
Orbis

A Journal of World Affairs

Volume 54, Number 1, Winter 2010

TWILIGHT OF U.S. NAVAL SUPREMACY?

Editor's Corner	Mackubin T. Owens	1
Bridging the Gap between Ideas and Actions	Thomas G. Mahnken	4
History Rhymes: The German Precedent for Chinese Seapower	James Holmes and Toshi Yoshihara	14
How the United States Lost the Naval War of 2015	James Kraska	35
Radical Islam in Europe	Leslie S. Lebl	46
Purifying the World: What the New Radical Ideology Stands For	Ernest Sternberg	61
Changes and the American Security Paradigm	Kenneth Allard	87
Why Foreign Fighters? Historical Perspectives and Solutions	David Malet	97
Sovereignty and the Foreign Fighter Problem	Ian Bryan	115
Prisoner Dilemmas: The American Obsession with POWs and Hostages	Dominic Tierney	130

REVIEW ESSAY

Terrorism as a Political and Cultural Phenomenon	Daniel J. Mahoney	146
---	-------------------	-----

Change and the American Security Paradigm

by Kenneth Allard

Kenneth Allard is a former U.S. Army Colonel whose military career included overseas service as an intelligence officer and tours of duty as an assistant professor at West Point, special assistant to the Army Chief of Staff and Dean of Students at the National War College. A former military analyst with NBC News, his most recent book is *Warheads: Cable News and the Fog of War*.

What do Mexican civil instability and an increasingly well-armed narco-insurgency mean for homeland defense? What lessons about confronting U.S. military power might the drug networks have learned from those other malevolent networks, the same ones responsible for 9/11? And while we have always assumed a neat institutional distinction between the United States' internal defenses and the military power mobilized to protect its international interests, are porous borders and trans-national syndicates blurring those boundaries? These questions become more urgent with the growth of affluent, aggressive, and highly networked groups where the traditional distinctions between criminal and terrorist are often rendered meaningless.

Recent Past as Prologue

Counterinsurgency expert David Kilcullen suggests the required shifts in our mental landscape (and possibly the physical ones as well) in his path-breaking book, *The Accidental Guerrilla*, which begins by recounting a pre-9/11 guest lecture at his Australian military staff college. The speaker, a visiting and recently retired U.S. general, breezily dismissed the notion of “serious ground combat” as an increasingly unlikely form of warfare. Instead, the distinguished visitor argued, future military competition was best understood as the optimum combination of advanced technologies, harnessed to deliver precision strikes through air and naval “systems of systems” in which Western countries, particularly the United States, had a clear and decisive edge. “Large scale. . . ground combat operations? Not so much.”¹

Kilcullen's cameo brilliantly captures the zeitgeist surrounding the revolution in military affairs, the prevailing neo-orthodoxy of the late 1990s

¹David Kilcullen, *The Accidental Guerrilla* (New York: Oxford University Press, 2009), pp. 1–2.

ultimately known by its own acronym: the RMA. With origins in the immediate aftermath of the first Gulf War, the RMA emerged as a hard-edged theoretical construct with the 1998 publication of “Network Centric Warfare: Its Origins and Future,” by Vice Admiral Arthur Cebrowski.² Newly fitted laser and digital guidance systems had given weapons unprecedented accuracy, e.g. the Joint Direct Attack Munition (JDAM) delivering a ton of high explosives with a sniper’s deadly precision. Better yet, the proliferation of information, surveillance and computing technologies might even provide U.S. generals with the god’s – eye view of future battlefields lusted for by commanders since antiquity. Cebrowski seemed to envision the twenty-first-century military being transformed into a kind of malevolent, hyper-efficient hybrid, halfway between Walmart and the Terminator.

Yet even before Iraq’s complications, remarkably ugly and persistent conflicts in Bosnia, Kosovo and elsewhere in the developing world seemed to suggest alternative realities; among them, the permanent ingenuity of the underdog and the resulting fog of war. At Washington’s National Defense University, I occasionally presided over seminars that Kilcullen would have recognized instantly, where impassioned techno-colleagues argued that the RMA meant not really having to go to war at all. “Look, we can just use information warfare to take down their stock markets instead.” But as 1996 ended, I returned from a Bosnian peacekeeping deployment with sobering news: the power and information gridlines had been destroyed; the only stock market in evidence swapped the few surviving Balkan bovines through tailgate exchanges of hard currencies lubricated by copious ample quantities of Slivovitz. The Serbs disrupted our intelligence collection by using cell phones or simply maintaining radio silence. Meanwhile, the army of NATO peacekeepers struggled mightily to protect their notoriously fragile computers from Bosnian mud and dust as well as the pandemic of electronic viruses accompanying the international coalition.

In Iraq many of those difficulties turned into contradictions as the occupation became a protracted and deadly fight against an enemy who proved adaptive and surprisingly aggressive in exploiting opportunities. To help limit troop casualties, U.S. commanders responded by retreating to the protection of jersey-walled compounds, wielding networked technologies to target guerrilla who remained elusive. For the U.S. contingent, the yang-and-yin of battlefield technology produced quantum proliferations of remotely piloted vehicles, the exploitation of geo-spatial intelligence and the aggressive use of combined arms.³ The insurgent response: the equally aggressive

²Vice Admiral Arthur K. Cebrowski, USN and John J. Garstka, “Network Centric Warfare: Its Origins and Future,” *Proceedings of the US Naval Institute* 124:1 (January, 1998), pp. 28–35.

³See, for example, the author’s *Warheads: Cable News and the Fog of War* (Annapolis, MD: Naval Institute Press, 2007), esp. pp. 125–143, for an eyewitness view of that evolution immediately prior to the Surge.

combinations of clandestine networks and lower technologies, combined into the improvised explosive device (IED) or the explosively formed penetrator (EFP)—the signature weapons of the Iraq war. Whether in its vehicle-borne or roadside versions, the IED produced more casualties than any other weapon, a precision weapon targeting the United States.

Because of its instinctive techno-advocacy, *Wired* magazine's 2007 critique was a chilling assessment:

For far too many units. . . war had been turned into a telecommute. Afghanistan, Iraq, and Lebanon were the first conflicts planned, launched, and executed with networked technologies and a networked ideology. They were supposed to be the wars of the future. And the future lost.⁴

Those words were written well before General David Petraeus took command, ordered U.S. troops out of their cantonments and produced the improbable turn-around that largely defeated the Iraq insurgency by early 2009. Wisely, General Petraeus consistently characterized those victories as fragile and reversible⁵ because military history contains ample precedents for similarly startling reversals (and even reversals of those reversals).

Great caution is therefore required before offering judgments while the jury is still out – or even asking if a new pattern has begun to emerge in the long evolution of revolutionary warfare. But awaiting the eventual verdict of history is unnecessary for considering how these military developments may affect more immediate challenges in U.S. homeland defense. It sometimes requires a conscious effort to recall that the wars in Afghanistan, Iraq and – at this writing – even in Pakistan, all began on 9/11. As the more recent attacks in Madrid, London and Mumbai occasionally remind us, enemies learn lessons too, particularly when they are multi-national networks arrayed against hierarchical state systems. And by early 2009, there were growing reasons for the new Obama administration to be concerned about war on the United States' own door-step.

Implications of War in the 'Near Abroad'

Hierarchies instinctively react to new challenges by spawning new hierarchies – hence the post-9/11 consolidations of the U.S. intelligence community and the creation of the Department of Homeland Security (DHS), the latter placing dozens of Federal security agencies under allegedly unified agency control. The problem was always what Samuel Huntington, the dean of U.S. political science and civil-military relations,

⁴ Noah Schachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks are -/Social Not Electronic," *Wired Magazine* (15:12) Nov. 27, 2007.

⁵ As quoted by Bob Woodward in *The War Within* (New York: Simon & Schuster, 2008) p. 426.

termed the “conservative Constitution.”⁶ Our system of government carefully divides power, particularly military power: between the President and Congress (control over the armed forces and declaring war); between House and Senate (appropriations and confirmation); and, even more profoundly, between state governors, Congress and Federal authorities (control over Reserves and National Guard, “the Militia”). As a practical matter, this constitutional division of labor places the outward projection of military power and the protection of the nation’s borders squarely in federal hands – though carefully controlled by those checks and balances U.S. kids used to study in high school.

Law enforcement – particularly against terrorists, organized crime or international syndicates – inevitably raises troublesome questions of jurisdiction. Whose law is being enforced: federal or state; and if it is the latter, then which one? This distinction is more than academic. Because of the Tenth Amendment to the U.S. Constitution, reinforced by two centuries of practice, police powers largely reside at state level, a constant source of tension given the more recent charter granted to DHS. In either a natural disaster or a 9/11-style attack, “the Feds” may well have overall responsibility; but it is local mayors, sheriffs and police departments that have the authority on the ground, where it usually counts most. Equally important: their practical clout is usually enhanced by local knowledge and control over available manpower. (Doubters should simply ask any Texas sheriff for a short and to-the-point tutorial.)

But these comforting U.S. customs and traditions take on an entirely different meaning when examined from the contrasting perspective of military strategy. This viewpoint considers such carefully drawn distinctions simply as “seams”: those organizational weak-points, vulnerabilities and fault lines which an alert adversary is certain to notice. Networked adversaries are especially quick to exploit such flaws – simply because that is what networks do, both in business and in war. In Islamic radicalism, we have already encountered the first of the two networks challenging bedrock U.S. interests, from 9/11 to the ongoing confrontation with U.S. military power at multiple points around the globe. But the second is that loose confederation of shifting rivalries, alliances and counter-alliances collectively known as the Mexican drug cartels. The cartels are a highly efficient, ruthlessly entrepreneurial supply-and-demand network exemplifying Adam Smith’s teachings. Their supply chain stretches from Latin American jungles to the branch offices present in at least 200 U.S. cities and many rural neighborhoods.⁷ And with a product line valued – in Mexico alone – at between \$14–30 billion per year,

⁶ Samuel P. Huntington, *The Soldier and the State* (Cambridge: Harvard University Press, 1957), especially ch. 7.

⁷ National Drug Intelligence Center. “Cities in Which Mexican DTOs Operate in the United States.” April 11, 2009. 2008. <http://www.usdoj.gov/ndic/pubs27/27986/27986p.pdf>. pp. 3–7.

they might otherwise qualify for seats on the U.S. stock exchange or membership in the nation's most prestigious business councils.⁸

The reason why they do not is, of course, because the cartels are an ongoing criminal conspiracy, making the fictional Soprano and the Corleone families seem like relatively benign amateurs. Cartel efficiency in supplying U.S. society's insatiable drug addiction is necessarily accompanied by violence, which appears to be growing even faster than their preferred cash crops. Because of the need to control lucrative drug routes into the U.S. heartland, 7,400 murders have been recorded adjacent to the border since 2007, with the violence steadily spreading north. While state governors have occasionally been wont to call out the National Guard to stem the violence, the cartels are already deeply entrenched in communities far beyond the border region. The executive director of Oklahoma's Bureau of Narcotics and Dangerous Drug Control, told his state's leading newspaper, "Oklahoma's No. 1 threat is the Mexican drug cartels. Make no mistake." That is a shocking statement given his state's propensity for being routinely hit with range fires and F-5 tornadoes; other officials explained that 90 percent of Oklahoma's drugs come from the cartels.⁹

Urban Warfare and Open Sources

The possible confluence of these two seemingly unrelated networks – Islamic terrorists and drug smugglers – has become the mission and passion of a military studies boutique of which few have ever heard. Founded in 2007 through grants by the U.S. Army Research Laboratory, the Urban Warfare Analysis Center (www.uwac-ok.com) is an analytical outpost loosely affiliated with a half-dozen area universities and improbably located next to an oilrig in Shawnee Oklahoma. Its stock-in-trade is open-source intelligence, produced by a small group of analysts best described as young, diverse and interesting. A graduate student in nano-technology might compare notes with a Persian linguist cross-trained in political science. A young mechanical engineer checks his analysis of IED technologies with a research director recently retired from the CIA's analytical directorate. The group's focus on urban warfare may represent a startling departure from the standard fare of security studies, but the list of analytical papers (eighty produced over the last two years) by UWAC is impressive by any standard.

⁸ Woodrow Wilson International Center for Scholars Mexico Institute. "The United States and Mexico: Towards a Strategic Partnership." January 2009, p. 3. Sourced in: *Sullivan, Mark P.*, "Mexico–U.S. Relations: Issues for Congress." *Congressional Research Service*. December 18, 2008.

⁹ Ron Jackson, "Mexican drug cartels are Oklahoma's most dangerous threat," *The Oklahoman*, April 25, 2009.

Many of these reports reflect fascinating glimpses into what the young analysts believe may be the most interesting new developments in revolutionary warfare. Among the more recent titles:

- “Chinese Military Tactics in Tibet”
- “Bayonets in Basra: A Case Study on Insurgent Adaptation”
- “Text Messaging by Insurgents and Terrorists: A Potent Force Multiplier”
- “Emerging Nanotechnologies for Urban Warfare”
- “ Hamas and Hezbollah Sleeper Cells in the United States”

Because of small budgets, an absence of agency agendas, and correspondingly few bureaucrats to stifle curious minds, UWAC analysts can simply gather open-source data through the Internet and offer their independent judgments to subject-matter experts for debate, comment or disagreement. Thus far at least, they have been allowed to go in whatever directions the evidence leads them.

For those reasons alone, we need to pay particular attention to the linkages the analysts are finding between insurgent practices refined during the war on terror and the growing possibilities for their use against targets in the United States. Consider the IED, used with such devastating effects in Iraq and Afghanistan: could those weapons be used here and what could we do if they were? A UWAC team recently analyzed these questions and concluded that “advances in IED technology and tactics (would likely) inspire extremist groups intent on attacking (targets) inside the United States.”¹⁰ One of the analysts who produced that report told me: “Terrorists learn lessons too, usually preferring weapons that have worked best for them in the past. And seventy percent of the time in Iraq, that has been the IED. It is a classic weapon that the weak really love to use against the strong.”¹¹ The report goes on to suggest that the IED is a terror weapon typically used to create civilian casualties, that the U.S. transportation infrastructure is uniquely vulnerable to such attacks, and that the precedents for high-profile IED attacks were previously established with the first bombing of the World Trade Center as well as those in Oklahoma City and at the Atlanta Olympics – all deliberately chosen with civilian casualties in mind.¹²

In an era of swine flu outbreaks and persistent fears of a global pandemic, a UWAC report late in 2008 had a usefully chilling effect: “Bio-terror Martyrdom: Suffering, Slaughter and Salvation.” Its principal findings: the odds of a domestic bio-terror attack have increased, despite the challenges of procuring biological agents (suicide bombers willing to carry the agent were much easier to find). Even worse: the barriers to terrorist exploitation terror

¹⁰ Broun, James, Edwin Halpain, Justin Kent, and Chris Lorenz. *The IED Threat in America*. Urban Warfare Analysis Center: 25 March 2009. p. 3.

¹¹ James Broun, Senior Military Intelligence Analyst, Urban Warfare Analysis Center.

¹² Broun, et al., *IED Threat*, pp. 9, 17, et passim.

task have been lowered by “the lack of stringent (worldwide) security measures for biological research.”¹³ Seasoned intelligence analysts – either within the government or outside it – tend to base the worth of their sometimes lonely judgments by correlation; that is, when other reports arrive tending to confirm their findings. UWAC analysts must have experienced bursts of *Schadenfreude* in early June, 2009, when U.S. counter-terrorism officials authenticated an al Qaeda video boasting of biological weapons being smuggled into the U.S. via tunnels under the border with Mexico. The video showed an al Qaeda recruiter boasting that the terrorist group was casing that border to determine the best smuggling routes.

Four pounds of anthrax in a suitcase. . .carried by a fighter through tunnels from Mexico into the US are guaranteed to kill 330,000 Americans within a single hour if . . .properly spread in population centers. . .What a horrifying idea (that) 9/11 will be small change in comparison!. . .One person with the courage to carry 4 pounds of anthrax will go to the White House lawn and will spread this ‘confetti’ all over them. It will turn into a real celebration.¹⁴

Appalling as it is, this report was merely the latest in the growing body of evidence which has convinced UWAC analysts that increased cooperation between the smuggling and terror networks is inevitable. “They are completely different animals, organized for very different purposes, even contradictory ones. But you can’t rule out individual cells working together for their own interests in ways the larger network might even oppose.”¹⁵ In its most recent report on this issue,¹⁶ UWAC points to four closely linked developments bringing the groups closer together:

1. *The expanding arsenals of the cartels, including the automatic weapons, armor-piercing munitions and anti-tank weaponry typically found in well-equipped light infantry units;*

“They’ve got weapons, high-tech radios, computers, cell phones, global positioning systems (and) spotters. . .And they have no hesitancy to attack the agents on the line with anything from assault rifles (and) improvised Molotov cocktails. . .”¹⁷

2. *The ominous growth in the military sophistication of the cartels, the original members of one of the most powerful cartels, Los Zetas, having been recruited from elite Mexican military units;*

¹³ UWAC Report, Bio-Terror Martyrdom: Suffering, Slaughter and Salvation,” October 13, 2008, pp. 3, 4–7.

¹⁴ Sara A. Carter, “Al Qaida eyes bio attack from Mexico,” *Washington Times*, June 3, 2009.

¹⁵ Justin Walker, Social Science Analyst, Urban Warfare Analysis Center.

¹⁶ Walker, Justin. *Mexican Drug Cartels and Islamic Radicalism: Prospects for Collaboration*. Urban Warfare Analysis Center: May 7, 2009. (Referred to in the following section as “UWAC Collaboration Report”)

¹⁷ U.S. Border Patrol Veteran, January 2009, quoted in UWAC Collaboration Report p. 5.

“(In the Mexican military) Los Zetas received training in small unit tactics, advanced weapons, surveillance techniques, interrogation skills, intelligence gathering and counter-intelligence.”¹⁸

3. *The ability to control well-established logistical routes from the Mexican border into the U.S. heartland; originally established to move drugs, they can easily transport cash, weapons or terrorists;*

“The Mexican cartels have no loyalty to anyone. . . They will willingly or unknowingly aid other nefarious groups through the routes they control. It has already happened.”¹⁹

4. *The growing presence of the cartels – in as many as 200 U.S. cities – also provides the networks with manpower, financial and intelligence resources dwarfing the capabilities of most local law enforcement agencies.*

“The same folks who are rolling heads in the streets of Ciudad Juarez are operating in Atlanta. Here they are just better behaved.”²⁰

Overall, these findings suggest that, while the two networks have little in common, the terrorists may find the cartels irresistible. With an effective monopoly on weapons, clandestine cells, secure logistical networks and well-established operational bases, the cartels control the available infrastructure. Terrorists, intent on carrying out a devastating attack on the U.S. interior, will use Los Zetas or any other drug cartel for the same reasons they would rent an automobile from Hertz or Avis. From a purely strategic perspective, the cartels would certainly deplore any provocation leading to a law enforcement crack-down and interfering with business – as a 9/11-style attack surely would. But no network, however well-armed and well-organized, is likely to exert global control over each one of its cells – even for part of the time. Some of those supremely local organisms might well find their own reasons to rent their local drug tunnel for a single midnight hour to a Middle Eastern man with a small suitcase and the right amount of convertible currency. And the choice of weapon – be it anthrax or fissile materials – is primarily a terrorist procurement issue. The infiltration and movement of such weapons into the U.S. heartland present roughly the same probability-of-intercept problem encountered with marijuana, crack cocaine and heroin – all of which are here in some profusion.

Conclusions

1. The United States security paradigm is shifting as the drug and terrorist networks are drawn into increasingly odd couplings: the cartels are already well-established in the U.S. while the terrorist networks single-mindedly

¹⁸ Ibid., p. 7.

¹⁹ Anonymous U.S. law enforcement officer quoted in *ibid.*, p. 13.

²⁰ Jack Killorin, Office of National Drug Control Policy, quoted in *ibid.*, p. 6.

probe for openings. This cooperation may occur whether or not the two groups approve of one another (they do not). Instead, their relationship is more akin to what complexity theory understands as “strange attractors” – a perfect storm created from two unrelated systems following utterly independent pathways. With all the uneasy certainty of an approaching hurricane season, there is every reason to believe that this storm is upon us.

2. The U.S. security establishment is a loose collection of hierarchies whose long-established seams may be torn open by a very different kind of Surge – this one a storm surge as the drug and terrorist networks are drawn into de facto cooperation, each for its own purposes. It may well be easier to deal with the aftermath of a domestic IED campaign or a weapon of mass destruction exploding in one of our cities than to shore up the many contradictions of an aging Federal system. But just as business hierarchies create matrix teams from existing organizations, it may be possible to engineer new information pathways - especially in intelligence and communications – that simply by-pass existing structures. One obvious place to start is with the inter-operability conundrum highlighted above. However improbable future historians may find it, this is a largely unchanged U.S. vulnerability eight years after the warning shots of 9/11.

3. For all its flaws, seams and contradictions, the U.S. system has a way of regularly producing innovative groups like UWAC. Inducing policy-makers to pay attention to their findings, however, is another matter because such groups typically operate well outside the mainstream of established government and academic hierarchies. But especially in the intelligence world, such independence is a rare and precious commodity because of its potential to produce the early warnings that often elude complacent agencies. Something in the culture of any hierarchy – let alone the top-heavy aggregations of the U.S. intelligence community – instinctively stifles the urge to shout “Iceberg! Dead ahead!” The 9/11 Commission is only the most recent study to suggest that federal agencies are typically inundated with intelligence which contains too little that is truly useful. In contrast, state and local police agencies carry the weightiest security responsibilities but often exist in effective information vacuums. Often these agencies even find themselves challenged to cope with a changing population in which language and cultural differences are defining characteristics.

The conundrums outlined above – as well as new ones springing up every day – are evidence of the tectonic shifts now re-shaping the underlying realities of U.S. security. In fairly dramatic ways, that changing landscape is likely to highlight the dangers of complacency as well as the practical limits of hierarchy as an instinctive organizing principle. This is especially true as dawn breaks on mankind’s second great information revolution, when survival itself may depend on the lightning-fast transfer of information as well as the mechanisms for sharing that information efficiently throughout an increasingly

networked society. Two hundred years of U.S. history have inevitably reshaped and softened its basic outlines. But it is worth recalling that the federal system was founded on the assumption that experimentation and innovation were best performed at the state and local levels, the natural laboratories of future directions for the nation. Because its success ultimately depends more upon measures applied by the several states than in Washington, D.C., perhaps the transformation of homeland security is the appropriate place to re-apply lessons that the Founders knew very well. In adjusting the bureaucratic, top-heavy superstructure currently characterizing the U.S. security establishment, perhaps it is now time to begin reversing the pyramid.

If so, then the organizational models suggested by UWAC and similar groups may be appropriate places to begin: small, independent, non-bureaucratic, open-source, and relentlessly useful through ties with academic and subject-matter experts of every description. Best of all: well away from Washington but with direct linkages into its key policy agencies. What better way to energize inside-the-Beltway policy debates than to enlist fresh new perspectives from outside-the-Beltway? This is especially true of experts whose credentials derive from having worked in open-source intelligence rather than from having been celebrated in the great policy salons of Washington or the green rooms of cable television. The final and possibly most useful precedent for the future is that open-source intelligence organizations are winnowed through the useful discipline of “being paid for being right” rather than for simply answering “Present,” whenever appropriations are handed out.

