The Coming Counterrevolution in Military Affairs

Geoffrey S. French, Veridian
10455 White Granite Drive, Suite 400
Oakton, Virginia 22124
geoff.french@veridian.com

Abstract

As the U.S. military pursues concepts such as network-centric warfare and information dominance, it ties itself to operational strategies designed to be politically acceptable in addition to advantageous in battle. The use of long-range precision-guided munitions as well as sensor-to-shooter technology is meant to make engagements safe for U.S. troops and deadly for enemy combatants, limiting collateral damage. This has increased the pace and exactitude of combat to the point where some analysts believe that the United States has achieved a revolution in military affairs. This superiority, however, is not ironclad. The basic principles of information warfare—the effects of attacks on information systems and the data they contain—undermine this operational style because it is information and perception intensive. An adversary could pursue operational goals on the battlefield based not on attrition or annihilation, but on attacking the information infrastructure and public opinion that supports the U.S. campaign. This would subvert U.S. strategy by directly challenging the information- and perception-intensive tactics and command-and-control practices, posing a counterrevolution in military affairs. This paper explores potential methods that might lead to a counterrevolution and attempts to identify the entities most likely to adopt such a counterstrategy.

Introduction

Current U.S. dominance in military affairs is largely the result of an asymmetric response. The technologies and doctrine that contribute to modern U.S. operations were envisioned and initiated during the Cold War as a counterbalance to the Communist armies that enjoyed advantages in size and geographic proximity to U.S. allies in Europe and Asia. Aside from a pointless strategic nuclear response, a conventional force that had advantages in technology and tempo was the only viable counter to Communist advantages for the United States and its allies. Only the collapse of the Soviet Union has left such a clear gap between the U.S. military and the rest of the world. It is possibly because of this underlying influence in the development of U.S. power that the United States is so

keenly aware of the potential for asymmetric responses to its current strength. Few dominant military forces in history have invested as much time and energy attempting to anticipate future developments in warfare as the United States. As they attempt to identify the next technology or tactic that tips the balance in another's favor, however, strategists may be overlooking a simpler change that is currently attainable by its adversaries. To understand this potentially crippling response to preponderant American power, it is necessary to recognize the trends in U.S. warfare and the progress toward a revolution in military affairs (RMA). This will allow an appreciation of the current adaptations in strategy and tactics that U.S. adversaries are implementing to counter American strength, and a projection of how these changes could be enhanced to undermine the very nature of U.S. strength: a counterrevolution, in a sense. The final sections of this paper will attempt to identify adversaries likely to employ such tactics, and steps that the United States can take immediately to maintain its advantages.

Trends in U.S. Warfare

The current doctrine of the U.S. military is largely the fruition of its traditional ideals that can be traced through the world wars to the U.S. Civil War. General Ulysses S. Grant sought to blend the battle with the campaign, fighting "all the time, every day, keeping the enemy army always within his own army's grip, allowing the enemy no opportunity for deceptive maneuver, but always pounding away until … the enemy at last disintegrated."[1] World War II planners knew U.S. strength lay in "advanced weapons systems—technical prowess and stupendous capability."[2] And despite General William Tecumseh Sherman's advice against it, the United States has continually sought to refine war by defining combatants, preserving life wherever possible, and minimizing collateral damage. These ideals are reflected in several trends in the modern U.S military: long-range precision, information-intensive operations, and progress toward network-centric warfare.[3]

Long-Range Precision

Modern militaries have historically had to choose between long-range attacks and precision strikes. Only recently has technology allowed precise strikes from outside visual range or over the horizon. These have taken several forms that allow U.S. troops to engage the enemy outside of the enemy's range of fire: cruise missiles, high altitude bombing, and unmanned aerial vehicles, guided by lasers, the Global Positioning System (GPS), visual identification, or remote control. As important, this "technical prowess" enables constant engagement and allows for highly precise target selection. The United States does not have a monopoly on highly lethal firepower, but the combined range and precision of these platforms provide the United States a capability long imagined but never realized.

[1] R.F. Weigley, *The American Way of War* (Bloomington: Indiana University Press, 1973), p. 143.
[2] A.C. Wedemeyer, *Wedemeyer Reports* (New York: Holt, 1958), p. 66.
[3] For a broader discussion of the American tendency to emphasize technology and speed as a counter to enemy manpower and size, see J.A. Engel, "Cold War at 30,000 Feet" (2001, PhD Dissertation, University of Wisconsin-Madison), pp. 1–51.

Information-Intensive Operations

Superior firepower alone, however, is not a guarantee of military success. To enable a firepower-centered strategy, the U.S. military has worked to shorten the movement of data from reconnaissance and sensors to the warfighter. This has included improving communications between ground and air forces, providing intelligence and imagery more rapidly to multiple command and control (C2) levels, and better integrating theater surveillance from such systems as the Joint Surveillance and Target Attack Radar System (JSTARS) and the Airborne Warning and Control System (AWACS). This "sensor-to-shooter" emphasis allows pilots and commanders enormous flexibility to engage mobile or temporarily vulnerable targets. The resulting increased tempo and continuity of operations is a true advantage on the open battlefield because it allows decisive maneuver while preventing enemy deceptive maneuver.

These advantages, however, carry corollary risk. More lethal firepower implies heightened risk of friendly fire or collateral damage, especially with an increased tempo of operations. This firepower-centered doctrine, therefore, requires high quality of data at almost every level of the chain of command. The U.S. military has always invested in communication technology and certainly *Joint Vision 2010* looks to information technology (IT) to "improve the ability to see, prioritize, assign, and assess information …. to determine accurate locations of friendly and enemy forces."[4] Although *Joint Vision 2020* retreats from the stronger language about IT's ability to mitigate the fog and friction of war,[5] it still calls for IT to integrate "all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign."[6] To support this capability, the U.S. Department of Defense has begun to build a global information grid (GIG): the "globally interconnected, end-to-end set of information capabilities, associated processes, and people to manage and provide information on demand to warfighters." These systems will not only integrate intelligence and surveillance information, but also logistical, personnel, and medical support systems.[7]

Network-Centric Warfare

All of these trends are seen to converge in the "ideal" of network-centric warfare (NCW). NCW represents a shift from "attrition-style warfare to a much faster and more effective warfighting style characterized by the new concepts of speed of command and self-synchronization."[8] In other words, multiple, rich IT connections throughout the operational force will have two related results. The first is that the command intent will

[4] Joint Chiefs of Staff, *Joint Vision 2010* (Washington D.C.: U.S. Department of Defense, 1995), p. 13.
[5] For an in-depth comparison of the documents, see P.J. Ridderhof, "Thinking out of the box: Reading military texts from a different perspective," *Naval War College Review* LV(4):83–95.
[6] Joint Chiefs of Staff, *Joint Vision 2020* (Washington D.C.: U.S. Department of Defense, 2000), p. 9.
[7] D.S. Alberts, J.J. Garstka, R.E. Hayes, and D.A. Signori, *Understanding Information Age Warfare* (Washington D.C.: Command and Control Research Program, 2001), p. 150.
[8] A.K. Cebrowski and J.J. Garstka, "Network-centric warfare: Its origin and future" *U.S. Naval Institute Proceedings* 124(1):28–35.

saturate the C2 structure so that all involved understand the goals and objectives without a detailed, micromanaged plan. The second is that operations will be highly synchronized and mutually supporting. Ideally, the force will attain self-synchronization where warfighters share awareness and respond to each other's needs as they emerge, constantly adapting to the changing environment. Other derivative advantages are that NCW allows geographically dispersed forces to mass effect and thereby shorten the campaign. Taken together, these effects lead to full spectrum dominance, the stated end goal of *Joint Vision 2010* and *2020*.

Toward a Revolution in Military Affairs

Although the trends described above had been developing for decades, they reached a new level of proficiency in the Persian Gulf War. In that conflict, U.S. advanced weapons systems, with their technical prowess and stupendous capability, provided an enormous advantage over Iraqi forces. Doctrine played an equally important role in overcoming an adversary with modern equipment, but without the quality personnel and support to successfully engage U.S. and coalition forces. The juxtaposition led many to speculate that the United States had attained or was on the threshold of an RMA—a fundamental shift in the organization and pursuit of military objectives.[9]

RMAs have historically resulted from technological advances (e.g., gunpowder or nuclear weapons) or rapid changes in doctrine (usually a shift from linear to maneuver warfare), and often from both in conjunction. The development of *blitzkrieg* warfare is a commonly cited example of an RMA. Although stark contrasts (such as Germany and France in 1940) may help clearly identify the advent of an RMA, its essence is "not the rapidity of the change in military effectiveness relative to opponents, but rather the magnitude of the change compared with preexisting military capabilities."[10] For this reason, RMA skeptics argue that even though the infusion of IT has made the U.S. military highly potent, the change is improved effectiveness, not qualitatively different capability.[11] This debate is important, primarily because RMA proponents argue that the United States must reorganize its C2, procurement, and training to capitalize on the fundamental changes in military technology, specifically long-range precision munitions and intelligence, surveillance, and reconnaissance (ISR) capabilities.

Even without sweeping changes, the United States is approaching the perfection of its strategy of annihilation through heightened integration and operational tempo. As importantly, the means to attain that excellence fits closely with creating the political environment to exercise military power. As the world's remaining superpower—and as a nation that has historically supported international laws and negotiations to resolve dis-

[9] See, for example, N. Davis, "An information-based revolution in military affairs," *Strategic Review* 24(1):43–53.
[10] J.R. FitzSimonds and J.M. van Tol, "Revolutions in military affairs," *Joint Forces Quarterly,* Spring 1994 (No. 4):24–31.
[11] M. O'Hanlon, *Technological Change and the Future of Warfare* (Washington D.C.: Brookings Institution Press, 2000).

putes between nations—the United States comes under international scrutiny when it chooses to intervene in world events militarily. Domestically, the U.S. public holds its government and military to high standards of behavior, discipline, and professionalism. The military's ability to avoid friendly fire, civilian casualties, and collateral damage plays an indispensable role in sustaining consensus at home as well as within any coalition. Just as its lethal firepower carries corollary risk, however, its internal and external expectations may expose a vulnerability that could undermine the way the U.S. military pursues its wartime objectives.

The Potential Counterrevolution

As the military strategist Carl Von Clausewitz argued, war is not "the action of a living force upon a lifeless mass," but the conflict between two forces hoping to achieve victory. Because of this, the U.S. military must expect its potential enemies to react to U.S. tactics and strategy. There are two general methods for responding. The first is to attempt to blunt U.S. advantage on the battlefield. Through tactical deception, oppositional forces can attempt to restore some of the fog and friction of war that U.S. ISR had eliminated. These tactics contribute to a strategy that hopes to outlast the U.S. effort and simply avoid defeat.[12] The second is to respond asymmetrically, employing methods of attack that neutralize or circumvent the U.S. military's ability to defend against or respond to hostile activity. These tend to focus on methods that expand the boundaries of battle, typically through weapons of mass destruction, ballistic missiles, and information operations directed at military or civilian infrastructure.

An examination of these two reactions more fully reveals their potential advantages, but also identifies how they might be combined into an information-based military strategy that challenges U.S. doctrine on the battlefield. Information warfare—in the truest sense of the phrase—would pursue operational goals based not on attrition or annihilation, but on attacking the information systems, infrastructure support, and public opinion that supports the U.S. campaign. This would go beyond simple deception, disruption, and perception management, and subvert U.S. strategy by attacking the information- and perception-intensive tactics and C2 practices, posing, in a sense, a counterrevolution in military affairs (cRMA). The next sections explore these concepts and the effect they could have on U.S. military operations.

Deception

Militaries with a significant disadvantage in technology and firepower must adapt their tactics and strategy to survive. This has held true for many adversaries the United States has engaged, including North Vietnam, North Korea, and Serbia.[13] Typically, the

[12] R.H. Scales, Jr., "Adaptive enemies: Achieving victory by avoiding defeat," *Joint Forces Quarterly,* Autumn/Winter 2000 (No. 23):7–14.
[13] J.W. Kipp and L.W. Grau, "The fog and friction of technology," *Military Review* LXXXII (September/October 2001):88–97.

goal of the adaptation is to (1) avoid annihilation by U.S. firepower and (2) prolong the engagement to increase the cost of the conflict to the United States, in both lives and finance.[14] The basic mechanisms of this adaptation are the dispersal of troops and equipment to minimize the effects of a single strike and the deception of U.S. forces to expend time, intelligence, and ammunition on false targets. This adaptation does not negate U.S. firepower per se, but rather exploits weaknesses in U.S. ISR. Even the most advanced sensors do not provide a complete and accurate reflection of reality. Surveillance and reconnaissance work optimally when quality analysts review and combine multi-source intelligence. The trend of directly linking sensors to shooters eliminates this crucial step. Even U.S. doctrine states that "the demands of modern battle tend to make the processing and production phases [of the U.S. intelligence cycle] indistinguishable."[15] Importantly, these weaknesses still exist, as demonstrated in the 1999 conflict with Serbia over Kosovo. Rudimentary tactics such as camouflage and simple decoys worked well, as did more the sophisticated tactic of exposing a real target to surveillance and replacing it with a decoy for the warfighter to destroy. Estimates of Serbian vehicles destroyed, for example, shrank from an original total of 120 tanks and 220 armored personnel carriers to a final count of 13 and 100, respectively.[16]

Deception tactics as a counter to American military superiority are likely to grow more aggressive in the short term for two reasons. The first is that deception is effective in a tangible sense. Whereas it is difficult to measure expenditure of energy and intelligence resources (a typical goal of deception), it is possible to track the depletion of the U.S. precision-guided munitions inventory, which was severely taxed in the Kosovo campaign. U.S. adversaries can set realistic goals for outlasting a military conflict with the United States. Secondly, the ISR vulnerability born from linking the shooter to the sensor and eliminating multi-source analysis will likely grow in the short term. Because time constrains any processing when attacking mobile targets, the intelligence cycle continues to compress. Although this may provide an immediate advantage, it is likely to expose the U.S. military to a tremendous vulnerability from basic deception techniques.

Disruption

A second reaction to U.S. dominance on the battlefield is to develop asymmetric capabilities, or methods that differ significantly from conventional military operations. Typical lists of asymmetric capabilities focus on nuclear, biological, and chemical weapons, and information operations. Of these, only information operations do not carry a stigma of being outside international norms for behavior in conflict; each other capability has a corresponding international convention to prevent its further development and proliferation. Information operations may have other advantages, especially in terms of cost and low visibility, but it may also have a more direct application on the battlefield. Some

[14] R.H. Scales, Jr., "Adaptive enemies: Achieving victory by avoiding defeat," *Joint Forces Quarterly,* Autumn/Winter 2000 (No. 23):7–14.
[15] U.S. Joint Chiefs of Staff, Joint Publication 2-01, *Joint Intelligence Support to Military Operations* (Washington D.C.: Government Printing Office, 1996), p. III-2.
[16] T.L. Thomas, "Kosovo and the Current Myth of Information Superiority," *Parameters* XXX(1):13–29.

analysts, in fact, consider basic deception as described above to be tactical application of information operations.[17] Although a rigorous definition of information warfare would not include basic deception,[18] successful deception tactics may be supplemented by (and therefore encourage) attacks on the communications and computers that link C2 with ISR (collectively referred to as C4ISR).

On the battlefield, information operations become information warfare—defined here as "attacks on the information technology base of a military."[19] This can take several shapes, but at its most basic, it would involve physical attacks against communication and computer nodes and cyber attacks against classified and unclassified military networks. Even limited success would have the general effect of causing random breakdowns in secure U.S. communications. This would offer two advantages to an adversary. The first is additional opportunities for intelligence collection (which could easily support deception tactics). Several authors have described the general tendency of individuals and groups to use insecure methods of communication when secure methods are disrupted or unavailable; this phenomenon is likely what led to Serbian interception of U.S. communications during the Kosovo conflict.[20] The second advantage is the introduction of entropy, or the general degradation of cohesion in U.S. operations. The concept of entropy-based warfare "derives from the fact that a military force must maintain certain cohesive properties based on orderly construction and operation."[21] Although studies of entropy-based warfare have tended to focus on the potential effect on an adversary, they have also acknowledged that the U.S. military may be susceptible to its effects. The information-intensive nature of U.S. operations, however, makes them very sensitive to entropy. By the logic of NCW, entropy in a highly networked military would erode shared battlefield awareness, disrupt battlefield management, and degrade synchronization. For a geographically dispersed, technologically advanced, and highly mobile military, its information infrastructure may ultimately be its most logical center of gravity.

Combination

Simple disruption of U.S. C4ISR would certainly have detrimental effects on military operations. Manipulation of data on those networks, however, would have an even more pronounced effect. If an adversary could alter the data in a system, "even a small amount of wrong information can have a major impact on the quality of situational

[17] K. McKenzie, Jr., *The Revenge of the Melians: Asymmetric Threats and the Next QDR* (Washington D.C.: National Defense University, 2000), pp. 32–33.
[18] G.S. French, "Building a deterrence policy against strategic information warfare," 2002 Command and Control Research and Technology Symposium, June 10–13, 2002, pp. 3–5.
[19] G.S. French, "Building a deterrence policy against strategic information warfare," 2002 Command and Control Research and Technology Symposium, June 10–13, 2002.
[20] B. Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: John Wiley & Sons, 2000), 261; W.S. Cohen and H.H. Shelton, "Joint statement on the Kosovo After Action Review," statement before the Senate Armed Services Committee, October 14, 1999, 106 Cong. 1 sess.
[21] M. Herman, "Entropy-based warfare: Modeling the revolution in military affairs," *Joint Forces Quarterly,* Autumn/Winter 1999 (No. 20):85–90.

understanding and lower the chances of high-quality military decisions."[22] Moreover, commanders who receive inaccurate information from a system tend to avoid all other information from that system. Importantly, this latter effect can be created without successful manipulation of a network, in that it relies only on perception—that is commanders who "do not *trust* the quality of information available or do not *have confidence* in their information systems"[23] will not make use of their information systems (emphasis added). This can be created by combining deception and disruption. If a commander is aware of cyber attacks (regardless of their success) and sees failed operations (due to deception), the commander may attribute the failure to the information or the IT system rather than on deception. Aggressive pursuit of both deception and information warfare would accelerate entropy in U.S. operations.

Poor quality decisions in high tempo operations involving lethal firepower can lead to several adverse outcomes: friendly fire, collateral damage, and civilian deaths. In U.S. operations specifically, those outcomes are very dangerous because the military, the U.S. public, and the international community are extremely sensitive to them. (Note as examples the reactions to the bombings of the Canadian forces conducting a live-fire exercise in Afghanistan in 2002, the Albanian refugee convoy in Kosovo in April 1999, and the al Firdos bunker in Baghdad in 1991.) Modern conflicts are so political and so well covered by the international media that "the battle for public opinion is as much a condition of victory as killing the enemy."[24] Whereas entropy can lead to random generation of poor decisions, both deception and information warfare could be designed to generate specific poor decisions and specific outcomes. If pursued, this would allow an adversary to replace the typical goals of military operations with another, not simply undermining U.S. advantages in technology and firepower, but turning those advantages against it.

Counterrevolution

In this light, the fragility of the system can be seen. Militarily, the United States operates in an environment that is hypersensitive at every level to adverse outcomes. The potential counterrevolution in military affairs would exploit this as none have, going far beyond pure adaptation and media manipulation. Enemies in the past have used many of these techniques individually and enemies in the future will combine some aggressively. Their true revolutionary employment, however, exchanges one set of military goals for another: tactics that deceive U.S. warfighters and attack communication and computer nodes, causing poor decisions; operational goals of creating specific adverse outcomes that would lead to friendly fire or collateral damage; a strategy meant to attack the domestic and international support for the entire campaign. Enemies interested in countering American power may no longer seek to shoot down a stealth fighter, for example, but

[22] D.S. Alberts, J.J. Garstka, R.E. Hayes, and D.A. Signori, *Understanding Information Age Warfare* (Washington D.C.: Command and Control Research Program, 2001), p. 86.
[23] D.S. Alberts, J.J. Garstka, R.E. Hayes, and D.A. Signori, *Understanding Information Age Warfare* (Washington D.C.: Command and Control Research Program, 2001), p. 86.
[24] A.H. Cordesman, "Arms Control, Technology, and the Revolution in Military Affairs," Center for Strategic and International Studies, 2000, p. 62.

may attempt instead to cause that stealth fighter to strike friendly ground troops. Where Serbians sought to cause U.S. planes to bomb a decoy, future adversaries may attempt to deceive U.S. ISR to bring fire on a school bus. This strategy is not meant to simply survive an attack from a high-powered Western military, but to overturn U.S. strategy that it is built on precision and perception.

Even so, the strategy is simple enough that it would not require highly centralized C2, a usual necessity for elaborate deception campaigns.[25] In fact, the decentralized C2 of guerrilla warfare may actually improve tactical deception by not standardizing the stratagems meant to re-create situations like those mentioned above, causing the United States to hit civilian shelters, refugees, or coalition troops. Importantly, almost no amount of moral superiority would immunize the United States from such adverse outcomes. During the Kosovo campaign, NATO frequently found itself defending its humanitarian intentions, even though its Serbian adversaries were actively killing or forcing Albanian Kosovars out of their homes. Iraq's appeals to international sympathy have met with similar acceptance. This counterrevolution, then, would require little coordination, necessitate little direct conflict with U.S. forces, and frustrate most U.S. advantages.

Potential Revolutionaries

Historically, conceptual changes in military strategy tend to be forced rather than to emerge on their own. The German emphasis on mobility in the interwar period, for example, was more a reaction to the demand for an army limited in size by treaty to defend a wide geographic area than it was a conscious decision to develop a new style of warfare. Similarly, it is doubtful that a U.S. adversary is conceptualizing the cRMA described above and looking for an opportunity to employ it. It is more likely that an adversary will find itself in conflict with the United States and combine adaptations with basic information warfare from necessity. Although it is impossible to predict future developments with certainty, an examination of potential adversaries may indicate some probability of where this threat may arise.

The Spectrum of Threats

Nation states with the highest actual or self-perceived military strength are the least likely to feel the need to adopt measures that challenge rather than mirror or embrace Western-style military forces and operations. Nations with nuclear weapons, therefore, would be the least likely candidates to adopt this cRMA because their nuclear weapons provide a strategic deterrent to U.S. superiority in conventional strength. If a more limited (likely extraterritorial) conflict with these nations were to take place, each current nuclear power has a Western-style military capable of some combined arms operations, and would likely rely on selective engagement as opposed to a fundamental shift in strategy. This is not to say that nuclear powers such as Russia, India, or the People's

[25] M.N. Vego, "Operational deception in the Information Age," *Joint Forces Quarterly,* Spring 2002 (No. 30):60–66.

Republic of China are not looking for asymmetric strategies or investing in information warfare technologies. As mentioned, however, the cRMA requires a shift away from traditional military goals and will mostly likely be necessitated by weakness rather than spurred by research.

Rogue nations are hoping to attain a comparable strategic deterrent through the pursuit of non-conventional weapons delivered by ballistic missiles (which could also serve as a tool of intimidation and coercion). Even so (or perhaps subsequently), rogue nations are more likely to become engaged in a conflict with the United States than nuclear powers. Rogue nations tend to exhibit a confidence that their conventional forces could inflict some casualties on U.S. and allied forces. Even so, any conflict may be seen as a fight for the state's existence, which could drive it toward more extreme measures. The possibility for the cRMA cannot be dismissed here. In fact, the U.S. military should expect to see the pieces of the cRMA in play (manipulation of the press, deception, attacks on C4ISR nodes) especially because some rogue states have witnessed firsthand the adverse outcomes of poor decisions in U.S. operations and none would hesitate to put civilians at risk if it served the interests of the state. It is unlikely, however, that the pieces would be assembled in a revolutionary manner; that is, it seems more plausible that the rogue nation would employ more aggressive rather than more adaptive responses. Ultimately, neither nuclear powers nor rogue nations may feel the acute need to adopt revolutionary tactics and strategy.

The weaker end of the spectrum poses a more likely threat to challenge current military operational strategy. Non-nuclear belligerents have conventional militaries capable of meeting their immediate security needs, but with limited ability to project power or engage in high-intensity warfare. If nations from this group become involved in a conflict with the United States, they are at a major disadvantage and are unlikely to pose a significant threat to U.S. and coalition forces. For any chance to survive a confrontation, they are likely to feel compelled to push adaptation to its limits.

Weaker still are sub-states. These are not simply failed states, but areas where illegitimate powers have military power and perform state-like functions, such as taxation and police functions.[26] This category is difficult to define because it does not meet many of the criteria of a typical Westphalian state. Afghanistan serves as a useful example. When the United States invaded in 2002, most of the country was ruled by the Taliban, which was recognized by only a very small number of other nations. The United States invaded because the terrorist organization Al-Qaida had numerous training camps in the country, and had become intertwined with the Taliban. The United States was toppling a government it did not recognize because of its involvement in and assistance to a non-nation-state group. There are other areas of the world with sub-states, where the putative government cannot or will not establish the rule of law or where powerful paramilitary organizations have de facto authority. These include Indonesia, Sudan, and Colombia. It is in these areas where the U.S. military concept is at its most fragile and most likely to meet a challenge to its basic democratic and Western underpinnings.

[26] R.I. Rotberg, "The new nature of nation-state failure," *The Washington Quarterly* 25(3):85–96.

One Example: Revolutionary Armed Forces of Colombia

To illustrate, one potential adversary highlights the characteristics that give a state or sub-state the potential to subvert current U.S. strategy: the *Fuerzas Armadas Revolucionarias de Colombia* (Revolutionary Armed Forces of Colombia; FARC). A Marxist rebel group in Colombia with roots that trace back to the civil war of 1948–58, FARC has gained hold in the southeast portion of the nation (the savannah and jungle) and has grown in sophistication since the 1980s when it became involved in narcotics trafficking. The roughly $300 million it obtains from "taxation" of the drug trade has allowed FARC to grow to an organization with 18,000 fighters that control approximately 40 percent of the country.[27] Militarily, FARC has used modern communication equipment to operate with a high degree of synchronization, which has proven itself in such incidents as the overrunning of a Colombia Army base in 1996 and the prepared ambush and subsequent annihilation of a counterguerrilla battalion in 1998.[28] FARC is not simply a military force; it is also a terrorist organization, with links to the Irish Republican Army and the *Euskadi Ta Askatasuna* (Basque Fatherland and Liberty; ETA),[29] and it is capable of highly sophisticated attacks. A recently frustrated plot involved five car bombs, each with roughly 250 kg of explosives and equipped with an improvised video and hydraulic systems that that allowed remote control, navigation, and detonation.[30] FARC targets are not limited to typical terrorist targets, such as hotels and airports, however. FARC aggressively attacks infrastructure assets, such as oil pipelines, telecommunications nodes, power plants, and dams.[31]

Taken together, FARC's characteristics make it a prime candidate for the cRMA. It is aggressive in target selection and innovative in attack technique. Although it lacks true combined arms capabilities, it has fused technology into its operations. It has experience working with international media and has often manipulated negotiations with the state to gain military advantage. If the United States becomes militarily engaged in assisting Colombia to address the FARC forces, FARC could rapidly implement cRMA tactics and strategy. It could attack the infrastructure assets supporting U.S. forces, straining day-to-day operations. It could attack C2 nodes and IT networks (especially coalition networks with inherent problems in compatibility), spoof messages, and corrupt data with recruited or planted insiders, introducing entropy. Using its ability to ambush, it could lay in wait for coalition forces to approach on ground, and then fire at U.S. air assets, hoping

[27] J. McDermott, "Colombia's most powerful rebels," BBC News, January 7, 2002, available at http://news.bbc.co.uk/2/hi/Americas/1746777.stm; J. McDermott, "FARC: Rebels without a cause," BBC News, May 21, 2002, available at http://news.bbc.co.uk/2/hi/Americas/1998304.stm.

[28] T. Marks, "Colombian Army Adaptation to FARC Insurgency," Strategic Studies Institute, U.S. Army War College, 2002.

[29] S. O'Driscoll, "Plan to combat 'hi-tech terror,'" *Belfast Telegraph*, February 21, 2003.

[30] BBC News, "Colombian leader murder plot foiled," December 11, 2002, available at http://news.bbc.co.uk/2/hi/americas/2567503.stm

[31] Associated Press, "Suspected rebels attack Colombia's second largest pipeline, communication towers," December 19, 2002; Xinhua, "FARC attacks cause damage to infrastructure in 50 towns," February 27, 2002; Y. Ferrer, "Rebel attacks leave countryside in the dark," Inter Press Service, February 28, 2002; BBC News, "Mayor steps up security as FARC attack Bogota dam," January 25, 2002.

to make them attack coalition troops. It could set up mock communication nodes in civilian buildings or shelters, drawing U.S. fire. Throughout, it could engage the international press about the oppression of the people from the government in Bogota and the ruthlessness of the U.S. attacks. All of these activities are well within FARC capabilities currently and, combined, would have a debilitating effect on U.S. operations.

Maintaining the Advantage

Although the U.S. military still wields an unmatched advantage in almost every dimension of comparison to an opposing force, the cRMA bares certain vulnerabilities in its operations: ISR sensitive to deception, C4ISR sensitive to disruption and corruption, and political support sensitive to adverse outcomes. Each of these can be exploited individually, so each poses an obstacle to full spectrum dominance and each demands mitigation. Basic steps to address these vulnerabilities and maintain the U.S. advantage include improvements in use of light infantry, the C4ISR process, and media relations.

Better Use of Light Infantry

In contrast to its dynamic views on the application of air power and technology to a range of military conflicts, the U.S. military's views towards ground forces remains very traditional, tied to concepts of taking and holding territory on a battleground with coherent front and rear areas. To some extent this is understandable; ground troops inherently incur more risk than those that are geographically removed, and the larger numbers of personnel involved multiply the effects of missteps. These missteps can have a profound effect on public opinion and may even determine the strategic outcome of an operation, just as the loss of 18 Rangers in Mogadishu in 1993 effectively ended U.S. involvement in Somalia. Other factors that contribute to the lack of innovation in use of ground forces include the more complex logistical support and political constraints. The net effect, however, is a reluctance to use ground troops unless full support is available (e.g., armor, artillery, and tactical air support, among others). This supports a grand strategy that avoids conflict except in defense of vital interests and meets adversaries with overwhelming force. It fails to meet the needs of one where the United States engages in low-intensity conflicts in multiple, remote areas of the world, and it has stunted the development of tactics where light infantry could provide an invaluable complement to U.S. air power. Ground forces are better able to identify oppositional forces and are less vulnerable to deception directed toward long-range ISR. They also prompt a dispersed force to either dig in (making them a static target for U.S. airpower) or mass for a counterattack (making them a mobile, but highly vulnerable target for U.S. airpower).[32] The U.S. military needs to invest in the technology to support light infantry strikes in a fluid battlefield and develop the doctrine to support it.

[32] R.H. Scales, "From Korea to Kosovo: How America's Army has learned to fight limited wars in the precision age," *Armed Forces Journal International* 137(5):36–39,41.

Better Use of C4ISR

The U.S. military should also reexamine its C4ISR processes, from beginning to end. First, the data in ISR systems require better security. The general trend in information technology is towards increasing complexity, and this is reflected in military technology and systems, such as the GIG.[33] Many analysts have stated that complexity inherently undermines security.[34] Information security can no longer be an afterthought; radical solutions such as restrictive operating systems and protocols should be considered. Under any circumstances, security should be a high priority reflected in procurement, research, and development. Second, better C4ISR processes could reduce inaccuracies in ISR data. To date, time reductions in the ISR cycle have been passed on to the warfighter, linking the shooter to the sensor. Time reductions may be better invested in improving the decision-making cycle (linking the analyst to the shooter) rather than simply shortening it.[35] Finally, the C4ISR process must account for entropy. Both commanders and warfighters need to have a better understanding of what sensor data indicate and how to utilize intelligence. A commander that understands the nature of ISR data—and how they may be inaccurate—is less likely to discard an entire system due to a single bad incident. Even with an ideal C4ISR model, however, the real-world system will likely have unforeseen failures. Exercises, therefore, should take this into account and warfighters should be trained to make decisions based on partial information, rather than to train solely in a high-quality, data-rich environment.

Better Use of the Media

Finally, if winning the battle for public opinion is as much a condition of victory as killing the enemy, then the U.S. military should invest in it more heavily. When the Kosovo campaign began in 1999, for example, the headquarters public affairs staff had only three media specialists and "the only flag officer authorized to conduct media interviews in the area of responsibility was General [Wesley K.] Clark, the supreme allied commander."[36] One result was delay in providing information after the accidental bombing of Albanian refugee convoy, and the differing accounts of the event issued by NATO badly eroded its credibility. Modern military operations should involve a larger number of media specialists who are available to truthfully discuss events as they unfold. The military must also urge its civilian counterparts that the explanation of the need for a particular military action requires public support, and therefore a coordinated message com-

[33] See, for example, potential logistics support systems described in *Understanding Information Age Warfare*, p. 147.
[34] B. Schneier, *Secrets and Lies: Digital Security in a Networked World* (New York: John Wiley & Sons, 2000); M. Grebb, "Complex networks too easy to hack," Wired News, December 9, 2002, available on-line at http://www.wired.com/news/politics/0,1283,56766,00.html.
[35] T.P.M. Barnett, "The seven deadly sins of network-centric warfare," In: *Information Age Anthology Volume III*, D.S. Alberts and D.S. Papp (eds), (Washington D.C.: DoD C4ISR Cooperative Research Program, 2001).
[36] G. Pounder, "Opportunity lost: Public affairs, information operations, and the air war against Serbia," *Aerospace Power Journal*, XIV(2):56–78.

municated to the public. The U.S. Department of Defense in particular needs a group of media-savvy officers that can explain and defend U.S. military operations.

Perhaps it is as important, however, to change the view of public information as "battle space that must be dominated like any other."[37] This can create from the outset an adversarial relationship with journalists and a hypersensitivity to criticism.[38] Instead, the military's relationship with media should be considered more of a partnership. The U.S. Department of Defense already accredits journalists who accompany U.S. forces overseas, and more can be done to offer training and education that can provide them with context to understand the nature of military intelligence, strategy, and tactics. From classes or seminars at universities to workshops for professionals, the military needs to start creating opportunities to educate and communicate with the media. Educated members of the media will be better equipped to explain the intricacies of military operations to the U.S. and world public. This will never be enough to explain away military errors, but it will make them more easily understood.

Conclusion

"You cannot qualify war in harsher terms than I will," warned General Sherman. "War is cruelty, and you cannot refine it." In spite of this admonition, the United States has sought to refine it, and it is partly this refinement that has exposed vulnerabilities in the C4ISR process, encouraged a reluctance to use anything other than long-range weapons, and narrowed the political support on which military operations depend. Together, these could allow an adversary to pose a significant challenge to the way the United States carries out military operations. Even so, the effort to refine war is rooted deeply in the American character and should not be abandoned. Instead, it should be acknowledged and used as a method of strengthening processes that need to become more robust under any circumstances. A thoroughly strong military system not only limits the ability of other nations to pose asymmetric threats to the United States, but more importantly allows the United States to pose asymmetric responses to adversaries around the world.

[37] G. Pounder, "Opportunity lost: Public affairs, information operations, and the air war against Serbia," *Aerospace Power Journal*, XIV(2):56–78.
[38] R.M. Williams, "The truth, the whole truth or nothing: A media strategy for the military in the Information Age," *Canadian Military Journal* 3(3):11–19.