New Paradigms for 21st-Century Conflict

David J. Kilcullen

©AP Images/Hussein Malla

The multinational force monitoring the ceasefire following the 2006 war between Israel and Hezbollah is an example of recent cooperation among the international community to address the new types of conflict that have arisen in the 21st century. Here, U.N. Secretary-General Ban Ki-moon thanks the men and women from the 30 countries participating in this effort.

David J. Kilcullen, PhD, a former Australian Army lieutenant colonel, is currently senior counterinsurgency adviser to the commanding general, Multi-National Force - Iraq. He previously served as chief strategist in the U.S. Department of State's Office of the Coordinator for Counterterrorism and as the Pentagon's special adviser for irregular warfare and counterterrorism on the 2006 Quadrennial Defense Review. *He regularly contributes to the* Small War Journal Blog. *This paper, like his postings, solely reflects his personal views.*

Despite our rather rosy hindsight view of World War II, there was considerable dissent at the time about the war's aims, conduct, and strategy. But virtually no one disagreed that it was indeed a war or that the Axis powers were the enemy/aggressors.

Contrast this with the war on terrorism. Some dispute the notion that the conflict can be defined as a war; others question the reality of the threat. Far-left critics blame American industrial interests, while a lunatic fringe sees September 11, 2001, as a massive self-inflicted conspiracy. More seriously, people disagree about the enemy. Is al-Qaida a real threat or a creature of Western paranoia and overreaction? Is it even a real organization? Is al-Qaida a mass movement or simply a philosophy, a state of mind? Is the enemy all terrorism? Is it extremism? Or is Islam itself in some way a threat? Is this primarily a military, political, or civilizational problem? What would "victory" look like? These fundamentals are disputed, as those of previous conflicts (except possibly the Cold War) were not.

In truth, the al-Qaida threat is all too real. But ambiguity arises because this conflict breaks existing paradigms— including notions of "warfare," "diplomacy," "intelligence," and even "terrorism." How, for example, do we wage war on nonstate actors who hide in states with which we are at peace? How do we work with allies whose territory provides safe haven for nonstate opponents? How do we defeat enemies who exploit the tools of globalization and open societies, without destroying the very things we seek to protect?

A New Paradigm

British General Rupert Smith argues that war— defined as industrial, interstate warfare between armies, where the clash of arms decides the outcome—no longer exists, that we are instead in an era of "war amongst the people," where the utility of military forces depends on their ability to adapt to complex political contexts and engage nonstate opponents under the critical gaze of

global public opinion.[1] Certainly, in complex, multisided, irregular conflicts such as Iraq, conventional warfare has failed to produce decisive outcomes. We have instead adopted policing, nation-building, and counterinsurgency approaches—and developed new interagency tools "on the fly."

Similarly, we traditionally conduct state-based diplomacy through engagement with elites of other societies: governments, intelligentsia, and business leaders, among others. The theory is that problems can be resolved when elites agree, cooler heads prevail, and governments negotiate and then enforce agreements. Notions of sovereignty, the nation-state, treaty regimes, and international institutions all build on this paradigm. Yet the enemy organizes at the nonelite level, exploiting discontent and alienation across numerous countries, to aggregate the effects of multiple grassroots actors into a mass movement with global reach. How do elite models of diplomacy address that challenge? This is not a new problem—various programs were established in U.S. embassies in the Cold War to engage with nongovernmental elements of civil societies at risk from Communist subversion. But many such programs lapsed after 1992, and problems of religious extremism or political violence require subtly different approaches.

Likewise, traditional intelligence services are not primarily designed to find out what is happening but to acquire secrets from other nation-states. They are well-adapted to state-based targets but less suited to nonstate actors—where the problem is to acquire information that is unclassified but located in denied, hostile, or inaccessible physical or human terrain. Even against state actors, traditional intelligence cannot tell us what is happening, only what other governments believe is happening. Why, for example, did Western intelligence miss the imminent fall of the Soviet Union in 1992? In part, because we were reading the Soviet leaders' mail—and they themselves failed to understand the depth of grassroots disillusionment with Communism.[2] Why did most countries (including those that opposed the Iraq war) believe in 2002 that Saddam Hussein's regime had weapons of mass destruction? Because they were intercepting the regime's communications, and many senior Iraqi regime members believed Iraq had them.[3]

Long-standing trends underpin this environment. Drivers include globalization and the backlash against it, the rise of nonstate actors with capabilities comparable to some nation-states, U.S. conventional military superiority

that forces all opponents to avoid its strengths and migrate toward unconventional approaches, and a global information environment based on the Internet and satellite communications. All these trends would endure even if al-Qaida disappeared tomorrow, and until we demonstrate an ability to defeat this type of threat, any smart adversary will adopt a similar approach. Far from being a one-off challenge, we may look back on al-Qaida as the harbinger of a new era of conflict.

Adapting to the New Environment

Thus, as former U.S. Counterterrorism Ambassador Hank Crumpton observed, we seem to be on the threshold of a new era of warfare, one that demands an adaptive response. Like dinosaurs outcompeted by smaller, weaker, but more adaptive mammals, in this new era, nation-states are more powerful but less agile and flexible than nonstate opponents. As in all conflict, success will depend on our ability to adapt, evolve new responses, and get ahead of a rapidly changing threat environment.

©AP Images/Kenneth Lambert

The names of U.S. government agencies engaged in the fight against terrorism are displayed during a hearing on federal reorganization to combat terrorism in June 2002.

The enemy adapts with great speed. Consider al-Qaida's evolution since the mid-1990s. Early attacks (the East African embassy bombings, the USS *Cole*, and 9/11 itself) were "expeditionary": Al-Qaida formed a team in Country A, prepared it in Country B, and clandestinely infiltrated it into Country C to attack a target. In response, we improved transportation security, infrastructure protection, and immigration controls. In turn, terrorists developed a "guerrilla" approach where, instead of building a team remotely and inserting it secretly to attack, they

Five Practical Steps

In responding to this counterintuitive form of warfare, the United States has done two basic things so far. First, we improved existing institutions (through processes like intelligence reform, creation of the Department of Homeland Security, and additional capacity for "irregular"—that is, nontraditional—warfare within the Department of Defense). Second, we have begun developing new paradigms to fit the new reality. These are yet to fully emerge, though some—such as the idea of treating the conflict as a very large-scale counterinsurgency problem, requiring primarily nonmilitary responses coupled with measures to protect at-risk populations from enemy influence—have gained traction.[5]

©AP Images/Lefteris Pitarakis

In a warehouse on the outskirts of the Jordanian capital of Amman, workers store blankets donated by the U.S. Agency for International Development for distribution in Iraq.

grew the team close to the target using nationals of the host country. The Madrid and London bombings, and attacks in Casablanca, Istanbul, and Jeddah, followed this pattern, as did the foiled London airline plot of summer 2006.

These attacks are often described as "home grown," yet they were inspired, exploited, and to some extent directed by al-Qaida. For example, Mohammed Siddeque Khan, leader of the July 7, 2005, London attack, flew to Pakistan and probably met al-Qaida representatives for guidance and training well before the bombing.[4] But the new approach temporarily invalidated our countermeasures—instead of smuggling 19 people in, the terrorists brought one man out—side-stepping our new security procedures. The terrorists had adapted to our new approach by evolving new techniques of their own.

We are now, of course, alert to this "guerrilla" method, as the failure of the August 2006 plots in the United Kingdom and other recent potential attacks showed. But terrorists are undoubtedly already developing new adaptive measures. In counterterrorism, methods that work are almost by definition already obsolete: Our opponents evolve as soon as we master their current approach. There is no "silver bullet." Similar to malaria, terrorism constantly morphs into new mutations that require a continuously updated battery of responses.

But in a sense, policy makers today are a little like the "Chateau Generals" of the First World War—confronting a form of conflict that invalidates received wisdom, just as the generals faced the "riddle of the trenches" in 1914-1918. Like them, we face a conflict environment transformed by new technological and social conditions, for which existing organizations and concepts are ill-suited. Like them, we have "work-arounds," but have yet to develop the breakthrough concepts, technologies, and organizations—equivalent to *blitzkrieg* in the 1930s—that would solve the riddle of this new threat environment.

There is no easy answer (if there were, we would have found it by now), but it is possible to suggest a way forward. This involves three conceptual steps to develop new models and, simultaneously, two organizational steps to create a capability for this form of conflict. This is not meant to be prescriptive, but is simply one possible approach. And the ideas put forward are not particularly original—rather, this proposal musters existing ideas and integrates them into a policy approach.

1. Develop a new lexicon: Professor Michael Vlahos has pointed out that the language we use to describe the new threats actively hinders innovative thought.[6] Our terms draw on negative formulations; they say what the environment is not, rather than what it is. These terms include descriptors like *un*conventional, *non*state,

*non*traditional, *un*orthodox, and *ir*regular. Terminology undoubtedly influences our ability to think clearly. One reason why planners in Iraq may have treated "major combat operations" (Phase III) as decisive, not realizing that in this case the post-conflict phase would actually be critical, is that Phase III is decisive by definition. Its full doctrinal name is "Phase III—Decisive Operations." To think clearly about new threats, we need a new lexicon based on the actual, observed characteristics of real enemies who:

- Integrate terrorism, subversion, humanitarian work, and insurgency to support propaganda designed to manipulate the perceptions of local and global audiences
- Aggregate the effects of a very large number of grassroots actors, scattered across many countries, into a mass movement greater than the sum of its parts, with dispersed leadership and planning functions that deny us detectable targets
- Exploit the speed and ubiquity of modern communications media to mobilize supporters and sympathizers, at speeds far greater than governments can muster
- Exploit deep-seated belief systems founded in religious, ethnic, tribal, or cultural identity, to create extremely lethal, nonrational reactions among social groups
- Exploit safe havens such as ungoverned or undergoverned areas (in physical or cyber space); ideological, religious, or cultural blind spots; or legal loopholes
- Use high-profile symbolic attacks that provoke nation-states into overreactions that damage their long-term interests
- Mount numerous, cheap, small-scale challenges to exhaust us by provoking expensive containment, prevention, and response efforts in dozens of remote areas

These features of the new environment could generate a lexicon to better describe the threat. Since the new threats are not state-based, the basis for our approach should not be international relations (the study of how nation-states interact in elite state-based frameworks) but anthropology (the study of social roles, groups, status, institutions, and relations within human population groups, in nonelite, nonstate-based frameworks).

2. Get the grand strategy right: If this confrontation is based on long-standing trends, it follows that it may be a protracted, generational, or multigenerational struggle.

This means we need both a "long view" and a "broad view"[7] that consider how best to interweave all strands of national power, including the private sector and the wider community. Thus we need a grand strategy that can be sustained by the American people, successive U.S. administrations, key allies, and partners worldwide. Formulating such a long-term grand strategy would involve four crucial judgments:

- Deciding whether our interests are best served by intervening in and trying to mitigate the process of political and religious ferment in the Muslim world, or by seeking instead to contain any spillover of violence or unrest into Western communities. This choice is akin to that between "rollback" and "containment" in the Cold War and is a key element in framing a long-term response.
- Deciding how to allocate resources among military and nonmilitary elements of national power. Our present spending and effort are predominantly military; by contrast, a "global counterinsurgency" approach would suggest that about 80 percent of effort should go toward political, diplomatic, development, intelligence, and informational activity, and about 20 percent to military activity. Whether this is appropriate depends on our judgment about intervention versus containment.
- Deciding how much to spend (in resources and lives) on this problem. This will require a risk judgment taking into account the likelihood and consequences of future terrorist attacks. Such a judgment must also consider how much can be spent on security without imposing an unsustainable cost burden on our societies.
- Deciding how to prioritize effort geographically. At present most effort goes to Iraq, a much smaller portion to Afghanistan, and less again to all other areas. Partly this is because our spending is predominantly military and because we have chosen to intervene in the heart of the Muslim world. Different choices on the military/nonmilitary and intervention/containment judgments might produce significantly different regional priorities over time.

Clearly, the specifics of any administration's strategy would vary in response to a developing situation. Indeed, such agility is critical. But achieving a sustainable consensus, nationally and internationally, on the four grand judgments listed above, would provide a long-term basis for policy across successive administrations.

3. Remedy the imbalance in government capability: At present, the U.S. defense budget accounts for approximately half of total global defense spending, while the U.S. armed forces employ about 1.68 million uniformed members.[8] By comparison, the State Department employs about 6,000 foreign service officers, while the U.S. Agency for International Development (USAID) has about 2,000.[9] In other words, the Department of Defense is about 210

© AP Images/Irwin Fedriansyiah

Soldiers from many nations, including these Indonesian commandos who are applauding their colleagues during an anti-terror exercise conducted outside Jakarta in 2006, have joined in the international fight against terrorism.

times larger than USAID and State combined—there are substantially more people employed as musicians in Defense bands than in the entire foreign service.[10]

This is not to criticize Defense—armed services are labor- and capital-intensive and are always larger than diplomatic or aid agencies. But considering the importance, in this form of conflict, of development, diplomacy, and information (the U.S. Information Agency was abolished in 1999 and the State Department figures given include its successor bureau), a clear imbalance exists between military and nonmilitary elements of capacity. This distorts policy and is unusual by global standards. For example, Australia's military is approximately nine times larger than its diplomatic and aid agencies combined: The military arm is larger, but not 210 times larger, than the other elements of national power.

To its credit, the Department of Defense recognizes the problems inherent in such an imbalance, and said so in the 2006 *Quadrennial Defense Review*.[11] And the Bush administration has programs in train to increase nonmilitary capacity. But to succeed over the long haul, we need a sustained commitment to build nonmilitary elements of national power. So-called soft powers, such as private-sector economic strength, national reputation, and cultural confidence, are crucial, because military power

alone cannot compensate for their loss.

These three conceptual steps will take time (which is, incidentally, a good reason to start on them). But in the interim, two organizational steps could prepare the way:

4. Identify the new "strategic services": A leading role in the war on terrorism has fallen to Special Operations Forces (SOF) because of their direct action capabilities against targets in remote or denied areas. Meanwhile, Max Boot[12] has argued that we again need something like the Office of Strategic Services (OSS) of World War II, which included analysis, intelligence, anthropology, special operations, information, psychological operations, and technology capabilities.

Adjectives matter: Special Forces versus Strategic Services. SOF are special. They are defined by internal comparison to the rest of the military—SOF undertake tasks "beyond the capabilities" of general-purpose forces. By contrast, OSS was strategic. It was defined against an external environment and undertook tasks of strategic importance, rapidly acquiring and divesting capabilities as needed. SOF are almost entirely military; OSS was an interagency body with a sizeable civilian component, and almost all its military personnel were emergency war enlistees (talented civilians with strategically relevant skills, enlisted for the duration of the war).[13] SOF trace their

origin to OSS; yet whereas today's SOF are elite military forces with highly specialized capabilities optimized for seven standard missions,[14] OSS was a mixed civil-military organization that took whatever mission the environment demanded, building capabilities as needed.

Identifying which capabilities are strategic services today would be a key step in prioritizing interagency efforts. Capabilities for dealing with nonelite, grassroots threats include cultural and ethnographic intelligence, social systems analysis, information operations (see below), early-entry or high-threat humanitarian and governance teams, field negotiation and mediation teams, biometric reconnaissance, and a variety of other strategically relevant capabilities. The relevance of these capabilities changes over time—some that are strategically relevant now would cease to be, while others would emerge. The key is the creation of an interagency capability to rapidly acquire and apply techniques and technologies in a fast-changing situation.

©AP Images/David Guttenfelder
A U.S. national guardsman works with an Iraqi police officer at the Major Crime Unit in western Baghdad..

5. Develop a capacity for strategic information warfare: Al-Qaida is highly skilled at exploiting multiple, diverse actions by individuals and groups, by framing them in a propaganda narrative to manipulate local and global audiences. Al-Qaida maintains a network that collects information about the debate in the West and feeds this, along with an assessment of the effectiveness of al-Qaida's propaganda, to its leaders. They use physical operations (bombings, insurgent activity, beheadings) as supporting material for an integrated "armed propaganda" campaign. The "information" side of al-Qaida's operation is primary; the physical is merely the tool to achieve a propaganda result. The Taliban, GSPC (previously, the Salafist Group for Preaching and Combat, now known as al-Qaida in the Islamic Maghreb), and some other al-Qaida-aligned groups, as well as Hezbollah, adopt similar approaches.

Contrast this with our approach: We typically design physical operations first, then craft supporting information operations to explain our actions. This is the reverse of al-Qaida's approach. For all our professionalism, compared to the enemy's, our public information is an afterthought. In military terms, for al-Qaida the "main effort" is information; for us, information is a "supporting effort." As noted, there are 1.68 million people in the

U.S. military, and what they do speaks louder than what our public information professionals (who number in the hundreds) say. Thus, to combat extremist propaganda, we need a capacity for strategic information warfare—an integrating function that draws together all components of what we say and what we do to send strategic messages that support our overall policy.

At present, the military has a well-developed information operations doctrine, but other agencies do not, and they are often rightly wary of military methods. Militarizing information operations would be a severe mistake that would confuse a part (military operations) with the whole (U.S. national strategy) and so undermine our overall policy. Lacking a whole-of-government doctrine and the capability to fight strategic information warfare limits our effectiveness and creates message dissonance, in which different elements of the U.S. government send out different messages or work to differing information agendas.

We need an interagency effort, with leadership from the very top in the executive and legislative branches of government, to create capabilities, organizations, and doctrine for a national-level strategic information campaign. Building such a capability is perhaps the most important of our many capability challenges in this new era of information-driven conflict.

Tentative Conclusions

These notions—a new lexicon, grand strategy, balanced capability, strategic services, and strategic information warfare—are merely speculative ideas that suggest what might emerge from a comprehensive effort to find new paradigms for this new era of conflict. Different ideas may well emerge from such an effort, and, in any case, rapid changes in the environment due to enemy adaptation will demand constant innovation. But it is crystal clear that our traditional paradigms of industrial interstate war, elite-based diplomacy, and state-focused intelligence can no longer explain the environment or provide conceptual keys to overcome today's threats.

The Cold War is a limited analogy for today's conflict: There are many differences between today's threats and those of the Cold War era. Yet in at least one dimension, that of time, the enduring trends that drive the current confrontation may mean that the conflict will indeed resemble the Cold War, which lasted in one form or another for the 75 years between the Russian Revolution in 1917 and the collapse of the Soviet Union in December 1991. Many of its consequences—especially the "legacy conflicts" arising from the Soviet-Afghan War—are with us still. Even if this confrontation lasts only half as long as the Cold War, we are at the beginning of a very long road indeed, whether we choose to recognize it or not.

The new threats, which invalidate received wisdom on so many issues, may indicate that we are on the brink of a new era of conflict. Finding new, breakthrough ideas to understand and defeat these threats may prove to be the most important challenge we face. ∎

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.

Endnotes

1. See Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred A. Knopf, 2007), especially pp. 3-28 and 269-335.

2. See Gerald K. Haines and Robert E. Leggett, *Watching the Bear: Essays on CIA's Analysis of the Soviet Union* (Washington, D.C.: Central Intelligence Agency, Center for the Study of Intelligence, 2003), especially chapters VI and VII.

3. See Kevin M. Woods et. al, *Iraqi Perspectives Project: A View of Operation Iraqi Freedom from Saddam's Senior Leadership* (Joint Forces Command, Joint Center for Operational Analysis), p. 92.

4. Intelligence and Security Committee, *Report Into the London Terrorist Attacks on 7 July 2005* (London: The Stationery Office, May 2006), p. 12.

5. See David Kilcullen, "Countering Global Insurgency," *Small Wars Journal* (November 2004) and available at *http://www.smallwarsjournal.com/documents/kilcullen.pdf*; Williamson Murray (ed.), *Strategic Challenges for Counterinsurgency and the Global War on Terrorism* (Carlisle, PA: Strategic Studies Institute, 2006); and Bruce Hoffman, "From War on Terror to Global Counterinsurgency," *Current History* (December 2006): pp. 423-429.

6. Professor Michael Vlahos, Johns Hopkins University Applied Physics Laboratory, personal communication, December 2006.

7. I am indebted to Mr. Steve Eames for this conceptual formulation.

8. Compiled from figures in International Institute for Strategic Studies, *Military Balance 2007*, pp. 15-50.

9. Compiled from U.S. State Department and U.S. Agency for International Development, *Congressional Budget Justification 2007*, table 9.

10. The U.S. Army alone employs well over 5,000 band musicians, according to a March 2007 job advertisement; see *http://bands.army.mil/jobs/default.asp*.

11. Department of Defense, *Quadrennial Defense Review Report* (2 February 2006): pp. 83-91.

12. See Max Boot, Congressional Testimony Before the House Armed Services Committee, 29 June 2006, at *http://www.globalsecurity.org/military/library/congress/2006_hr/060629-boot.pdf*.

13. See Central Intelligence Agency, *The Office of Strategic Services: America's First Intelligence Agency* at *https://www.cia.gov/cia/publications/oss/index.htm*.

14. The seven standard SOF missions are Direct Action (DA), Special Reconnaissance (SR), Unconventional Warfare (UW), Foreign Internal Defence (FID), Counter-Terrorism (CT), Psychological Operations (PSYOP), and Civil Affairs (CA).