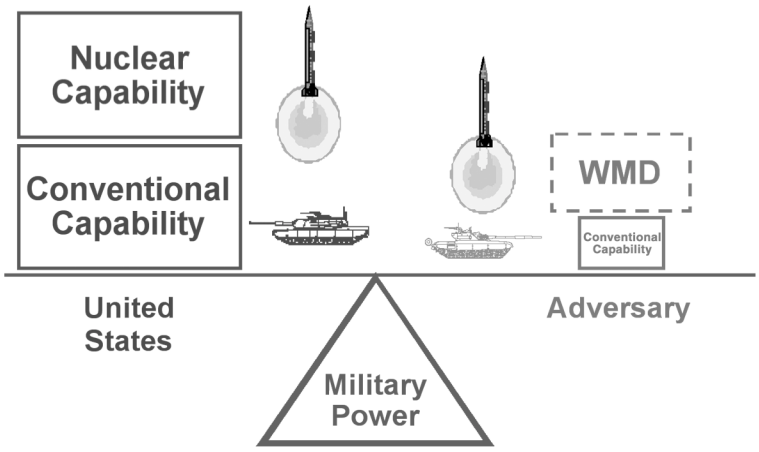

Figure 2.1—Symmetric View of Military Power

pabilities. During the Cold War, many smaller states accepted this imbalance because the Soviet Union counterbalanced U.S. strength. But now they face the United States on their own and cannot afford the U.S. level of military capabilities.

U.S. conventional military superiority remains focused on its traditional threats: armored and air assaults over relatively open terrain to conquer territory of a U.S. ally. In the 1990s, theorists spoke of a revolution in military affairs (RMA) that would allow the United States to use technology to overwhelm such a threat. "An RMA . . . renders obsolete or irrelevant one or more core competencies of a dominant player."[13] Indeed, the United States has made most opposing forces of armor, aircraft, and ships obsolete in symmetric conflicts against it.

Figure 2.2 suggests that because adversaries cannot achieve a military balance with the United States using symmetric approaches, they have been induced to find other ways to undermine U.S. mili-

[13]Richard O. Hundley, *Past Revolutions, Future Transformations,* MR-1029-DARPA, RAND, 1999, p. 9.

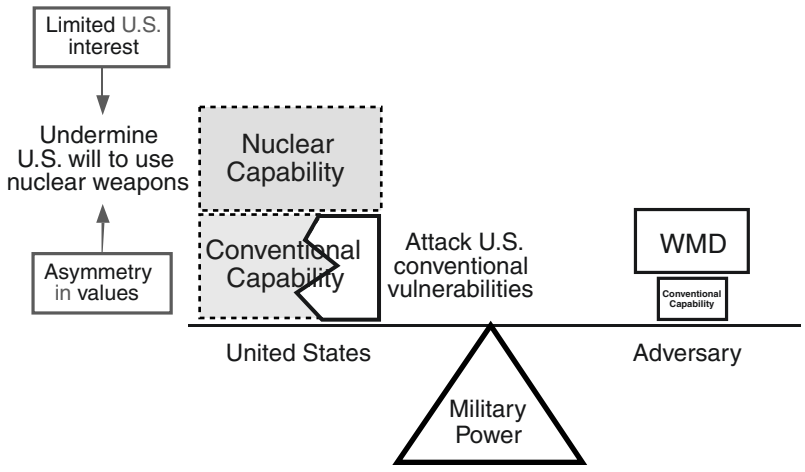

Figure 2.2—How Adversaries Might Use Asymmetric Threats

tary power—by attacking U.S. military vulnerabilities or America's will to use its military might.[14] Any of the approaches could remove a significant part of U.S. strength from the balance, giving adversaries a chance to prevail.

Few U.S. adversaries now contemplate a conventional force invasion of a neighboring territory, especially one allied with the United States, but they have still sought to improve their military capabilities.[15] They are also pursuing asymmetric approaches to achieve their objectives, such as standoff coercion, guerilla warfare, subversion, and information warfare. The little "RMAs" that play a role in the pursuit of these approaches include cover, concealment, and deception to prevent the United States from recognizing threats or

[14]This very simple depiction ignores the role of U.S. allies and U.S. forward basing. Figure 2.3 extends this simple approach.

[15]One exception, North Korea, may yet invade its neighbor, South Korea, using conventional forces. Its asymmetric "facilitating force," which would remove or suppress many U.S. and South Korean defenses, includes artillery with chemical shells that would be used against U.S. and South Korean ground forces; special forces and ballistic missiles armed with CBW to suppress airfields, ports, command, control, communications, and logistics; and cruise missiles and aircraft to sustain CBW contamination.

countering them; new delivery means, such as ballistic and cruise missiles or unmanned aerial vehicles (UAVs) that are inexpensive and difficult for the United States to counter; and WMD to affect military operations or coerce neighbors.

EXAMPLES OF ASYMMETRIC THREATS

Examples of asymmetric threats might include the following:

- Computer hackers use e-mail viruses to destroy U.S. military personnel records and the software used to process them, thereby seeking to delay U.S. force deployments and mobilization.
- Terrorists explode bombs against civilian targets in New York City.[16]
- Adversary special forces fire handheld surface-to-air missiles (e.g., SA-16s) against U.S. cargo aircraft, tankers, and command-control aircraft taking off from theater airfields.
- Operating from fishing ships, Iraqi special forces spray BW upwind of U.S. Navy ships in the port of Jabal Ali in the United Arab Emirates. (Jabal Ali is the largest port in the Persian Gulf.)
- Seeking to split the U.S.-led coalition against Iraq, Saddam Hussein claims that U.S.-sponsored sanctions are starving Muslims in Iraq.
- North Korea uses chemical weapons (CW) against the Republic of Korea.
- China threatens a nuclear attack on U.S. cities if the United States interferes in its actions against Taiwan.

These threats may employ novel weapons but need not do so; the weapons can be similar to those of the target. What makes threats asymmetric is the difference in CONOPs and that such threats are used against the target's unexpected vulnerabilities. The target is usually surprised, and the stun effect may delay a response—all of which amplifies the impact. It takes years to build appropriate mili-

[16]This example was in the first draft of this text, which was prepared well before September 11, 2001.

tary forces and capabilities to counter such threats. Asymmetric threats are relative; some are more asymmetric than others.

HOW WOULD ADVERSARIES SHAPE ASYMMETRIC THREATS?

Figure 2.3 refines the concepts of Figure 2.2. September 11 notwithstanding, most of the possible conflicts in which the United States will want to intervene will be far from U.S. shores. Hence, the United States must project military power into a region, which requires military means, U.S. will, and the will and support of regional allies that will allow U.S. force and logistics basing and often fight alongside the Americans. U.S. discussions of asymmetric threats usually focus on adversary operations against U.S. military capabilities, such as Scud missiles with chemical warheads being fired at airfields to degrade aircraft operations or disrupt the flow of combat aircraft and their support into the theater. Airfields and other combat support facilities make good targets because they are far more vulnerable than combat aircraft themselves. The United States tends to concentrate its military resources in a few locations in the theater (e.g., airfields, ports, and command facilities) to minimize costs and coordination efforts, but such "massed" facilities make excellent targets for WMD, as well as for conventional weapons delivered by special forces.[17] Despite the recent U.S. focus on protecting these facilities, they remain vulnerable to at least some asymmetric threats.

However, adversaries may find it easier and safer to undermine the will and support of key U.S. regional allies than to attack U.S. military capabilities. Allies understand that their military forces and civilians tend to be more vulnerable than U.S. deployed forces. Their interests frequently differ from those of the United States, especially if they are not the immediate targets of an adversary's invasion. In 1990, when Iraq's invasion victimized only Kuwait, other countries in the Persian

[17]An adversary's military culture may lean toward asymmetric threats. For example, because most of North Korea's political and military leadership came out of the special forces Kim Il Sung operated in World War II, North Korea has emphasized special forces operations. By contrast, most U.S. military analysis expresses concern over special forces operations but largely ignores the damage they can do and thus devalues potential actions to counter them.

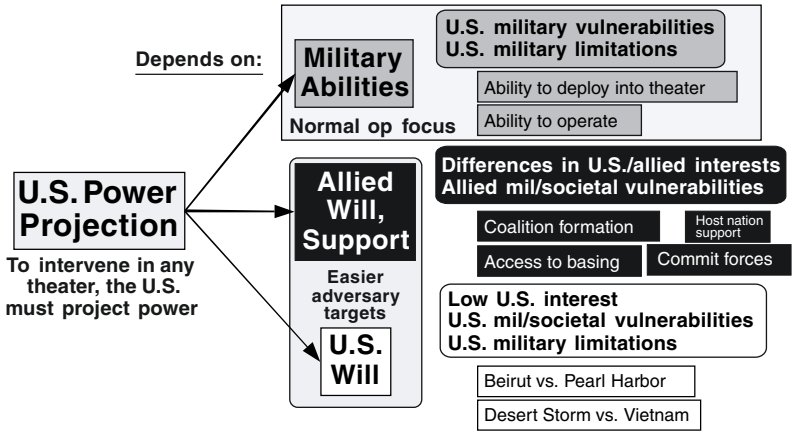

Figure 2.3—U.S. Requirements for Military Power Projection

Gulf were initially uncertain about how much access and support to give the United States. Each worried about its vulnerability to Iraq, fearing that allowing U.S. forces to attack Iraq from its soil might lead to Iraqi retaliation. That is, in fact, what happened: Iraq responded with Scud missiles.

Even when the United States can gain access to regional states, to operate it needs "host nation support"—workers for docks and airfields; power, water, communications, and transportation infrastructure; and so on. Unless these workers are protected against WMD threats by either the host nation or the United States, they may become casualties or flee. Either would degrade U.S. deployment and operations.

U.S. will is especially at risk because U.S. interest in recent and prospective regional conflicts far from home has been limited. U.S. military casualties caused a collapse of U.S. will in the Beirut, Lebanon (1983) and Mogadishu, Somalia (1993) interventions. Some foes contemplate how the U.S. will to intervene, especially in offensive roles, such as in Kosovo, can best be defeated—by posing a

strategic threat to the United States[18] or by simply raising the cost of U.S. involvement so that it exceeds the advantages to be gained in interventions of low U.S. interest.

Yet calculating the effects that asymmetric threats or attacks will have on U.S. will is no easy task for would-be adversaries. The 1983 attack on the Marine barracks in Beirut led to a U.S. withdrawal from Lebanon. U.S. interest was very low, and the imposed cost—several hundred soldiers killed—was moderate, with the result that the United States decided to discontinue the intervention. However, the 1941 Japanese attack on Pearl Harbor drove the United States into World War II. The United States perceived its interest in Hawaii to be so vital that Japan was unable to impose too high a price for U.S. intervention. Instead, America felt compelled to remove Japan as a threat to U.S. national security. Getting the threat just right requires imposing costs large enough to prevent U.S. intervention but not so large as to trigger a U.S. change in objectives and/or a demand for revenge.[19] After September 11, there was continued concern about losing too many American lives, but there was no doubt that the United States would do what was required to overturn Afghanistan's Taliban regime and attack Al Qaeda.

The statement of a North Korean sympathizer evokes the dilemma would-be adversaries face: "Which is better prepared for nuclear exchange, North Korea or the USA?. . . The DPRK can be aptly described as an underground fortress. . . . For their part, the North Koreans are

---

[18]See, for example, Northeast Asia Peace and Security Network, "DPRK Report #19: The Importance of NK Missiles," August 9, 1999, http://www.nautilus.org/pub/ftp/napsnet/russiadprk/dprk_report_19.txt. In addition, in an article in the *New York Times*, Michael R. Gordon quotes Chinese official Sha Zukang as saying, "Once the United States believes it has both a strong spear and a strong shield, it could lead them to believe that nobody can harm the United States and they can harm anyone they like anywhere in the world. There could be many more bombings like what happened in Kosovo." Gordon then goes on to say, "He [Sha Zukang] made plain that China's fear was not that the United States would launch a surprise attack on China, but that a missile shield would lead American politicians to believe that the United States was so powerful and well protected that it could act with virtual impunity." (Michael R. Gordon, "China Looks to Foil U.S. Missile Defense System," *New York Times,* April 29, 2001, p. 6.)

[19]Because the United States has learned that many adversary's threats are idle, an adversary may be tempted to demonstrate its capabilities to make its threats credible. Such a demonstration, especially if carried out within the United States, would almost certainly be escalatory.

highly motivated candidate martyrs well prepared to run the risk of having the whole country exploding in nuclear attacks from the USA by annihilating a target population center."[20] Arguably, even the current U.S. interest in Korea would not justify risking a single nuclear attack on the U.S. homeland. But the very first North Korean nuclear attack on U.S. soil would challenge U.S. survival, likely making the United States prepared to withstand great losses to eliminate the North Korean threat.

It is also tempting to think of adversaries posing only a single asymmetric threat—i.e., just one of the examples cited here—even though adversaries may plan some diversity and combination of threats. Then, because U.S. military power requires a combination of many factors, damage to any one of those factors could degrade U.S. combat capability. According to Mark Mateski, the Provisional Irish Republican Army (IRA) once warned Margaret Thatcher, "We only have to be lucky once—you will have to be lucky always."[21] Osama bin Laden might have said the same thing.

THE IMPORTANCE OF SURPRISE AND ANONYMITY

Asymmetric threats target unappreciated vulnerabilities, and they tend to result in surprise. Attacking at unexpected times or in unexpected ways heightens the surprise; so does hiding the preparations or misleading the victim about one's objectives, strategy, capabilities, and deployments. Adversaries that avoid having attacks attributed to them may achieve many objectives *and* avoid retaliation. According to CIA Director George Tenet, "More than ever we risk substantial surprise. This is not for a lack of effort on the part of the

---

[20]Kim Myong Chol, "The Future of the Agreed Framework," Northeast Asia Peace and Security Network, Policy Forum Outline (#23C), November 24, 1998, http://www.nautilus.org/pub/ftp/napsnet/special%5Freports/pf23c%5Fkim%fFon%5Fagreed%5Fframework.txt.

[21]Mark Mateski, "The Policy Game," *Red Team: The Journal of Military Innovation*, August 1998, http://www.redteamjournal.com/issuePapers/issue_paper2.htm. In the same article, Mateski says, "And while we spend our strength chasing Bin Laden, each potential adversary will continue to prepare to fight us on its own terms, whatever terms suit it best. For Iraq, the preferred way of war may be another ground assault supplemented with chemical and biological weapons. For North Korea, it may be a massive frontal onslaught. For China, it may be a cat-and-mouse maritime contest. In any case, we must be prepared for them all."

Intelligence Community; it results from significant effort on the part of proliferators."[22]

The possibility of surprise is increased by the fact that U.S. planning and analysis remain so dominated by high-end, largely symmetric threats that resemble those of the Cold War. Most defense policymakers and analysts lack a strategic appreciation for asymmetric threats (such as CBW threats in Korea before 1997), as well as a tactical/operational appreciation for them. They may have known, for instance, that terrorism was a threat in Saudi Arabia before the bombing of Khobar Towers in 1996, but not when and how the towers would be struck. Why the failure?

- U.S. threat-based planning is very susceptible to adversary deception. As a result, the United States mischaracterizes and often underestimates the adversary's threat and thus feels increased surprise when the threat is carried out.
- Analysts tend to "mirror image" an adversary when intelligence on the adversary's strategy and CONOPs is thin.
- Large bureaucracies, plagued by groupthink, have trouble accomplishing the "thinking outside the box" needed to understand how an adversary would employ a threat in novel ways. This also stifles projections of the effects an asymmetric threat may have and thus limits options for changing operations and forces to respond to them.
- Resource constraints tend to focus on force modernization in terms of traditional weapons, such as fighter aircraft, destroyers, and artillery. Less attention is paid to developing and fielding the

[22]"Text: DIA Director Tenet Outlines Threats to National Security," U.S. Department of State, International Information Programs Internet Site, Washington File, 21 March 2000. Tenet then cited four reasons why: "First and most important, proliferators are showing greater proficiency in the use of denial and deception. Second, the growing availability of dual-use technologies is making it easier for proliferators to obtain the materials they need. Third, the potential for surprise is exacerbated by the growing capacity of countries seeking WMD to import talent that can help them make dramatic leaps on things like new chemical and biological agents and delivery systems. . . . Finally, the accelerating pace of technological progress makes information and technology easier to obtain and in more advanced forms than when the weapons were initially developed."

equipment and forces required to respond to "unproven" asymmetric threats.

Without adequate preparation, the United States will lack the people and equipment it needs to counter new threats, and responding to such threats takes time.[23]

Most adversaries would like to defeat the United States without having to pay for it. They may attempt to avoid reprisal by hiding their strategy and CONOPs and, perhaps, by carrying out attacks covertly. They may not need to claim credit for the damage done, depending on their objectives. If the United States cannot attribute an attack to an adversary, it may lack the will to retaliate. Thus, deterrence will not work well against an adversary that thinks it can avoid attribution.

CHALLENGE AND RESPONSE CYCLES

As the United States and potential adversaries pursue new military capabilities, "challenge and response cycles" result.[24] Thus, as adversaries' threats create new challenges for the United States, the issue becomes one of how quickly the United States can respond. For example, in the Cold War the Soviet Union used the threat of a massive armored invasion to challenge the United States and its NATO allies. Their response was to seek higher-technology armored forces and, especially, air forces that could interdict Soviet armor. The quality of the U.S. response was inadequate until the late 1980s. As it turned out, this anti-armor response developed for the Soviet threat defeated Iraq's 1990 challenge in the Persian Gulf.

This U.S. anti-armor response challenged other potential adversaries, however. Many responded by developing CBW, thus posing

---

[23]Adversaries often fail to understand asymmetric operations and thus fail to exploit them. See, for example, the discussion of Germany's treatment of chemical weapons in World War I in Kenneth F. McKenzie, Jr., "An Ecstasy of Fumbling: Doctrine and Innovation," *Joint Forces Quarterly*, Winter 1995–96, pp. 62–68. Such failures may reduce the overall effect of the operations, but considerable damage may still be done (e.g., Germany's CW attacks in World War I).

[24]Sam Gardiner and Dan Fox originally described this cycle in unpublished RAND work on RMAs.

a new, asymmetric challenge to the United States, which has renounced the use of CBW. The United States counterresponded by threatening reprisals, which succeeded in deterring Iraq in 1991, and it has also worked on better defenses against CBW. But these responses have lagged adversaries' CBW challenges—even today, the United States remains relatively vulnerable to CBW attacks. And CBW is only one among a diverse set of asymmetric threats.

Worse, in today's relatively short wars (often only weeks or months long, as opposed to years), each side largely brings to the conflict the forces and capabilities it has prepared beforehand. If U.S. adversaries fight differently and the United States lags too far in the cycle, it may be leaving itself particularly vulnerable.

Its focus on threat-based planning has caused the United States to lag in many challenge and response cycles. Planning that is threat based requires an established threat. When adversaries hide the details of their threats, it can take years or even decades (if ever) to uncover the details, which puts the United States behind its adversaries.

The capabilities developed as part of the U.S. RMA also introduce new military vulnerabilities. For example, U.S. use of a global positioning system (GPS) allows precise weapons delivery—unless an adversary finds ways to jam the GPS in the area. In addition, many U.S. weapons that attack ground forces by scattering warheads over a broad area—a single CBU-97, which contains 40 sensor-fuzed weapons and covers an area of 15 acres,[25] or a SADARM (sense and destroy armor munition), which covers 20 acres[26]—may work well in deserts or behind adversary lines, but they can cause great collateral damage to friendly military vehicles or civilian vehicles intermixed with adversary forces (e.g., at the battlefield front, along adversary penetrations, or in urban areas). If adversaries focus on creating intermixed environments (a "nonlinear battlefield"), they can make it difficult for the United States to use its "superior" weaponry.

---

[25]Glenn W. Goodman, Jr., "Nowhere to Hide," *Armed Forces Journal International,* October 1997, p. 59.

[26]Goodman, "Nowhere to Hide," p. 61.

THE CHALLENGE OF WEAPONS OF MASS DESTRUCTION

A particularly fearsome class of asymmetric strategies involves WMD—nuclear, radiological, biological, and chemical weapons. These weapons can hurt military forces and civilians in great numbers and are thus a significant element of adversaries' threats. Not surprisingly, President Bush focused on WMD in his 2002 State of the Union Address: "Our nation will continue to be steadfast and patient and persistent in the pursuit of two great objectives. First, we will shut down terrorist camps, disrupt terrorist plans, and bring terrorists to justice. And, second, we must prevent the terrorists and regimes that seek chemical, biological or nuclear weapons from threatening the United States and the world."[27]

President Bush specifically identified North Korea, Iran, and Iraq as states with WMD and as being part of an "axis of evil." A CIA report immediately after the president's speech also identified Russia and China as key suppliers of WMD technology, and Libya, Syria, Sudan, India, Pakistan, and Egypt as states acquiring technology relating to WMD and advanced conventional munitions.[28] It has been widely reported that North Korea possesses 2,500 to 5,000 tons of CW, that Iran possesses thousands of tons, and that Russia has had some 40,000 tons of CW and potentially thousands of tons of biological agents.[29]

Although often discussed as if they were a single category of weapons, the various WMD differ greatly, as Table 2.1 indicates. Many of their effects are a function of the wind blowing fallout or CBW aerosols. Some BW are incapacitating but not lethal; others, such as anthrax (which was spread by letters in the wake of September 11), are quite lethal. Many BW, especially those dispersed as sprays, are neutralized in minutes or hours by sunlight and rain; others (e.g., smallpox) are contagious and spread from person to person. Some CW (e.g., VX) persist in liquid form on the ground and become a protracted vapor and contact hazard until they evaporate or are ab-

---

[27]See http://www.whitehouse.gov/news/releases/2002/01/20020129-11.hmtl.

[28]See http://www.cia.gov/cia/publications/bian/bian_jan_2002.htm.

[29]See, for example, Office of the Secretary of Defense, *Proliferation: Threat and Response*, January 2001, pp. 56–57.

Table 2.1

Comparing Weapons of Mass Destruction[a]

Weapon Type	Size	Lethal Effect	Time to Effect	Area Covered	Potential Fatalities
Nuclear	100 Kt	Blast	Seconds	35 km^2	100,000–320,000
		Fallout	Hours to weeks	~800 km^2	100,000s
Biological (anthrax)	100 kg	Disease	Days	45–300 km^2	100,000–1,000,000+
Chemical (sarin)	1,000 kg	Nerve damage	Minutes	0.7–8 km^2	3,000–80,000

[a]See Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction: Assessing the Risks,* August 1993, pp. 53–54. This reference assumes that nuclear blast effects in excess of 5 psi overpressure are, on average, lethal. The anthrax and sarin areas were offered for three different weather conditions. Based on other sources, these were apparently the areas of 50 percent lethality; some lethality would occur at far greater distances, especially for anthrax. The fallout area was estimated from Samuel Glasstone and Phillip J. Dolan, *The Effects of Nuclear Weapons,* 1977, pp. 427–430. From their table on p. 430, the downwind distance and maximum width were estimated for a 100 rads/hr dose with a 100-Kt weapon; these were then multiplied by each other and by 0.7 to reflect the actual character of the pattern. Potential fatalities are calculated assuming no treatment and 3,000 to 10,000 people living in each kilometer affected, though the fallout and BW effects will likely go well beyond the range of a city and thus much of the area covered will not have a high population density.

sorbed into the ground (after which they can come back out of the ground over a long period of time). Their persistence varies with temperature, wind conditions, and surface absorption rates.

Because of the large areas they affect, these weapons can be force multipliers. To reduce WMD effects, defenders must employ various protections (reasonable ones exist for CBW, but nuclear weapons are harder to defend against). All of these protections reduce the defending force's effectiveness, but adversaries that deploy CBW risk contaminating areas where their own forces are positioned or need to go, which could cause casualties among their own personnel or degrade performance for their forces.

U.S. threats of retaliation against WMD use, such as that made against Iraq in the Persian Gulf War, are often enough to deter adversaries—at least if those adversaries are not more worried about regime survival than about the U.S. threat. However, the large CW

inventories in several countries suggest that some adversaries see using CBW as an operational necessity.[30] They would likely use CBW early, to maximize surprise and devastation, rather than using WMD only to avert final defeat. BW are best employed before an invasion begins because of their long incubation periods; early use (e.g., at D–2) would sicken defenders around the time of D-Day. BW could also be used to cause disruption in a crisis, the adversary seeking to wreak damage while avoiding attribution and thereby escaping retaliation. Yet most adversaries are risk averse, so even a small potential of attributing WMD use to them, associated with the expectation of serious U.S. retaliation, should be sufficient to deter BW use in most circumstances.

A FRAMEWORK FOR RESPONDING TO ASYMMETRIC THREATS

Asymmetric threats pose a quandary for the United States because they threaten U.S. and allied forces, civilians, and interests in diverse ways that are difficult and expensive to counter. This section proposes a framework for responding to asymmetric threats, focusing on responses to CBW threats as an example of the more general problem. The framework is based on two response approaches identified in the 1997 QDR: institutionalizing and internationalizing.[31]

To be effective, responses must be institutionalized. This would require the military to recognize and address all forms of policy—doctrine, strategy, and CONOPs preparation; force structure and equip-

---

[30]For example, North Korea is reported to have 2,500 to 5,000 tons of CW (South Korean Ministry of National Defense, *Defense White Paper, 2000*, p. 86), and Iran apparently has several thousand tons of CW (CIA, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions*, January 1 through June 30, 2000). These inventories are far greater than would be needed for strategic deterrence and regime survival. Because the U.S./South Korean plan for war calls for defeat and destruction of the North Korean regime as well as military conquest of the country, any war would be a total war from the North Korean perspective. As such, North Korea would have little incentive to withhold weapons early in a campaign. See "KBS Reports Plan to Topple Kim Il Sung," *Washington Times*, March 25, 1994, p. 16; and Ranan R. Lurie, "In a Confrontation, 'North Korea Will Definitely Be Annihilated,'" *Los Angeles Times* (Washington ed.), March 24, 1994, p. 11.

[31]William S. Cohen, *Report of the Quadrennial Defense Review*, 1997, p. 49.

ment development; and personnel management and training—something DoD does not do well today. There is no single solution to CBW threats, no "silver bullet" that defeats even any individual threat component, let alone the totality.[32] Responses to even the related CW and BW threats often differ greatly, complicating DoD's ability to institutionalize responses to such threats. Instead, an integrated defense effort must include two elements of response institutionalization: institutionalization through protection and institutionalization through threat management. It must also include internationalization, which entails extending the two elements of institutionalization so as to coordinate with U.S. allies and coalition partners. These three parts of an integrated approach are described in the following sections.

Institutionalization Through Protection

Protection against CBW effects has four components: attack operations (destroying delivery systems before they can be launched), active defenses (destroying delivery systems and their payloads en route), avoidance (maneuvering around contamination or working from places not contaminated), and passive defenses (protecting from contamination). As shown in Figure 2.4 and discussed next, these four components of response currently have limited effectiveness for defeating CBW.

Most adversary CBW and delivery vehicle stocks are so large that attack operations, especially in the face of adversary cover, concealment, and deception efforts, would take a long time to make a large dent in them. Active defenses work well against some CBW delivery means, such as combat aircraft and naval ships. Yet very short-range ballistic missiles (e.g., the CSS-8) can fly under current defenses, and longer-range ballistic missiles (e.g., the NoDong) descend at angles and speeds that pose problems for current systems.

---

[32]That an anthrax vaccine suffices for that specific threat may be largely true (even if some share of the victims still die). But this "solution" ignores the challenge and response cycle: eventually, someone may well defeat the anthrax vaccine. Therefore, the United States needs to seek redundant, robust defenses.

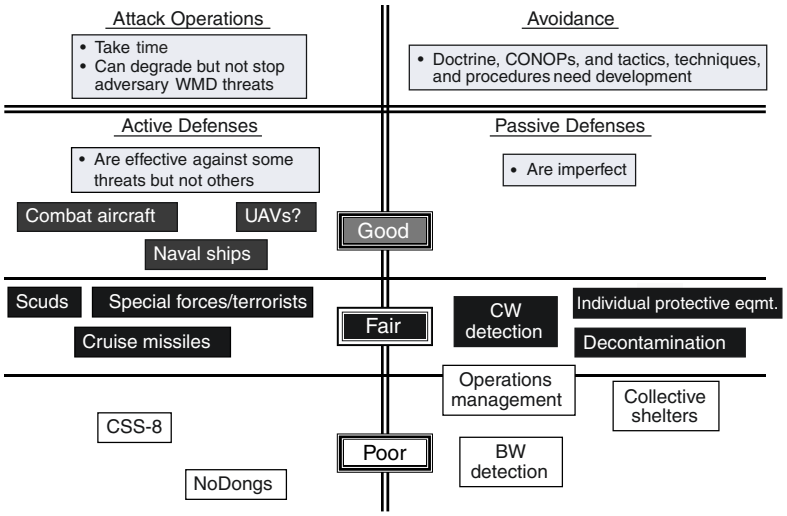

Figure 2.4—Shortcomings of Today's Means of Force Protection Against CBW

Although CBW contamination avoidance can help, the related doctrine, CONOPs, and procedures need more work. Passive defenses against CBW threats provide a fair degree of protection, but only in some cases. Note that attack operations and active defenses work together with avoidance and passive defenses by reducing the amount of chemical and biological material that arrives in the area being defended. The United States is improving its capabilities in all these areas.[33]

All military personnel need to be trained in how to operate in CBW threat and contaminated environments. Today's training is hampered by inadequate doctrine, CONOPs, and procedures; it deals with very short-term chemical threats and tends to neglect biological threats and longer-term chemical threats (partly be denying the latter will take place). Training needs to be broadened to cover the range of CBW threats and to become more universal (all personnel should be

[33]See, for example, the description of the new U.S. protective suit technology in Curt Biberdorf, "CB Protective Field Duty Uniform," *CB Quarterly*, March 2001, pp. 17–18.

trained) so that military personnel think in terms of fighting in a CBW environment.

Similar limitations apply in the case of other asymmetric threats. Protecting against the use of nuclear weapons is even more difficult; it is also difficult to protect against terrorism or attacks on information systems.

Attack Operations. One way to reduce CBW threats is to attack their delivery systems, although large CBW stockpiles and large numbers of delivery systems mean that eliminating them takes time. Destroying CBW on the adversary's territory at least makes the foe suffer most of the consequences, but successful attacks require capable munitions and good information about the threats: what and where they are, and how best to destroy them while controlling collateral damage. Attacking CBW preemptively is difficult because of the risk of collateral damage that can occur in areas surrounding CBW facilities. U.S. planning normally anticipates that attack operations against adversary CBW will not start until the adversary has used some CBW, but this approach requires that the CBW attack be correctly attributed. The United States needs to show that the adversary is, in the end, responsible for the damage because it used CBW first.

For example, say the United States plans to use radar to follow ballistic missile tracks back to their launchers, the goal being to kill launchers before they can pack up and move on. Since most missile launchers have in storage five to 20 missiles, destroying launchers means potentially preventing the launch of multiple missiles. If each launcher in a 50-launcher force has a 20 percent risk of being killed each time it launches (a high level of effectiveness), after 10 launches each (over five to 10 days?), the force will be cut down to five (which is enough to still do some damage). Thus, attack operations take days or weeks to have much effect; they do little to attrite the threat early unless there are only a few launchers and they are left out in the open. Still, anything that reduces launch rates relieves pressure on active defenses (and limits the odds of their being saturated).

Active Defenses. The next component of response against CBW threats is interception of CBW delivery systems en route. Active defenses can include ballistic missile defenses, air defenses, naval

defenses, border guards, and custom agents. They must be matched to the threatening delivery system(s).

The key determinants of an active defense are saturation (how many delivery means can be engaged at one time) and leakage (what percentage get through short of saturation). For example, a Patriot battery with eight launchers (and four missiles per launcher) would be able to engage up to 32 missiles and/or aircraft (the saturation threshold) before reload is needed; if it used two missiles per incoming vehicle, the saturation threshold would be 16 vehicles. If each Patriot missile had a 50 percent probability of killing an opposing ballistic missile, leakage would be 50 percent if only one Patriot were fired per adversary missile, and roughly 25 percent if two Patriots were fired per missile, assuming the kill probabilities were independent of one another.

Beyond saturation and leakage, defenders face other concerns in the challenge and response cycle. A special forces team can more easily destroy a Patriot missile battery than an inaccurate Scud missile can. Adversaries are likely to use combined arms against active defenses, so the United States and its allies need to protect their active defenses. Doing so should let them remove a large fraction—but not all—of the threat.

Avoidance. Force operations can be changed to reduce their vulnerability to adversary CBW threats, even after the United States and its allies develop enhanced defenses. Avoiding contamination is one of the three doctrinal approaches to reducing U.S. vulnerability.[34]

Consider the following analogy. In World War II, the Soviets massed their forces—up to 600 artillery tubes per kilometer—in a breakthrough sector to maximize their ability to penetrate German lines. But in the Cold War, as their vulnerability to U.S. nuclear weapons became clear, the Soviets adjusted their massing factors, eventually settling on artillery densities of about 100 tubes per kilometer in breakthrough sectors. Such a reduced force density complicated breakthrough efforts but prevented a dramatic failure if the opponent targeted the massed forces.

---

[34]Joint Chiefs of Staff, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments*, Joint Pub 3-11, July 11, 2000, p. III-6.

To avoid contamination, eight basic adjustments can be made to force operations:

1. *Density reduction*. Forces can be spread out in depth, more reserves can be provided (to replace forward-most forces suffering serious damage), and fires rather than forces can be massed. Density in the rear can be reduced by spreading forces across more bases.
2. *Standoff*. CBW effects can be avoided if forces perform their missions from bases outside the adversary's range.
3. *Dispersal/evacuation*. Forces and personnel, especially those associated with fixed facilities, can be moved away from likely targets (preemptive dispersal/evacuation), and targets already contaminated (remedial dispersal/evacuation).
4. *Relocation*. CBW effects can be reduced or avoided if forces en route to contaminated bases are rerouted to uncontaminated ones.
5. *Avoiding CBW contact*. All forces can try to be indoors during the 30-plus minutes a cloud of aerosolized CBW is passing through. Forces near or in contaminated areas can use reconnaissance to locate and then avoid or decontaminate such areas. Ground forces can maneuver around contaminated terrain.
6. *Threat avoidance*. Ground forces can mount substantial reconnaissance efforts well in front of advancing forces (perhaps 100 km or so) to discover CBW and their delivery systems and destroy them before they are used.
7. *Sequencing operations*. Standoff operations can be used at the start of a conflict to interdict CBW and their delivery means. Once this task is almost finished, forces can enter the theater in greater numbers to complete operations without facing as high a risk.
8. *Quarantine/travel limitations*. Quarantines prevent or limit the spread of contagious BW. Travel limitations imposed during the incubation period of all BW can prevent the appearance that BW were also used elsewhere (i.e., the limitations keep persons exposed at the original site from appearing to have become infected at another location).

Passive Defenses. The final component is passive defenses, which aim to prevent damage from CBW use or to mitigate CBW damage that has occurred. Preventive measures include detection, protective clothing, collective protection shelters, cleanup of residual effects, and consequence management (medical care, personnel replacements, and public information). Figure 2.5 summarizes the current approaches to passive defense, illustrating differences between the CW and BW approaches. The following paragraphs discuss the various elements of the passive defense process.

CW detectors can detect the threat in time to avoid it, but BW detectors cannot currently do so. Thus, passive defense against CW "detects to protect," though CW effects could occur without detection, especially among a civilian population. The persistence of many CW agents also requires reconnaissance and decontamination to finish the job. Passive defense against BW "detects to treat," in part by determining when and by what agent(s) victims have been affected so as to start treatment as soon as possible. Because BW detectors are few and far between, most BW attacks will be detected only by disease surveillance when victims show up at hospitals and clinics.

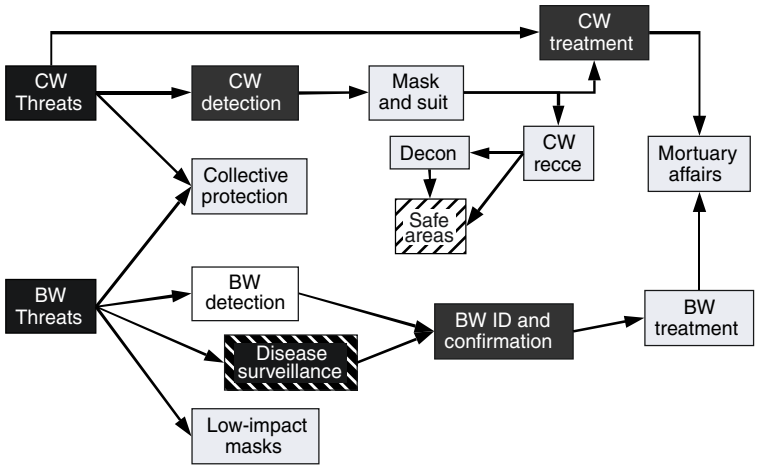

Figure 2.5—Current Passive Defense Efforts

Collective protection keeps CBW out of buildings; it helps those who work indoors avoid exposure. Recent seminars have suggested that it be required in all new construction within potential combat zones. A recent initiative seeks to develop masks that would have less operational degradation than today's CW masks and yet protect against BW (recognizing BW detection limitations) after BW have been used in a theater. CBW medical treatment would be helped by agreements with other governments to provide supplies and specialists, as needed.

Because no single protection suffices, efforts must be combined across them to provide protection packages. Collective protection, for instance, is an ideal defense against CBW for forces that work indoors. If such facilities also have CBW detection, people can be warned to stay indoors when threats loom. By contrast, ground forces in forward units rarely have collective protection against CBW. Masks and suits would be their principal line of defense (plus CBW detection to tell them when to put this equipment on). To avoid overloading their masks and suits, forward units would also maneuver around any contamination they detect by CBW reconnaissance. Reducing the density of forces decreases their value to the adversary as a target and provides reserves to fill holes created by successful adversary attacks. As mentioned earlier, far-forward reconnaissance screens are needed to detect CBW delivery systems and destroy them first.

Although some people working in airfields, ports, and logistics facilities work indoors and can benefit from collective protection, the many people who work outdoors require masks, suits, and CBW detection. In addition, they would be best supported by the use of substantial active defenses—provided by air, missile, naval, and special operations forces (SOF)—to reduce the burden on their passive defenses.

Institutionalization Through Threat Management

The second element of institutionalization is to try to manage asymmetric threats by inhibiting their development in the first place, deterring their use, and mitigating the damage that adversaries seek from them. This element needs to combine prevention, dissuasion, preemption, deterrence, and information operations. While the

focus here is on WMD and, specifically, CW and BW as examples of asymmetric threats, in many ways it will be easier for the United States to manage these threats than other asymmetric threats.

Prevention. It is best to prevent asymmetric threats from being developed or, if this is not possible, to get countries to reduce or destroy them. Most prevention strategies are based on arms control; they assume that agreements can be made and enforced to limit or remove certain classes of threats, as was accomplished by the Strategic Arms Limitations Treaty (SALT) and CFE agreements. It is difficult to enforce or verify agreements covering WMD and ballistic missiles even in the case of signatories, however, and many countries are not signatories. The history of Iraqi resistance to WMD-related sanctions suggests that sanctions are no panacea either.

The Bush administration's emphasis on preventing WMD threats runs into obstacles, in particular the "demand" for WMD:

- *Strategic demand.* While the United States has agreed to give up CBW, it still feels it must possess a significant number of nuclear weapons for legitimate national security reasons, including the threat of reprisals. Many other countries appear to feel the same way, though most have focused on CBW because they are less expensive than nuclear weapons. For many of these countries, WMD are the ultimate guarantor of regime survival. They also stand as a symbol of national power while providing some level of coercive power. The United States has not recognized most countries' possession of WMD as legitimate for these purposes.
- *Operational demand.* A number of countries apparently view possession of WMD as an operational military advantage. This is most obvious in countries such as North Korea and Iran, whose inventories of thousands of tons of CBW are difficult to justify for strategic purposes alone.

It is extremely difficult to get countries with these interests to renounce and destroy all their WMD. The United States has not found alternatives for these strategic and operational needs in most cases, making arms control very difficult, especially with regard to countries already possessing these capabilities.

The United States also has arms control concerns on the "supply" side:

- *Moving to "zero" supply*. While the United States has "done away with" all its BW, it still maintains small stocks of many biological agents for defensive development purposes. Recently, it was revealed that even in the United States, the government construed such defensive purposes to include fairly significant biological production efforts to see what a terrorist or other group might be able to produce.
- *CBW breakout*. With BW, most countries prefer to keep primarily small "seed stocks" because of the dangers of storing large quantities and because large quantities can be grown from smaller ones in days or weeks (it takes longer to weaponize the resulting products). Thus, even if a country accepts a "zero" supply, it may be able to produce a substantial wartime capability within months, given adequate expertise and appropriate facilities. Most CBW production facilities have dual civilian and military purposes. Most or all of their production in peacetime might be for civilian purposes, but this could change with little or no warning and few (if any) observables if the decision to prepare for conflict were made.
- *CBW inspections*. Inspections of potential production and storage facilities are a key means for catching countries that are violating WMD restrictions. But since BW production can be done quickly and covertly, it is extremely difficult to catch violators. (Indeed, the UN experience with Iraq after the Persian Gulf War suggests how difficult this process can be.) Moreover, countries are reluctant to enter agreements requiring inspections because they thus open themselves to espionage against key new bioengineering industries. Concerns in this regard have caused the United States to reject the proposed inspections protocol for the Biological and Toxin Weapons Convention.

If all countries were to move to "zero" WMD, a potential adversary could quickly and with little or no notice produce significant quantities of CBW (especially BW) to create an unacceptable coercive or warfighting advantage. Arms control of WMD thus provides only a

limited ability to prevent WMD threats. Looking beyond WMD, arms control has even less potential for success with other asymmetric threats such as information warfare and terrorism.

Dissuasion, Intelligence, and the Planning Framework. U.S. efforts to dissuade adversaries from developing or possessing certain asymmetric threats depend on an early understanding of the potential threats, the principles of the challenge and response cycle, and the willingness to invest in capabilities that nullify the threats. If, for example, the United States, anticipating that the smallpox virus has been developed for use against U.S. forces, develops and deploys a smallpox vaccine, few if any adversaries will see utility in further virus development, production, or use. But if the United States does not develop, much less deploy, a vaccine until it has firm evidence that several countries already have weaponized smallpox, it loses the opportunity to prevent this threat, and must instead turn to countering it (which also depends largely on the smallpox vaccine).

Traditional defense planning has been threat-based planning, which copes poorly with asymmetric threats. The defense policy and planning community and the U.S. intelligence community have traditionally required confirming evidence of threats before those threats are included in intelligence estimates.[35] The time it often takes to acquire such confirming evidence means that traditional intelligence estimates lag most adversary capabilities by several years; and they lag adversary asymmetric threats by more years because of a lack of emphasis coupled with the normal difficulties of observing such threats. For example, the production and weaponization of BW agents produces very few of the observables that intelligence agencies usually pursue. Even if BW were observed, the United States would have little information about how they might be used. And since U.S. R&D programs have historically been justified based on such established threats, the United States has tended to seriously lag in the challenge and response cycle associated with asymmetric threats.

---

[35]Ironically, DoD usually ignores the opposite requirement: to confirm that an adversary is *not* developing such a threat before excluding the threat from planning.

The answer for DoD is to try to understand the spectrum of potential asymmetric threats and U.S. vulnerabilities to them.[36] Only then can the United States identify potential threats, search for related adversary developments and strategies, and respond to them. This is the essence of the "capabilities-based planning" proposed in the 2001 QDR. The United States can refine this spectrum of threat alternatives based on cultural and other details of the potential adversary.[37] Planning would then seek to respond to a reasonable threat spectrum.

In essence, the dissuasion strategy element calls on DoD to recognize potential threats and to jump on the leading edge of the challenge and response cycle (rather than being on the trailing edge). It takes the threat spectrum identified in capabilities-based planning, prioritizes it based on threat likelihood and seriousness, and focuses on preventing the top priority threats. To prevent serious threats, the United States must be prepared to invest significantly in developing and fielding appropriate threat counters (such as the smallpox vaccine) well before intelligence can confirm the existence of the threats. The United States must then be prepared to describe the counter to the world in order to convince potential adversaries that the related threat is no longer of use.[38]

Preemption. An alternative to two of the forms of prevention, arms control and dissuasion, is preemption—destroying the threat before it can be used or soon after an early use. Many who heard the 2002 State of the Union Address believe that the United States is threatening North Korea, Iran, and especially Iraq with preemption of their WMD if they do not accept WMD arms control. The U.S. national

---

[36]A focus on known threats leaves the United States open to developing threats. Adversaries would logically start military planning from objectives and develop strategies to achieve them—in part by exploiting perceived U.S. vulnerabilities. Planning of U.S. counters would logically start from a similar perspective. Because the United States may not recognize its own vulnerabilities, this effort must be pursued in part by experts who understand U.S. operations and what can be done to counter them.

[37]One example would be North Korea's interest in special forces and weapons they could use effectively (such as BW), as noted above.

[38]The United States should exercise some care in doing so, as the counter it has developed may, in turn, become the focus of adversary searches for vulnerabilities.

security strategy published in September 2002 included strong support for preemption.

Preemption is akin to attack operations, but would be undertaken as a U.S. offensive action before a war existed with the country in question. Nevertheless, such a preemption would likely begin a war; indeed, North Korea has claimed that President Bush's 2002 State of the Union Address was "little short of declaring a war" on North Korea.[39] In the end, the United States would need to (1) justify to the world that the WMD threat warranted a war, and (2) prove to the world that the preemption largely or entirely removed the WMD threat. To satisfy most countries with regard to the first point, the United States will most likely have to do much more in the way of information operations (many countries do not think WMD threats warrant even President Bush's accusations). And as described earlier, in the discussion on attack operations, the United States will have difficulty entirely destroying the WMD (it will take days or weeks, and may not be possible at all). Moreover, attacks on adversary WMD may well force the adversary into a "use it or lose it" mode in which it responds to preemption with WMD use—for which the United States may then be blamed.

Deterrence. Because protection cannot prevent all losses to asymmetric attacks such as CBW, the United States must deter specific CBW uses.[40] Many equate deterrence with an ability to impose unacceptable damage on the adversary (a reprisal), but the 2001 QDR makes it clear that deterrence by denial (preventing CBW attacks from being effective) is the essence of the new U.S. strategy. Deterrence by denial overlaps very heavily with protection, as discussed above. Still, reprisals do have a role, as do post-conflict sanctions. Because reprisals and sanctions with penalties require that a CBW attack be attributed, the United States needs to prepare plans for achieving attribution in the more difficult cases, such as covert use of BW.[41] And because reprisals and sanctions are escalatory, the United

---

[39]Quoted in David R. Sands, "North Korea Assails 'Axis' Label," *The Washington Times*, February 1, 2002, p. 1.

[40]See Donald H. Rumsfeld, "Toward 21st-Century Deterrence," *Wall Street Journal,* June 27, 2001.

[41]Sometimes attribution is easy. Ballistic missiles, for instance, can usually be traced back to their source (though the country's leadership could claim that they did not

States will need an ability to control escalation, as well as clear knowledge of the price that it and its allies are willing to pay to resolve an adversary's CBW threats.

Inasmuch as no country today is using CBW against the United States, deterrence may be said to be working. The risks of CBW use may far exceed the gains to be achieved, given the probability that those gains can be achieved. But terrorists may feel exempt from such assessments. And if state adversaries begin to feel desperate, their deterrence calculation may change. For instance, if the North Korean regime feared that it was going to be overwhelmed by internal opposition, it might invade South Korea to unify its own citizens; CBW might be an integral component of this invasion. Deterring the desperate from using CBW or other asymmetric threats is hard. The United States can try to prevent desperation through aid, and it can try to convince countries that warfare and CBW use will not solve their problems, or even permit them to achieve what they might want. Potential adversaries should be convinced that the more likely outcome from a CBW attack will be disaster from U.S. reprisals and international economic and political penalties.

Information Operations. Any WMD use would be major international news. Adversaries might seek to ward off penalties, such as international sanctions, in many ways: by denying responsibility, by claiming they are responding to earlier WMD use by the United States or its allies, by depicting themselves as David against the U.S. Goliath, and/or by hindering news coverage of the attack. In using WMD against third countries, they may not even need to pursue these approaches. For example, Iraq's use of CW in its 1980s war with Iran provoked little international response.

---

authorize the launch and will punish the perpetrators). But proving the origins of special forces, terrorist groups, or even cruise missiles is difficult. Without confirmation, the United States may be wary of attacking the wrong party and suffering embarrassment and thus may not act. Adversary deception makes attribution even harder. Given, say, a CBW attack against a U.S. base in the Persian Gulf while Iran is acting militarily against U.S. interests, the United States may well assume Iran did it. But Iraq may actually have done it, hoping the United States would blame and then hurt its archenemy, Iran, in reprisal. The resulting change in the regional balance of power may well be worth the risk for Iraq. Better U.S. capabilities for attribution are needed, and a doctrine of presumed responsibility should be considered, as discussed below.

In peacetime, the United States needs to "prepare the information battlefield." It needs to do so by demonstrating that it and its allies have no plans to use CBW and no deployed capabilities (U.S. CBW has been or is being destroyed), and that U.S. adversaries do have substantial CBW stocks, which they plan to use in wartime and which can inflict a level of damage that easily justifies U.S. and allied protection/defensive efforts. Patriot and weapons systems like Patriot need to be clearly characterized as defenses against serious adversary threats even though some countries' psychological operations (PSYOPs) describe missile defenses as offensive systems.

To justify reprisals, the United States needs to prove that U.S./allied forces were attacked by WMD, convincingly demonstrate the attacker's identity, and show that the United States and its allies have not used CBW and thus are not responsible for whatever CBW casualties occurred in the context of U.S. operations. Otherwise, global nonproliferation efforts will be jeopardized. The United States must clearly describe the damage (especially civilian damage) that resulted from the adversary's CBW use if it is to justify not only the postconflict sanctions needed to remove the CBW threats, but also the U.S. reprisals—especially if these were carried out with nuclear weapons.

Achieving these objectives in the face of enemy propaganda will be challenging. It will be critical to set international expectations for wartime objectives. Absent clear attribution of adversary CBW attacks, the United States may have to implement a doctrine of "presumed responsibility" that places the burden of proving innocence on regional adversaries with large CBW inventories.

Finally, consequence management requires that the United States be prepared to describe the character and anticipated consequences of a CBW attack, as well as the procedures (e.g., evacuation, medical treatment, and psychological operations to reduce panic) that need to be undertaken after the event.

Internationalization

The United States must also internationalize its response to asymmetric threats, because it will invariably need the support of allies in future conflicts. DoD must prepare itself to fight alongside allies

against asymmetric threats, sharing equipment and CONOPs with allies until the latter can meet U.S. standards, which most cannot do yet. Current U.S. efforts offer the opportunity to involve allies in formulating CONOPs and equipment R&D, thereby involving them and potentially reducing U.S. costs. Unfortunately, many U.S. efforts to develop counters to asymmetric threats are pursued on a "U.S.-only" basis, constraining and often directly thwarting U.S. efforts to internationalize the results. This is particularly true with regard to the development of new technologies.

Internationalizing the U.S. approach to CBW threats involves the following five elements:

Understanding the Threat. The United States will need to help its allies understand the CBW threat. Much U.S. information is acquired through technological means; the United States can gain much from the human intelligence (HUMINT) and cultural awareness of its regional allies (especially relative to terrorism). The United States must exchange this information with allies systematically and comprehensively, taking into account all concerns about sensitive sources and recognizing the potential unreliability of such information. The United States and its allies might disagree on the relative likelihood of elements across the threat spectrum, but the spectrum itself should be an easy basis for the consensus needed to establish a common background for strategy and planning.

Synchronizing Operations. Most allies lag the United States in developing CONOPS for CBW threats. Once allies appreciate such threats, they generally welcome U.S. ideas for reducing force vulnerabilities, especially when those vulnerabilities can be reduced merely by adjusting CONOPS. Because U.S. allies lack many of the protections against CBW threats, the United States needs to field phased sets of CONOPs that cover situations from minimal protection through well-developed protection. For example, the first thing all airfield workers should do after a CW attack is get indoors and turn off the ventilation systems that could bring in contamination from the outside. Those who have protective clothing should then put it on; those without protective clothing may not be as well protected, but they will survive better indoors than out.

It is important to set operational norms. For example, in a serious CBW environment, forces ought not be committed to frontline roles without protective clothing. Having this restriction mandated in combined planning would help allies see that acquiring such clothing is a priority if their forces are to be included in desired operations.

Sharing Protections. The United States leads most of its allies in developing protections against CBW. Some of these have been made available to U.S. allies,[42] but not all of them have, so most allies will have inferior protection or none at all. The United States should share as many of its protections as it can in order to facilitate combined operations and promote the use of similar tactics, techniques, and procedures. DoD also needs to appreciate how leaving allies less well protected may lead to sharp criticism of the United States in the foreign media. Until allied protection comes up to U.S. levels, the United States should balance the protections—e.g., offer active defenses (such as Patriot) for key allied facilities that have little or no passive defenses. Such acts will strengthen combined efforts and help to secure allied involvement in difficult conflicts.

Coordinating Destruction. In targeting adversary CBW supplies, there must be clear coordination of U.S. and allied military planning to reduce duplicated effort, avoid collateral damage, and minimize contamination that would impair future maneuver or other operations. Such concerns would be particularly important if U.S. nuclear weapons were used in attack operations. Because most CBW are stored underground, U.S. nuclear attacks on them would rely on ground bursts, which generate fallout. Cleaning up this fallout would be expensive and time consuming. Thus, nuclear weapons should be used against targets only where fallout can be avoided or under wind conditions that would deposit fallout in less sensitive areas. Also, the destruction of BW could lead to a spread of contaminants that would require U.S. and allied efforts to quarantine or control travel in the

[42]There are various reasons for not sharing protections with allies: (1) other allies may have helped to develop a protection and may thus be in a position to disapprove its release; (2) a protection that is understood can be countered, so sharing information about a protection with allies makes it more likely that adversaries will find out the details; and (3) some U.S. protections are just too expensive for allies to purchase in sufficient quantity.

affected areas. Finally, because special forces are often the best way to find and destroy CBW stocks and delivery systems, counter-CBW roles for allied special forces need to be developed.

Cooperating to Prevent and Dissuade. Given how hard it is to prevent the development of CBW and their delivery systems, such a task is almost always best performed as a coalition. It is hard for the United States, even as a superpower, to dictate terms to other countries.

Cooperative prevention requires the United States to share with allies a common understanding of CBW threats and their implications. The United States then needs to reach agreements on appropriate objectives for prevention efforts: Can CBW development be completely stopped? If not, what limits are achievable? What must be done to achieve these objectives? How well can prospective adversaries hide or otherwise conceal their CBW efforts? In this regard, the U.S. experience with Iraq is discouraging and suggests that it will be difficult to prevent CBW developments without some degree of cooperation from the countries under suspicion.

CONCLUSIONS

Adversaries are unquestionably pursuing asymmetric threats to counter U.S. and allied military power. U.S. and allied responses are limited by adversary efforts to conceal these developments, forcing the United States to deal with a very uncertain threat spectrum. Dealing with such threats requires an approach having many dimensions—not least of which are forces and CONOPs to sustain military operations against asymmetric threats and to prevent or counter the surprise and operational disruptions that adversaries will seek to achieve.

Because asymmetric threats are diverse and ever-changing, challenge and response cycle analysis seeks to keep U.S. responses ahead of the cycle's curve. Finally, key capabilities, such as the ability to attribute attacks and control escalation, need more attention from U.S. planners.