Foreign Policy Research Institute

E-Notes

A Catalyst for Ideas | *Distributed via Fax & Email and Posted at www.fpri.org* | January 2008

AMERICA'S "LONG WAR(S)"

by Mackubin Thomas Owens

The 2006 *Quadrennial Defense Review Report* asserted that the United States is engaged in a "long war" against Islamic terrorism, a war that is now centered in Iraq, Afghanistan, and potentially a nuclear Pakistan. Containing violent Islamic extremism, however, is just one of several challenges the United States will face in the future. Others include nuclear-armed regional powers like North Korea, growing security competition in Asia, especially the growing power of a rising China; and a Russia that is increasingly both authoritarian and assertive. Accordingly, the United States must prepare for a variety of contingencies in the future, and planners must think in terms of not just one, but several, long wars.

In *The Art of the Long View: Planning for the Future in an Uncertain World* (1991), Peter Schwartz 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 the key to the methodology. Driving forces affecting the security environment include globalization; terrorism and irregular warfare; ideological and religious extremism; the proliferation of ungoverned spaces; the rise of China and India and the reemergence of an assertive Russia; competition over natural resources, especially water and energy; changing demographics (a "youth bulge" and aging populations); environmental issues such as climate change and natural disasters; the proliferation of militarily useful technology; information technologies that give everyone—including adversaries—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. As former Secretary of Defense Donald Rumsfeld acknowledged in 2003, this advantage has dissipated. "The cost-benefit ratio is against us! Our cost is billions against the terrorists' costs of millions."[1] 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)."[2]

We also need to make an educated guess about the types of military competition that may take place in the future, including power projection vs. anti-access strategies; "hider" vs. "finder;" and precision strike vs. active defense.[3] We can expect greater competition in space and cyber-space, as adversaries seek the capability to launch difficult-to-detect electronic or information attacks from great distance.

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, e.g. 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 OF WAR

It is now clear that the emerging technologies of the 1990s have not changed the very nature of war, as many claimed they would. War remains, as Carl von Clausewitz described it, a violent clash between opposing wills. The enduring characteristics of war remain the persistence of "general friction" as a structural component of combat; the impossibility of eliminating uncertainty from war; and the critical importance of "moral factors."[4]

The "character" of war is infinite. A weaker adversary can adopt various modalities of war to engage and defeat a stronger power. Success in war has traditionally gone to the side that can best bear the costs of the conflict relative to what Clausewitz called "the value of the object." Accordingly, the materially weaker side has prevailed in conflicts 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. Indeed, meeting threats from outside *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 and new methods of mass destruction, this is no longer true.[5]

THE SECURITY ENVIRONMENT

The emerging security environment exhibits a number of characteristics that will affect the character of war into the future, chief among them global interdependence, which permits terrorists and other violent ideologues to inflict damage at a very low cost and risk to themselves. Robb cites the words of the late Shamil Basayev (killed in 2006), mastermind of the Chechen separatists' 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." Robb observes that guerrillas now possess "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 are *global guerrillas* who represent "a broad-based threat that far exceeds that offered by terrorists or the guerrillas of the past."[6]

Global guerrillas exploit the dissonance caused by "spiky" economic development and urbanization, the diffusion of and impact of technology, and the dislocation caused by globalization and demographic bulges. They effect "systems disruption" in advanced economies by causing "cascading" failures in the system. Interdependence means that failures within a single network can cause the failure of others. Not only do the transportation, water, and fuel networks depend on the electricity network, but also 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."[7]

CATEGORIES OF WAR—MULTIDIMENSIONAL CONFLICT

While the categorization of war by the 2004 Defense Strategy and the 2006 QDR—Traditional, Irregular, Catastrophic, and Disruptive—represents an advance in thinking, it implied that adversaries would focus on only one of these categories. But war, properly understood, is always *multidimensional*.

Even in the past, when the traditional category was central, combatants also pursued irregular or disruptive strategies. But one particular form of multidimensional warfare may constitute the most demanding challenge to American planners in the future: "complex irregular warfare,"[8] one characteristic of which is that future adversaries will likely be "hybrids."

A prototype hybrid is Hezbollah. During the 2006 war with Israel, Hezbollah exhibited state-like capabilities—long range missiles, anti-ship cruise missiles, sophisticated anti-armor systems, armed UAVs, and SIGINT—while skillfully executing guerrilla warfare. Such a hybrid has the potential to complicate future U.S. military planning and execution. Hezbollah could stand up to the Israel Defense Force by adapting to the particular circumstances it faced. 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. Hezbollah fielded modular units and adopted mission-type orders. It was effective in its innovative use of weapons and perfectly willing to accept a loss ratio of about five Hezbollah fighters to one IDF soldier. Hezbollah's intelligence performance was also surprisingly effective.

The hybrid threats generated by complex irregular warfare may well constitute the most demanding and potentially most costly type of future conflict. Wars against hybrid threats will likely be extremely lethal and protracted, and since they will often take place in contested urban zones, they will be manpower intensive. They will be widely distributed by distance, complexity, and mission. In most cases, these hybrid threats will seek to wage 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 will likely be characterized by close encounters between friendly forces and an enemy that seeks to blur the distinctions between conventional and unconventional, between combatants and non-combatants, conflict and stability operations, and 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 will attempt to exploit the political effects of a conflict, seeking to undermine the legitimacy of U.S. military actions. They will try to leverage "Lawfare," the use of the rules of warfare against the United States (while ignoring these rules themselves), for example, by taking refuge among the civilian population in an attempt to maximize civilian casualties.[9] They will take advantage of the fact that such casualties are magnified by the proliferation of media assets on the battlefield.

SANCTUARY: THE GEOPOLITICS OF TERRORISM AND INSURGENCY

For the 1929 edition of the *Encyclopaedia Britannica*, the editor commissioned T.E. Lawrence to write a piece on guerrilla warfare. Lawrence's article is remarkable—a concise but comprehensive treatment of a complex subject viewed through the lens of his own experience during the Arab Revolt against the Turks in 1916-18. His discussion of the importance of sanctuary stands out.

The guerrilla striking force must possess a safe haven, enabling it, in Lawrence's case, to always keep a means of "sure retreat" into an element which the enemy cannot enter. Lawrence concludes:

Rebellion must have an unassailable base, something guarded not merely from attack, but from the fear of it: such a base as the Arab revolt had in the Red Sea ports, the desert, or in the minds of men converted to its creed. It must have a sophisticated alien enemy, in the form of a disciplined army of occupation too small to fulfill the doctrine of acreage: too few to adjust number to space, in order to dominate the whole area effectively from fortified posts. It must have a friendly population, not actively friendly, but sympathetic to the point of not betraying rebel movements to the enemy. Rebellions can be made by 2 percent active in a striking force, and 98 percent passively sympathetic. The few active rebels must have … the technical equipment to destroy or paralyze the enemy's organized communications … . In 50 words: Granted mobility, security (in the form of denying targets to the enemy), time, and doctrine (the idea to convert every subject to friendliness), victory will rest with the insurgents, for the algebraical factors are in the end decisive, and against them perfections of means and spirit struggle quite in vain.

Thus in order to have any hope of success, a guerrilla force must be able to operate from a secure base. That base may be geographical but it may also be conceptual—lying within the minds of a friendly or sympathetic population.

This principle applies to the strategic level as well as the operational, making "sanctuary" the cornerstone of the geopolitics of insurgency and terrorism and the reason that insurgents, terrorists, and other armed groups must rely on the likes of Waziristan (for the anti-Musharraf insurgents), the Sierra Maestre (for the Cuban revolutionaries), or Shaanxi (for the Chinese Communists).[10] The likelihood that an insurgency will succeed increases significantly if it can gain sanctuary in neighboring states and obtain assistance from state and non-state actors.[11] But armed groups can also find sanctuary in remote areas within a state, e.g. a backwoods or highland area, as illustrated by the examples above.

Armed groups may also find sanctuary within an ethnic diaspora, either within the insurgency state or without. Diasporas often provide a source of recruits, training, finance, arms, logistics, and diplomatic backing. In the case of Islamic terrorism and insurgency, this form of sanctuary has been boosted by the emergence of a transnational jihadi network, which creates synergy between local and global groups.

Finally, terrorist organizations have been able to find sanctuary in cyberspace. In the case of Al Qaeda, jihadis are able to use the internet to spread its ideology, raise money, gain recruits, and signal operatives. Al Qaeda operates in cyberspace with impunity, using 6,000-plus web sites to recruit, proselytize, and plan, exploiting the virtual reality of Islam's global ummah.

The physical size of a sanctuary is a critical determinant of whether a terrorist group can transform itself into a full-blown insurgency. Robb explains the relationship between sanctuary and the size of an armed group, arguing that terrorist networks are distributed and dynamic and cannot scale like hierarchical networks, because the same network design that makes them resilient when attacked also establishes absolute limits on their size.[12] However, when a terrorist network possesses a sanctuary, it can grow larger because physical security and proximity permit it to operate as a hierarchy along military lines, complete with middle management. Before the United States responded to 9/11, Al Qaeda operated in this mode in Afghanistan, while maintaining distributed network outside of Afghanistan. Once it was driven from Afghanistan, it fragmented into smaller, less effective groups.

Dismantling terrorist enclaves is a critical component of anti-terrorism and counterinsurgency. This was the lesson of Afghanistan in 2002 and Fallujah in 2004. It also explains why Al Qaeda has been able to reconstitute itself in Waziristan and why this sanctuary cannot be tolerated.

PREEMPTING PREEMPTION

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

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

Third, as the U.S. is transporting its forces to the theater of action, an adversary will try to deny entry by military and political means, e.g. attacks and threats against U.S. allies in the region. And finally, as U.S. forces establish a lodgment and begin offensive operations, an adversary will seek to defeat U.S. forces.

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 US forces. This possibility is the result of another emerging characteristic of future conflict: "360 degree warfare."

Past wars have usually been characterized by "fronts" and secure "rear areas." Of course, airpower provided a means of attacking the enemy's rear, and long-range airpower and missiles threatened to extend to the homeland the ability to attack the rear. Nonetheless, actual attacks against the strategic rear of both sides were deterred by the likelihood of mutual destruction. The strategic emergence of true 360-degree warfare is a recent development, and Iraq and Afghanistan illustrate that our adversaries have adopted this approach.

Multidimensional war in the future is likely to be characterized by distributed, weakly connected battlefields; unavoidable urban battles and collateral damage exploited by 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 U.S. intelligence community was so focused on the rise of China prior to 9/11 that it was blind to the threat that manifested itself that day. 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? According to the Department of Defense's annual report to Congress on Chinese military power, the PLA is pursuing capabilities in winning "short-duration, high intensity conflicts against high-tech adversaries—which China refers to as 'local wars under conditions of informatization.'"[13]

China has enhanced its strategic strike capabilities and pursued a robust counter-space program, "punctuated by the January 2007 successful test of a direct-ascent, anti-satellite weapon." Its pursuit of area denial and anti-access strategies has expanded from "the traditional land, air, and sea dimensions of the modern battlefield to include space and cyber-space."

Hybrid warfare is not only a phenomenon associated with the "low end" of the spectrum of conflict. There is no reason a future peer competitor would restrict military competition with the United States to only the "traditional" category. It would logically also try to confront the United States asymmetrically. 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.[14]

THE FUTURE OF WAR

Any future adversary will, at a minimum, attempt to employ all the dimensions of warfare to asymmetrically counter critical U.S. military capabilities in such areas as conventional warfare, force projection, and C4ISR, including space operations and precision strike. 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.

Opponents will attempt to raise the cost of access by increasing the risk to the United States of naval and air operations by expanding the area of a "contested zone," seeking to destroy high-value assets, e.g. 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.

Adversaries will attempt to "bring down the network" by attacking U.S. space assets, degrading U.S. information systems, disrupting command and control, denying US surveillance and reconnaissance, and deceiving U.S. intelligence. They will seek to reduce U.S. standoff range, spoof U.S. guidance systems that enable precision attack, and disperse targets, including in populated areas. All of these methods have already been employed by adversaries and 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.

One cannot *predict* the future, but one can project a number of *plausible alternative futures* against which to test strategies and force structures. To do so, U.S. planners must develop a representative set of plausible contingencies that encompass the principal challenges the U.S. military might encounter—a representative array of contingencies encompassing the principal military challenges U.S. planners may confront over the planning horizon (15-20 years). As Andrew Krepinevich has written, this will enable them to "hedge" against uncertainty by testing concepts of operations and force structures against plausible alternatives and permit them to realistically assess the potential impact of a range of possible futures on relative military effectiveness.[15]

Gen. James Mattis, USMC, the new commander of U.S. Joint Forces Command, has paraphrased Sir Michael Howard to the effect that "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 don't get the future too wrong is by not confusing the *nature* of war with the *character* of war. The nature of war has not changed; the character of war is changing before our eyes. We have to see it plain if we are to win our Long War(s).

Mackubin Thomas Owens, an FPRI senior fellow, is Associate Dean of Academics for Electives and Directed Research and Professor of National Security Affairs at the Naval War College in Newport RI and the editor-designate of Orbis. He also served as a member of the "Future of War" Panel of the 2007 Defense Science Board Summer Study.

NOTES

1. Donald Rumsfeld, "War on Terror Memo," *USA Today*, October 16, 2003.

2. John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (Hoboken: John Wiley and Sons, 2007), p. 31.

3. Michael Vickers, *Warfare in 2020: A Primer (Washington DC: Center for Strategic and Budgetary Assessments, 1996), p. ii.*

4. Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. and trans. (Princeton University Press, 1976); Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War, *International Security*, Winter 1992/1993; Barry D. Watts, *Clausewitzian Friction and Future War*, McNair Paper 52 (Washington DC: National Defense University Press, 1996); and Mackubin Thomas Owens, "Technology, The RMA, and Future War," *Strategic Review*, Spring 1998).

5. Philip Bobbitt, *The Shield of Achilles: War, Peace, and the Course of History* (New York: Alfred A. Knopf, 2002), pp. xxi.

6. Robb, *Brave New War*, pp. 14-15.

7. Ibid., p. 102-3.

8. See Frank Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs," *Orbis*, Summer 2006.

9. William H. Taft, IV, "The Law of Armed Conflict After 9/11: Some Salient Features," *Yale Journal of International Law*, 2003.

10. Gonzalo Aguirre Beltran, *Regions of Refuge* (Washington, DC: Society for Applied Anthropology, 1979).

11. James D. Feron and David D. Laitin, "Ethnicity, Insurgency, and Civil War," *American Political Science Review*, February 2003.

12. John Robb, "The Optimal Size of a Terrorist Network," *Global Guerrillas*, March 2003.

13. Office of the Secretary of Defense, *Military Power of the People's Republic of China, 2007*, Annual Report to Congress, p. I.

14. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Los Angeles: Pan American Publishing Company, 2002).

15. Andrew F. Krepinevich, *The Quadrennial Defense Review: Rethinking the US Military Posture* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2005), pp. 56-59.

.

FPRI, 1528 Walnut Street, Suite 610, Philadelphia, PA 19102-3684.

For information, contact Alan Luxenberg at 215-732-3774, ext. 105 or email fpri@fpri.org or visit us at www.fpri.org.