Reflections on Future War

Mackubin Thomas Owens
Part of preparing for war is to understand it. What is the nature of war? What is the character of war? Will war in the future be like war in the past? These are critical questions that today’s military professional must attempt to answer. Unfortunately, our track record is not very good. To envision the future is to “look through a glass darkly.” A case in point is the debate that took place a decade ago in the wake of the Cold War’s end and Operation DESERT STORM, the first Gulf War, of 1991.

BACK TO THE FUTURE: THINKING ABOUT WAR DURING THE 1990S

During the 1990s, some argued that the age of war had finally come to an end. These “international optimists” claimed that the collapse of the Soviet Union and the subsequent globalization and increasing interdependence of the international system had converged with the recognition of the destructiveness of modern war to render the idea of large-scale, interstate conflict more or less unthinkable. They contended that while small-scale strife remained a possibility, it could be curbed by means of preventive diplomacy and cooperative structures based on liberal principles. This view prevailed during much of the Clinton administration.

Others argued that the future would not be that different from the past, that indeed the causes of war remained the same as during the time of Thucydides—“fear, honor, and interest”—and that therefore “bad times [would] return.” For example, Colin Gray predicted then, and continues to argue today, that the future security environment will feature the
reemergence of great-power politics, regional nuclear wars, and traditional ter-
ritorial conflict.³

Still others contended that while conflict was still possible, it would differ
from war in the past. This view took two forms. On the one hand were the tech-
nological optimists, who believed that the United States could maintain its domi-
nant position in the international order by exploiting the “revolution in military
affairs” (RMA). On the other were the technological pessimists, who rejected the
idea of a technological El Dorado, a “golden city of guaranteed strategic riches.”⁴

The rapid coalition victory over Saddam Hussein that drove Iraqi forces out
of Kuwait led some influential defense experts to argue that emerging technolo-
gies and the RMA had the potential to transform the very nature of war. One of
the most prominent advocates of this position was Admiral William Owens, vice
chairman of the Joint Chiefs of Staff from 1994 to 1996, who contended that
these emerging technologies and “information dominance” would eliminate
“friction” and the “fog of war,” providing the commander and his subordinates
nearly perfect “situational awareness,” thereby promising “the capacity to use
military force without the same risks as before.”⁵ Owens argued that “technology
could enable U.S. military forces in the future to lift the ‘fog of war.’ . . .
[B]attlefield dominant awareness—the ability to see and understand everything
on the battlefield—might be possible.”⁶ Furthermore, “if you see the battlefield,
you will win the war.”⁷

A publication of the National Defense University fleshed out this claim. “In
short,” it said, “we will move from a situation in which decision making takes
place under uncertainty, or in the presence of incomplete and erroneous infor-
mation, to a situation in which decisions are made with nearly ‘perfect’ informa-
tion.”⁸ The chief of staff of the Air Force at the time echoed this view, saying, “In
the first part of the 21st century, you will be able to find, fix or track, and tar-
get—in near real-time—anything of consequence that moves or is located on
the face of the Earth. Quite frankly, I can tell you we can do most of that today.
We just can’t do it in real-time.”⁹

Those who made this argument were essentially arguing that the classic
Clausewitzian trinity of primordial violence, chance and probability, and the
subordination of war to policy had been superseded by a new technological trin-
ity: intelligence, surveillance, and reconnaissance (ISR) technologies; advanced
command, control, communications, and computer (C4) systems; and preci-
sion strike munitions. During the 1990s, the technological optimists prevailed.
The collapse of the Soviet Union and the rapid U.S. victory in the first Gulf War
gave rise to an era of strategic optimism. Analysts concluded that because of its
edge in emerging technologies, especially information technologies, the posi-
tion of the United States in the world was unassailable for the foreseeable future.
At the same time, there was no “peer competitor” on the horizon capable of replacing the Soviet Union as an existential threat.

This apparent national security situation led U.S. planners in many cases to adopt simplified—if not simplistic—defense-planning assumptions:

- Challenges to U.S. security would arise primarily from regional powers and involve regional/theater contingencies featuring conventional major combat operations (MCOs).
- These likely adversaries would be smaller, less capable versions of the USSR.
- The American monopoly in strike, information technology, and stealth would constitute a barrier to entry for adversaries and would continue into the foreseeable future.

These assumptions led to major changes in U.S. force structure, including the “conventionalization” of the U.S. strategic bomber force and a shift in the focus of space and C3I* programs from the strategic level to the operational/technical level. Planners assumed that since future wars would be short, “strategic speed” had become critical. Thus joint planners stressed such concepts as “rapid halt,” “rapid decisive operations,” and “shock and awe.” One consequence of this perspective was a lack of focus on “phase V” operations: security, stabilization, transformation, and reconstruction.

The technological pessimists, on the contrary, rejecting the prevailing optimism, claimed that America’s technological edge would be of little use in dealing with the most likely future security environment, one in which conflict characterized by brutal, nasty, and merciless ethnic and religious warfare, large-scale banditry and the reemergence of the “warlord,” and transnational crime and terrorism would be the order of the day. They argued that the United States was ill prepared for the most likely conflicts of the future. While preparing for the wars it wished to fight—large-scale interstate wars for which it possessed unmatched capabilities—it ignored the conflicts that it would have to fight, those forced on it by the asymmetric strategies of future adversaries. Other rejected the claim that information “dominance” is sufficient in and of itself to provide the winning edge in future wars.

In early 1996, Colonel (now Major General) Charles Dunlap, USAF, wrote a remarkably prescient critique of the technology-as-panacea vision of future war that then dominated the Pentagon. In his article, entitled “How We Lost the High-Tech War of 2007: A Warning from the Future,” Dunlap imagines a future speech by an enemy leader explaining how his movement had used

* Command, control, communications, and intelligence.
“asymmetric” means to negate American technological superiority—indeed, had used information technology itself against the United States: “Praise the One Above, the microchip ended the educational and training advantage the American military had enjoyed.”

This enemy had also employed “information warfare” to defeat the United States. “We were confident we could influence the American public and its poll-sensitive decision-makers. . . . Thus it became part of our strategy to capitalize on television’s power to influence decision-makers by aiming to wage war in the most brutal—and public—way.” In Dunlap’s telling, this enemy even purposely detonates a nuclear device on its own holy city and then blames it on the United States. In retaliation for this purported American atrocity—which, of course, turns the international community against the United States—the enemy deliberately and viciously mutilates female POWs, subsequently returning them to the United States as part of an information campaign. “In no way did we try to hide what we did; to the contrary, we advertised it—using video clips on the Internet—as a warning of things to come.”

In this fascinating excursion into the future, Dunlap imagines a number of techniques that have become reality, now being employed by our enemies against us in Iraq and elsewhere. “America too often assumed that the [RMA] would favor technologically advanced nations like herself. She failed to consider how enemies with values and philosophies utterly at odds with hers might conduct war in the information age. Despite what many technology-infatuated strategists thought in 1995, cyberscience cannot eliminate the vicious cruelty inherent in human conflict.”

THINKING ABOUT FUTURE WAR

While the American experience in Iraq and other episodes of the “Long War” have failed to validate the more extreme claims of the technological optimists who largely dominated the debate in the 1990s, those claims continue to exert substantial influence on the debate. Indeed, it seems clear that the vision of the technological optimists essentially underpinned the efforts of President George W. Bush’s first secretary of defense, Donald Rumsfeld, to “transform” the U.S. military from a Cold War force to one that would be more responsive to the demands of the post–Cold War security environment. But is this the correct vision of future war, and should it constitute the primary guide for U.S. strategists and force planners?

In attempting to answer this question, it is important to recognize that, as the discussion above illustrates, planners do not have a stellar record when it comes to predicting the future. Indeed, as Loren Thompson of Washington’s Lexington Institute has observed, the United States has suffered a major strategic surprise on the average of once a decade since 1940.
In 2005, Secretary Rumsfeld issued *The National Defense Strategy of the United States of America*, which breaks the challenges that the United States may face in the future into four categories: *traditional, irregular, catastrophic, and disruptive*. The first is almost always associated with states employing armies, navies, and air forces in long-established forms of military competition. The second category describes the use of insurgency and other such approaches to erode American influence, patience, and political will. The insurgent threat in Iraq and Afghanistan is, of course, an example of irregular warfare.

The third category describes the troublesome nexus of transnational terrorism, proliferation, and problem states seeking weapons of mass destruction (WMD). The fourth category is concerned with possible revolutionary technologies and technological breakthroughs—such as biotechnology; cyber operations; space operations, including space-based weapons; or directed-energy weapons—that can exploit U.S. vulnerabilities and counter current advantages.

Critics of Defense Department investment categories argue that the Pentagon spends too much on systems for the arena in which the United States already is dominant—traditional threats—and not enough on the others, especially the irregular category. Critics observe that even as the war in Iraq was shifting to an insurgency, the Department of Defense issued its *Transformation Planning Guidance* (2003), a document that purported to provide a template for transforming the Cold War military into

> information age military forces [that] will be less platform-centric and more network-centric. They will be able to distribute forces more widely by increasing information sharing via a secure network that provides actionable information at all levels of command. This, in turn, will create conditions for increased speed of command and opportunities for self-coordination across the battlespace.

Critics claim that this proves that the Pentagon does in fact seek a technological El Dorado.

A counterargument to the prevailing techno-centric view has been advanced by those who espouse “fourth-generation warfare” (4GW). For instance, in *The Sling and the Stone*, T. X. Hammes argues that the Pentagon’s emphasis on high-tech warfare has prevented the U.S. military from adapting to a style of warfare in which guerrillas and terrorists employ low-technology tactics to counter American strengths and exploit American vulnerabilities.

According to its advocates, the goal of fourth-generation warfare is to convince the enemy that its strategic objectives are unachievable at acceptable cost. The methodology of 4GW is to use all available networks—political, economic, social, and military—to attack directly the will of the enemy. Hammes contends that 4GW has been the most successful form of warfare of the last half-century,
defeating the United States three times (Vietnam, Lebanon, and Somalia), the Soviet Union/Russia twice (Afghanistan and Chechnya), and France twice (Indochina and Algeria). Indeed, only 4GW, he argues, has succeeded against superpowers. Despite this, discussion of what Hammes calls 4GW has been largely absent from the debate within the Defense Department.

WHAT’S NEW?
As skeptics predicted and events such as 9/11 and Iraq have demonstrated, adversaries have adapted to American power by adopting asymmetric responses to U.S. advantages. The result has been the emergence of trends that undermine the older planning assumptions and require a rethinking of the character of future war.

Driving Forces and Areas of Future Military Competition
Several years ago, Peter Schwartz outlined a methodology for thinking about the future. He suggested that planners can best understand the emerging security environment by positing scenarios based on an assessment of driving forces, predetermined elements, and critical uncertainties. The first category—assessing future trends—is really the key to the methodology.

What are the dominant emerging trends in the security environment? They include—but are not limited to—the proliferation of militarily useful technology; unlimited access to information technologies, including lightweight movie cameras, cell phones, portable laptop computers, and satellite modems that ensure that everyone (including adversaries) has the capability to deliver images of conflict in real time; and aspects of globalization that permit terrorists and other armed groups to employ cheap means to achieve costly effects by exploiting the vulnerabilities of advanced, especially liberal, societies.

Indeed, the changing cost equation may be the most consequential trend of all. During the Cold War, the United States possessed a decided cost advantage in its competition with the Soviet Union. The Reagan administration took advantage of this by adopting an asymmetric and cost-incurring strategy to exploit the mismatch between the large and growing American economy and the much smaller Soviet economy. This cost-incurring strategy forced the USSR to expend resources the Soviet economy could not afford. The combination of the U.S. defense buildup, support for anti-Soviet forces in Afghanistan, and such programs as the Strategic Defense Initiative, which threatened to render obsolete or even obsolete the Soviet nuclear arsenal, was more than Moscow could withstand.

As Donald Rumsfeld acknowledged in 2003, this advantage has dissipated. “The cost-benefit ratio is against us! Our cost is billions against the terrorists’ cost of millions.” In fact, Rumsfeld understated the cost ratio. John Robb
contends that on 9/11 “a $250,000 attack was converted into an event that cost the United States over $80 billion (some estimates are as high as $500 billion).”

Another important aspect of thinking about the future is making educated guesses about the types of military competition that may take place in the future. Examples include power projection versus antiaccess strategies, “hider” versus “finder,” and precision strike versus active defense. We can also expect greater competition in space and cyberspace. Indeed, adversaries will seek the capability to launch difficult-to-detect electronic or information attacks from great distances.

Another emerging military competition involves countering the threat of attack on the homeland from either a large peer competitor or from terrorists who are able to wield much greater destructive power than in the past. To deal with the former, the United States must be prepared to counter “traditional” threats—for example, ballistic- and cruise-missile attack, which may occur with substantially less warning than was anticipated only a few years ago. Addressing the latter requires the capability to counter terrorists or other armed groups who may well gain access to chemical and biological weapons.

Changing Character (Not Nature) of War

As noted above, it was not unusual during the 1990s for planners to claim that emerging technologies had changed “the very nature of war.” But it seems clear that the nature of war—as best described by the Prussian “philosopher of war,” Carl von Clausewitz—remains constant. Clausewitz reminds us that war is a violent clash between opposing wills, each seeking to prevail over the other. In war, the will of one combatant is directed at an animate object that reacts, often in unanticipated ways. This cyclical interaction between opposing wills occurs in a realm of chance and chaos. He also identified as the enduring characteristics of war the persistence of “general friction” as a structural component of combat, the seeming impossibility of eliminating uncertainty, and the critical importance of “moral factors.”

On the other hand, the “character” of war is infinite. Thus a weaker adversary can adopt various modalities of war to engage and defeat a stronger power. Success in war has traditionally gone to the more adaptive side, the one that can bear the costs of the conflict relative to what Clausewitz called “the value of the object.” Accordingly, the record shows, the materially weaker side has prevailed in a conflict in a surprisingly large number of instances—around 40 percent of the time since World War II.

As Philip Bobbitt has observed, for five centuries it has taken the resources of a state to destroy another state. Only states could muster the huge revenues, conscript the vast armies, and equip the divisions required to threaten the survival
of other states. Indeed, meeting such threats created the modern state. In the past, every state knew that its enemy would be drawn from a small class of nearby potential adversaries with local interests. But because of globalization, global reach, advances in international telecommunications, rapid computation, and methods of mass destruction, this is no longer true.\(^{28}\)

**The Emerging Security Environment**

The present and still evolving security environment exhibits a number of characteristics that affect the character of war and will most likely continue to do so in the future. These include such phenomena as expanded global interdependence, which although seen as a boon to globalization, also permits terrorists and other violent ideologues to inflict damage at very low cost and risk to themselves. In the words of Shamil Basayev, a Chechen commander and mastermind of the Beslan massacre, “We are not bound by any circumstances, or to anybody, and will continue to fight as convenient and advantageous to us and by our rules.”\(^{29}\)

Citing this passage, John Robb observes that “this new method of warfare . . . offers guerrillas the means to bring a modern nation’s economy to its knees and thereby undermine the legitimacy of the state sworn to protect it. Furthermore, it can derail the key drivers of economic globalization: the flow of resources, investment, people, and security.” Those who adopt this form of warfare, says Robb, are not really terrorists but *global guerrillas*, who represent “a broad-based threat that far exceeds that offered by terrorists or the guerrillas of the past.”\(^{30}\)

Such global guerrillas are able to exploit the dissonance caused by “spikey” economic development and urbanization, the diffusion of and impact of technology (especially information technology), and the dislocation caused by globalization and demographic bulges. They are able to effect “systems disruption” in advanced economies, by causing “cascading” failures in the system: “If attackers can disrupt the operations of the hubs of a scale-free infrastructure network, the entire network can collapse in a cascade of failure.”\(^{31}\)

Because of interdependence, furthermore, failures within a single network can cause the failure of others. In a tightly interconnected infrastructure, not only do the transportation network, the water network, and the fuel network depend on the electricity network, but the electricity network depends on the fuel and transportation. “Global guerrillas have proven to be increasingly adept at using these interconnections to cause cross-networks of failure.”\(^{32}\)

**Categories of War: Multidimensional Conflict**

The categorization of war—*traditional, irregular, catastrophic, and disruptive*—by the 2004 Defense Strategy and the Quadrennial Defense Review represents an advance in thinking about future war, but it implied that adversaries
would focus on only one category. War, however, properly understood, is always multidimensional. In a past dominated by state-on-state warfare, the traditional or conventional category was central, but combatants also pursued strategies to exploit irregular capabilities, such as guerrilla warfare and insurgency, or disruptive—attempts to undermine an enemy’s public support for the war, by, say, acts of terrorism. But a particular form of multidimensional warfare may constitute the most demanding challenge to American planners in the future: “complex irregular warfare” (CIW).

One characteristic of CIW is the likelihood that future adversaries will be “hybrids.” These hybrid threats will seek to raise the potential cost of U.S. military action by adopting aspects of all of the warfare categories. An example of a prototype hybrid is Hezbollah. During the 2006 war with Israel, Hezbollah exhibited both statelike capabilities—long-range missiles, antiship cruise missiles, sophisticated antiarmor systems, armed unmanned aerial vehicles, and signals intelligence—while still skillfully executing guerrilla warfare. Such a hybrid has the potential to complicate future U.S. military planning and execution. Hezbollah was able to stand up to the Israel Defense Forces (IDF) because it was able to adapt skillfully to the particular circumstances that it faced. For instance, unlike U.S. forces, which must be prepared to fight in a variety of environments and under various conditions, Hezbollah was able to tailor its forces specifically to counter the IDF. Since Hezbollah did not have to organize for offensive operations, it was able to concentrate on defense in depth.

With decades of experience in low-intensity conflict with the IDF, Hezbollah understood its enemy’s strengths and vulnerabilities. The IDF’s ground forces remain structured for swift, conventional thrusts toward Damascus or Cairo. So Hezbollah leaders didn’t attempt to build traditional brigades or battalions equipped with armored vehicles—the classic Arab error. Instead, they concentrated on stockpiling the most sophisticated defensive weapons they could acquire, such as the Kornet, a lethal late-generation Russian antitank missile, as well as a range of rockets, from long-range, Iranian-made weapons to man-portable point-and-shoot Katyushas. Thanks to the Katyushas, an Arab military force was able to create a substantial number of Israeli refugees for the first time since 1948.

Hezbollah exhibited flexibility by fielding modular units and adopting mission-type orders. It was effective in its innovative use of weapons. Although most Hezbollah fighters did not seek death, the organization was willing to accept casualties. Hezbollah was perfectly willing to accept a loss ratio of about five of its fighters to one IDF soldier. Hezbollah’s intelligence performance was surprisingly effective. As Ralph Peters has observed, “Israel fought as a limping stepchild of Clausewitz. Hezbollah fought as Sun Tzu’s fanatical son.”
As suggested above, the sort of hybrid threats generated by CIW and illustrated by Hezbollah may well constitute the most probable, most demanding, and potentially most costly type of future conflict. Implications of wars against hybrid threats include the likelihood that they will be extremely lethal and protracted and the prospect that since they will often take place in contested urban zones (“feral cities”), they will be manpower intensive. They will be widely distributed by distance, complexity, and mission. In most cases, these hybrid threats will seek to win the war of perceptions, waging a “conflict among the people.” To prevail against such a threat requires “cultural intelligence” and exploitation of the “human terrain.”

The operational environment in such conflicts very likely will be characterized by close encounters between friendly forces and an enemy that seeks to blur the distinctions between the conventional and the unconventional, between combatants and noncombatants, between conflict and stability operations, and between the physical and the psychological. After all, hybrid war is a competition for influence and legitimacy, in which perceptions are paramount. As the current conflict in Iraq illustrates, in the battle for legitimacy religious identity may trump or negate better governance and economic benefits.

In general, hybrid foes utilizing complex irregular warfare will attempt to exploit the political effects of a conflict, seeking to undermine the legitimacy of U.S. military actions. Thus these enemies will try to leverage “lawfare,” the use of the rules of warfare against the United States (while ignoring these rules themselves), by, for example, taking refuge among the civilian population in an attempt to maximize civilian casualties. In turn, adversaries employing CIW will take advantage of the fact that such casualties are magnified by the proliferation of media assets on the battlefield. Again, CIW is above all a battle of perceptions. As Lawrence Freedman has observed, “In irregular warfare, superiority in the physical environment is of little value unless it can be translated into an advantage in the information environment. . . . Our enemies have skillfully adapted to fighting wars in today’s media age, but for the most part we, our country, our government, has not.”

**Preempting Preemption**

The best way to counter such threats is through preemption. To do so, the United States needs to establish favorable conditions for access, including a flexible forward-basing posture and an effective means to counter the asymmetric antiaccess strategies that hybrid opponents are likely to adopt. Such strategies would be designed to undermine the cornerstone of American global military power: the ability to project and sustain substantial military forces at great distances from the continental United States. In general, there
are four points at which an adversary may attempt to derail U.S. power projection.

First, as the United States is deciding to project power, an adversary may attempt to deter it by threatening actions that would make the cost of power projection too high, perhaps attacking targets in the homeland in order to undermine public support for an overseas intervention. Second, as the United States is deploying its forces to ports and airfields, an adversary may attempt to disrupt the deployment by terrorist attacks and sabotage of transportation means and the like. Such attacks in both of these phases would force the United States to use forces intended for power projection to defend against attacks at home.

Third, as the United States is transporting its forces to the theater of action and attempting to debark, an adversary will try to deny entry by military and political means—say, attacks and threats against allies in the region. Finally, as U.S. forces establish a lodgment and begin offensive operations, an adversary will seek to defeat them.

In the past, adversaries have focused their efforts on the last two points, denial and defeat. But in the future, an adversary's most cost-efficient actions may be to deter and disrupt the projection of U.S. forces. This possibility is the result of another emerging characteristic of future conflict, “360-degree warfare.” Past wars have usually been characterized by the existence of “fronts” and secure “rear areas,” whether at the strategic, operational, or tactical level. Of course, airpower provided a means of attacking the enemy’s rear, and long-range airpower and missiles threatened to extend the ability to attack the rear to the homeland. Nonetheless, actual attacks against the strategic rears of both sides were deterred by the likelihood of mutual destruction.

Guerrillas, insurgents, terrorists, and other armed groups have long sought to wage “war without fronts,” but the strategic emergence of true 360-degree warfare is a recent development. The 9/11 attack indicated that the ability of the United States to deter attacks against its homeland is no longer assured. Iraq and Afghanistan illustrate that our adversaries have adopted this approach at the operational and tactical levels of war as well. Thus multidimensional war in the future is likely to be characterized by distributed, weakly connected battlefields; unavoidable urban battles and unavoidable collateral damage exploited by the adversary’s strategic communication; and highly vulnerable rear areas. On such battlefields, friends and enemies are commingled, and there is a constant battle for the loyalty of the population. All of this is exacerbated by the proliferation of militarily useful technology, including nuclear weapons and delivery systems.
A Large Peer Competitor?
Some contend that the American intelligence community during the 1990s and the early 2000s was so focused on the rise of China to great-power status that it was blind to the threat that manifested itself on 11 September 2001. But has the pendulum now swung too far to the other extreme? Are we now so fixated on counterinsurgency and terrorism that we will not take the steps necessary to counter the military of a “large peer competitor?”

The leading candidate for the role of future peer competitor is China. According to the Department of Defense's annual report to Congress on Chinese military power,

much uncertainty surrounds the future course China’s leaders will set for their country, including in the area of China’s expanding military power and how that power might be used. The People’s Liberation Army (PLA) is pursuing comprehensive transformation from a mass army designed for protracted wars of attrition on its territory to one capable of fighting and winning short-duration, high-intensity conflicts against high-tech adversaries—which China refers to as “local wars under conditions of informatization.” China’s ability to sustain military power at a distance, at present, remains limited but, as noted in the 2006 Quadrennial Defense Review Report, it “has the greatest potential to compete militarily with the United States and field disruptive military technologies that could over time offset traditional U.S. military advantages.”

The report states that China’s economic growth has permitted it to accelerate the pace and scope of its military transformation. “The expanding military capabilities of China’s armed forces are a major factor in changing East Asian military balances; improvements in China’s strategic capabilities have ramifications far beyond the Asia Pacific region.” China has enhanced its strategic strike capabilities and pursued a robust counterspace program, “punctuated by the January 2007 successful test of a direct-ascent, antisatellite weapon.” Thus its continued pursuit of area-denial and antiaccess strategies has expanded from “the traditional land, air, and sea dimensions of the modern battlefield to include space and cyber-space.”

The case of China illustrates that hybrid warfare is not only a phenomenon associated with the “low end” of the spectrum of conflict. There is no reason that a future peer competitor would restrict military competition with the United States to the “traditional” category alone. It would logically also try to confront the United States asymmetrically in those areas where the United States is perceived to be less capable than in the traditional category. The publication in China several years ago of Unrestricted Warfare indicates the potential of hybrid complex irregular warfare at the “upper end” of the spectrum of conflict.
THE FUTURE OF FUTURE WAR

As the foregoing discussion illustrates, any future adversary, whatever his preferred mode of warfare, will at a minimum attempt to employ all the dimensions of warfare to counter critical U.S. military capabilities asymmetrically in such areas as conventional warfare, force projection, C4ISR (including space operations), and precision strike.

In the area of irregular warfare, opponents will attempt to impose untenable costs on the United States by using time-tested techniques against superior force, threatening a protracted war of attrition to undermine domestic public support, raising the level of violence and brutality, and expanding and escalating the conflict by targeting the U.S. homeland and those of its key allies. In the area of power projection, opponents will attempt to raise the cost of access by increasing the risk to the United States of naval and air operations, by, in turn, expanding the area of a “contested zone,” seeking to destroy high-value assets—for instance, aircraft carriers—dissuading allies and partners from providing bases and other forms of support to U.S. forces, and degrading the ability of the United States to deploy forces into an area of interest.42

In the area of C4ISR, adversaries will attempt to “bring down the network” by attacking American space assets, degrading information systems, disrupting command and control, denying surveillance and reconnaissance, and deceiving intelligence. In the area of precision strike, the enemy will seek to reduce stand-off range, spoof guidance systems that enable precision attack, and disperse targets, including into populated areas. All of these methods have already been employed by adversaries; they represent manifestations of the changing cost equation that will likely make it more difficult for the United States to use military force in the future.43

The best way to think about the future is not to try to predict it but to project a number of plausible alternative futures against which to test strategies and force structures. To do so, planners must develop a representative—not exhaustive—set of plausible contingencies that encompass the principal challenges the military might encounter “over the planning horizon” (more than fifteen to twenty years out). This approach is particularly relevant to the United States, which, given its global responsibilities, must be prepared for a variety of contingencies across the entire range of military operations.44

Andrew Krepinevich has suggested a useful methodology for addressing areas of future military competition—the reintroduction of the concept of “color plans” reminiscent of those the United States employed during the interwar period.45 His scenarios include

- China (disruptive peer) (Plan YELLOW)
• North Korea (nuclear rogue) (Plan RED)
• Pakistan (failed nuclear state) (Plan GREEN)
• Radical Islam (Plan PURPLE)
• Global energy network defense (Plan BLACK)
• Global commons defense (Plan ORANGE)
• Nuclear/biological homeland attack (Plan BLUE).

These illustrative scenarios seek to identify a representative array of contingencies encompassing the principal military challenges U.S. planners may confront over the planning horizon. As such, they presumably enable strategists and force planners to hedge against uncertainty by testing concepts of operations and force structures against plausible alternatives—not the most familiar ones or the contingencies believed to be the most likely—permitting planners to assess realistically the potential impact of a range of possible futures on relative military effectiveness.46

General James Mattis, USMC, the new commander of U.S. Joint Forces Command, who also has responsibility for transformation, hit the nail on the head when he remarked several years ago, “We are not likely to get the future right. We just need to make sure we don’t get it too wrong.” One way to ensure that we do not get the future “too wrong” is not to confuse the nature of war—which is immutable—with the character of war—which is infinitely variable. In thinking about future war, planners cannot afford to make this mistake.

NOTES
7. William A. Owens, speech before the Navy RMA Roundtable (Center for Naval Analyses, 5 May 1997). Cf. also Arnold Beichman,


13. Although no mention is made of the religion that this leader professes, his speech adumbrates the sort of rhetoric favored by Osama Bin Laden and other Islamists after 9/11. Of course, in 1996 few Americans outside of the intelligence community had ever heard of Bin Laden.


19. Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, Minn.: Zenith, 2004). In Hammes’ metahistory, the first three generations of war were 1GW—the era in which the tactics of the line and column were employed to mass manpower at the point of the main effort; 2GW—the era of massed firepower arising from advances in weapons technology (rifled muskets, breechloaders, machine guns, and indirect-fire artillery) that shifted the advantage from the offense to the defense; and 3GW—the era of maneuver warfare, which permitted the offensive to reclaim the ascendancy it lost during the second generation of warfare.

Hammes’ metahistorical excursion is unpersuasive and is not really necessary to his argument. His critique of the Pentagon’s emphasis on high-tech warfare does not depend upon it. The idea of clearly identifiable generations of warfare obscures rather than clarifies the true evolution of war and its implications for future defense policy. To begin with, one form of war does not arise directly from its predecessor and eventually displace it, as Hammes implies. Instead, advances in warfare usually develop in parallel: firepower was as important during the era of so-called third-generation warfare as it was in the second.

In addition, Hammes conflates the strategic and operational levels of war by portraying the first three “generations” of war in terms of military methods and operational concepts, viz., massed manpower, firepower/attrition, and maneuver, while describing “4GW” as an approach that applies the full panoply of means during war—information, cultural, social, religious, economic, and political as well as military—something states have been doing since at least the eighteenth century. In addition, insurgency and unconventional warfare, which lie at the heart of Hammes’ concept of 4GW, predate 2GW and 3GW. During the first part of the nineteenth century, both Carl von Clausewitz and Baron
Antoine-Henri de Jomini addressed the nature of insurgency.

20. A number of the points developed by the author in this section were incorporated into The Future of War as We Know It, the final report of the “Future of War” panel of the 2007 Defense Science Board Summer Study, on which the author served.


23. Donald Rumsfeld, ”War on Terror Memo,” USA Today, 16 October 2003.


27. The Future of War as We Know It, p. 29.


31. Ibid., p. 102.

32. Ibid., p. 103.

33. See, for example, Frank Hoffman, “Complex Irregular Warfare: The Next Revolution in Military Affairs,” Orbis (Summer 2006).


38. Cited in King, ”Hybrid War.”


41. Qiao Liang and Wang Xiangsui, Unrestricted Warfare: China’s Master Plan to Destroy America (Los Angeles: Pan American, 2002).

42. The Future of War as We Know It, pp. 17, 56.

43. Ibid., pp. 57–58.

