War in the Information Age

By THOMAS G. MAHNKEN

FIRST PRIZE 95 REVOLUTION IN MILITARY AFFAIRS

NORAD/SPACECOM Command Center, Cheyenne Mountain.

U.S. Air Force (Carol Floyd)

The strategic force commander sat in a dimly-lit subterranean command center, waiting for the battle to start. Each of his component commanders was settled in front of a luminescent screen which displayed aspects of an ongoing situation half a world away. Green icons marked positions of enemy command and control nodes as electronic lightning flickered across the displays revealing traffic over networks.

The war had begun three weeks ago when the President approved the infiltration of enemy information networks. Since then information warfare teams had worked hard to compromise enemy command and control systems. They saw themselves as commandos of the information age who moved unnoticed through information networks, searching out and mapping the sinews that bound the enemy together. Some they would destroy; others they would leave alone.

Thousands of miles away, the first strike began exactly at midnight. Fingers of light arced into the dark sky off the enemy coast as semi-submersible arsenal ships launched wave after wave of ballistic missiles. High overhead stealthy aircraft released their deadly payloads, cruise missiles armed with electromagnetic-pulse warheads designed to short-circuit electronic systems. Nearby, a wing of penetrating aircraft carrying precision-guided munitions peeled away and began bombing runs. In space above them, a constellation of small satellites began to de-orbit payloads of heavy-metal rods capable of destroying the hardest targets known to man.

The commander watched the attack take shape from his underground sanctuary. A network of satellites and unmanned air vehicles began to provide the command center with battle damage assessment data as the attack was still underway. The objective of the strike had been to blind the enemy by dismembering his command and control system, and initial reports showed that it had been largely successful. A red stain spread across the situational displays indicating that the initial waves of ordnance had ripped holes in enemy command and control networks. But other nodes remained functional. Here and there other green lights started to flicker, indicating the presence of previously unknown nodes only now coming to life in the wake of the first attack.

The automated battle manager had already evaluated the initial results of the attack and was formulating the next strike. A list of weapon-target pairings appeared on a screen in front of the commander. He deleted several targets, withholding them for later, then sent the list forward to his component commanders for execution. He looked over at his theater force commander, seated at another screen across the room. Only time would tell whether his men would be needed to bring this conflict to a close.

Over the next few decades, the growth of microprocessing and information technology will create a revolution in military affairs (RMA) that transforms the tools, conduct, and eventually the nature of war.[1] The emergence of long-range precision strike and information warfare may usher in an era of conflict based on paralysis and shock rather than attrition. While no panacea, concepts and organizations for waging war in the information age may offer us decisive advantages over a range of regional enemies as well as leverage against a peer competitor, should one emerge.

The development of systems which collect, process, evaluate, and distribute information is already changing the way we plan and conduct military operations. Advances in sensor technology and data processing will allow us to gather and interpret an extraordinary amount of information about our forces, those of prospective enemies, and the battlefield itself. Sensors operating across the electromagnetic spectrum will locate targets as information processors fuse data from disparate sensors into a single coherent picture. They will enable us to understand where force can be decisive as well as offer greater control over its use. Robust command, control, and communications (C^3) systems will help disseminate the resulting information in seconds, while stealthy precision strike systems will attack an enemy discriminately at long range. Advanced guidance technology, including data from global positioning system (GPS) navigation satellites, will let us strike targets with an accuracy of feet from standoff distances. As a result, we may be able to destroy virtually any enemy target that can be identified.

the most far-reaching effect is the ability to integrate a myriad of systems

The most far-reaching effect of the information revolution is the ability to integrate a myriad of systems into what the Vice Chairman, Admiral William Owens, calls a "system of systems."[2] The network's sensors could sweep the battlefield in search of an enemy, with data processing systems fusing sensor inputs into a single coherent picture and disseminating it to units worldwide. Individual weapon systems could use this information to "bid" on targets, much as traders bid on stocks, with an automated battle manager determining optimum weapon-target combinations. Data from space-based sensors might, for example, be used to target aircraft dropping precision-guided munitions, while special operations forces deep behind enemy lines might be called on to identify targets for long-range ballistic or cruise missile strikes. During and after strikes networked sensors would gather, evaluate, and disseminate battle damage assessment (BDA) much more rapidly than has heretofore been possible.[3]

The effectiveness of long-range precision strike systems will be decided by a game of hide-and-seek played by our sensors and enemy targets. If advances in stealth, deception, and mobility outpace the ability of sensors to acquire targets, then long-range precision strike systems will be ineffective. If, on the other hand, information fusion renders the battlefield transparent, long-range precision strikes will be lethal. Where we end up on this continuum will shape the character of war in the information age.

As the ability to gather, fuse, and disseminate information becomes more central to military affairs, information networks may themselves become critical targets. Thus information warfare, by which a state denies or manipulates the intelligence available to an enemy, may permeate all levels of conflict, from sophisticated tactical electronic warfare to strategic attacks against civil and military information infrastructure. Some see the information revolution as the dawning of a new, bloodless age of conflict dominated by "netwar" and nonlethal technologies.[4] More modestly, it is likely to expand the options available to decisionmakers for waging lethal war.

The Dawn of Shock Warfare

The increasing range and accuracy of weapons will enable us to mass extremely lethal fires at will. Rather than closing on an enemy, we may be able to engage and destroy it at long range. Moreover, the advent of information warfare may allow us to disrupt those networks that allow an enemy to act in a coordinated manner. In combination, long-range precision strike and information warfare capabilities may provide the means to focus our strengths against enemy weaknesses and thus crush its will to resist. The result is likely to be a new paradigm of warfare, based not on attrition but on the ability to paralyze and shock. A fundamental tenet of attrition warfare is that victory can be achieved through the progressive destruction of an enemy. In the end, it is the threat of further punishment that causes surrender. Shock warfare, by contrast, compels an enemy to follow the course that we desire by foreclosing options which we deem undesirable.

A campaign combining strategic information attack and long-range precision strike could afford us substantial leverage against a future enemy. The initial phase would seek to disorient or paralyze an enemy by disrupting its decision cycle. This may, in turn, undermine its confidence by creating uncertainty about controlling the course and outcome of a conflict. It may also increase our capacity to surprise an enemy. Strikes on hostile command and control systems, for example, could hamper enemy ability to employ forces effectively by interfering with the leadership's ability to collect, process, and disseminate information.[5]

Should the initial operation prove insufficient to break enemy will, we might destroy its capability to resist by massive, coordinated strikes on a range of key target networks.[6] Leverage could accrue from the ability both to achieve greater battlespace awareness than an

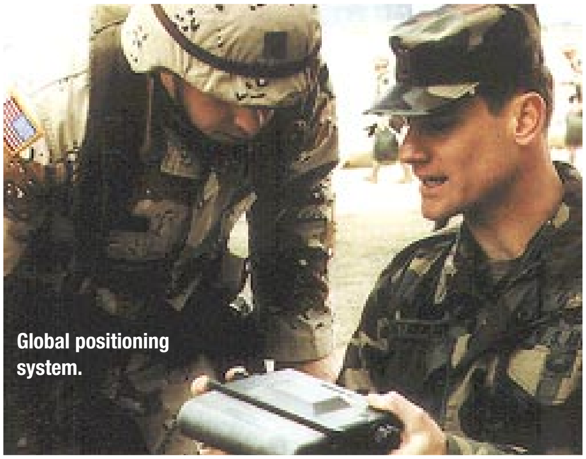
Ensign Thomas G. Mahnken, USNR, is assigned to the Office of Naval Intelligence and is currently a national security fellow in the John M. Olin Institute for Strategic Studies at Harvard University.

enemy and to exploit that advantage by operating faster than an enemy can react.

The effectiveness of such a strategy will depend in part on our ability to collect, assess, disseminate, and exploit information. There is, within reasonable bounds, a relationship between our level of battlespace awareness and the effectiveness of our forces. At a relatively low level of awareness, for example, we may be able to identify discrete targets but unable to understand their relationship. As awareness increases, we may understand how targets form systems and identify key nodes within each system. That may allow us to employ our forces more efficiently.[7]

Mobile communications terminal.

U.S. Army



Global positioning system.

U.S. Army

One way to increase the effectiveness of our forces in war will be to develop a sophisticated understanding of potential enemies in peace. Intelligence to support information warfare and long-range precision strike will, however, be a major challenge.[8] We will need not only to identify individual targets with precision but to understand how they fit into networks. In addition, we must understand which nodes and networks are vulnerabilities.[9] Highly centralized target systems such as national leadership may be vulnerable to a relatively small number of well-placed strikes. By contrast, highly distributed systems such as cellular communication networks might be much more resistant to disruption. Furthermore, we must understand the effect of our strikes upon an enemy's capacity and will to wage war. This will require not only the ability to view an enemy as a coherent system, but insight into its values and strategic culture. One way to improve our understanding of potential enemies might be to constitute multidisciplinary teams of analysts with expertise in intelligence, information systems, targeting, and weapons effects. Such teams could conduct both studies of an enemy's society and culture to determine the most effective ways to shatter its will and in-depth analyses of its target networks to identify vulnerabilities.

decisive outcomes are likely where one side has a marked information advantage

The shape of future warfare will largely depend on achieving an information advantage. One can imagine a situation in which neither side possesses a high battlespace awareness. In such circumstances, neither would be able to conduct decisive operations. Such a battle might resemble a duel between blind swordsmen. A conflict in which both sides enjoy a high level of battlespace awareness might look more like a chess match between grand masters, each maneuvering while waiting for the other to make a mistake. By contrast, decisive outcomes are likely to result from situations where one side enjoys a marked information advantage, as the United States did during the Battle of Midway and the Gulf War.

A future war may thus begin with an information suppression operation aimed at reducing our enemy's battlefield awareness while we protect our own. Achieving information dominance against a peer competitor with distributed and redundant sensor and communication networks is likely to be difficult. Gaining an information advantage will depend on how well we can identify and destroy the key nodes of an enemy's information infrastructure. The level of success required of such an operation will, however, depend on our overall objectives. It may be unnecessary, for example, to sever all links from enemy leadership to its forces. It may be sufficient to disrupt the timing and coherence of its military operations for a period.

The information suppression operation could include attacks on command and control networks, civil telecommunications, and even military and civilian leaders. Long-range ballistic missiles with high-explosive and earth-penetrating warheads, for example, could be used against leadership targets, including hardened facilities, while cruise missiles armed with electromagnetic-pulse warheads disrupted information networks. Some targets may be fixed and others mobile. Coordinating such an operation would include deciding which networks should be infiltrated and exploited and which ones destroyed.

However extensive prewar preparations, we are unlikely to ever enjoy perfect information about an enemy.[10] In the words of Jomini:

> [While it] *is unquestionably of the highest importance to gain [perfect] information, so it is a thing of the utmost difficulty, not to say impossibility; and this is one of the chief causes of the great difference between the theory and the practice of war.*[11]

We may fail to identify key nodes in an enemy's infrastructure or be unable to destroy those we attack. Nor will an enemy stand by passively as it is pummeled. Rather, it will attempt to repair individual targets, reestablish old networks, and build entirely new ones. Success will ultimately depend on destroying enemy information networks faster than they are rebuilt. Conducting rapid battle damage assessment and formulating and launching follow-on strikes before an enemy reacts may therefore be a key source of leverage.

An information suppression operation could shatter an enemy's will to fight and force it to sue for peace. If so, we may achieve Sun Tzu's ideal of victory without combat. Even should an information suppression operation fail to bring victory, we may hamper an enemy's capability to anticipate and react to our actions by disrupting its means of collecting and processing information. Moreover, we may reduce its capacity to transmit timely and coherent orders, thereby limiting its ability to coordinate its forces.

Having suppressed enemy information-gathering, we could attack capabilities that are vital to military operations. The selection of target systems will depend on the character of an enemy and our overall objectives. The scope and duration of the operation will depend on an enemy's sophistication and retaliatory capability as well as our ability to identify and swiftly strike its target systems. Against a relatively unsophisticated enemy with a limited infrastructure such an operation may be relatively straightforward; against a peer competitor it could involve the integrated use of tens of thousands of precision-guided munitions over hours or days. In any event, our capacity to inflict shock will depend on an ability to strike vital target systems in parallel over a short period.[12] In essence this was the approach of air planners prior to the Gulf War: rather than rolling back Iraqi air defenses before attacking strategic target systems, networks were bombed from the outset of the war.[13]

the ability to disrupt enemy information networks may deter aggression

Strategic air and missile defenses are a prerequisite to strikes against vital assets. Without them, an enemy could credibly threaten retaliation against U.S. forces and allies for strikes upon its homeland. Defenses could protect friendly forces and reduce an enemy's confidence in achieving its objectives by long-range strikes. Moreover, the combination of long-range precision strike and strategic defense may convince an enemy that continuing to employ offensive systems is futile. An enemy may instead decide to retain its forces for postwar bargaining.

A strategic campaign of the sort outlined above could prove insufficient to force an enemy to capitulate in and of itself. In such a case, we may need to deploy ground forces to defeat an enemy in the field. Long-range precision strikes may acquire a role as a precursor to theater power projection operations, just as naval gunfire has preceded amphibious landings. Such an operation could dismember an enemy's ability to command and control its forces, allowing our theater forces to defeat any remaining pockets of resistance in detail. At a minimum, it might disorient an enemy, reducing its ability to oppose the insertion of theater forces.

The combination of weapons of mass destruction and long-range precision weapons will make the future battlefield extremely lethal. To credibly project power abroad, we must develop organizations that fight effectively in such an environment. This may include the means to insert and extract forces rapidly. Once inserted in a theater, ground forces may have to disperse, reduce their signature, and move rapidly.[14] They may, in fact, come to resemble the Pentomic division, designed to operate on the nuclear battlefield.[15]

From Theory to Practice

No single concept of warfare can address the entire spectrum of conflicts we may face. The type of campaign described above, for example, will have limited utility at the low end of the warfare spectrum, though intelligence, surveillance, and reconnaissance capabilities may be useful in such contingencies. The combination of long-range precision strike and information warfare may instead provide our decisionmakers with expanded options to deter and wage war against regional powers or a peer competitor. The demonstrated ability to disrupt enemy information networks, for example, may deter aggression. Threats against command and control systems could render an enemy unable to direct its forces should war occur, while destruction of the civil telecommunications system could disrupt its economy. Moreover, in authoritarian states which rely upon repression for political control, such strikes could lead to civil unrest. The acquisition of long-range precision strike and information warfare may also provide options for non-nuclear extended deterrence of aggression against our friends and allies. While the emerging RMA is unlikely to provide a risk-free option for waging strategic warfare against a nuclear-armed enemy, at least without robust strategic air and missile defenses, long-range precision strike and information warfare could accomplish some of those missions heretofore reserved for nuclear weapons.

We cannot, however, expect potential enemies to sit idly by as we amass the means to dismember them. They may take any number of steps to reduce our ability to bring long-range precision strike and information warfare assets to bear upon them. Perhaps the best way to deter us from employing shock warfare would be to acquire nuclear weapons. An enemy may also use camouflage, concealment, and deception to reduce our ability to identify and target key nodes in its infrastructure. Or it could move them underground. Over time, an enemy might even attempt to eliminate all key nodes. Centralized switched telephone networks could be replaced by distributed cellular networks, and national power distribution could be replaced by local networks. An enemy could also use information warfare techniques to disrupt our command and control networks.

Nor may we be free to conduct long-range precision strikes and information warfare based on military effectiveness criteria alone. In the future as today, the use of force will be limited by political considerations. We may, for example, be constrained from striking an enemy homeland, especially if it possesses the means to threaten us with weapons of mass destruction. Future wars could come to resemble not the Gulf War, where our Armed Forces were free to strike virtually any military target they wanted, but the Korean War, where concern over potential Chinese and Soviet responses restricted our actions and created a sanctuary from which enemy forces operated with impunity. Or our dependence on space systems for navigation, communication, and intelligence collection may translate into a reluctance to launch attacks against an enemy's space systems for fear of retaliation. The use of information warfare may likewise be restricted, especially during peacetime. The President might, for example, preclude the Armed Forces from infiltrating an enemy's networks for fear that discovery of such activities could provoke a conflict. Or it might preclude information warfare attacks on networks carrying both civilian and military data for fear of collateral damage.

The emerging military revolution will not eliminate Clauzewitzian friction. Nor will it usher in a new age of bloodless conflict. It may, however, offer us leverage against a range of enemies in peace, crisis, and war. Long range precision strike and information warfare capabilities may deter a potential enemy and offer coercive leverage to resolve crises and conflicts in our favor. Should we fail to exploit the emerging RMA, however, we may well find ourselves at the mercy of another power who has mastered it. JFQ

NOTES

[1] See, for example, A.J. Bacevich, "Preserving the Well-Bred Horse," *The National Interest,* no. 37 (Fall 1994), pp. 43–49; Mary C. FitzGerald, "The Russian Image of Future War," *Comparative Strategy*, vol. 13, no. 2 (April–June 1994), pp. 167–80; James R. FitzSimonds and Jan M. van Tol, "Revolutions in Military Affairs," *Joint Force Quarterly*, no. 4 (Spring 1994), pp. 24–31; Andrew F. Krepinevich, Jr., "Keeping Pace with the Military-Technological Revolution," *Issues in Science and Technology*, vol. 10, no. 4 (Summer 1994), pp. 23–29; and Andrew F. Krepinevich, "Cavalry to Computer: The Patterns of Military Revolutions," *The National Interest* , no. 37 (Fall 1994), pp. 30–42.

[2] William A. Owens, "The Emerging System of Systems," *U.S. Naval Institute Proceedings*, vol. 121, no. 5 (May 1995), pp. 35–39.

[3] Implementing such a concept puts a premium on the ability to gather, correlate, interpret, and transmit information much more rapidly than previously possible. This then poses daunting challenges to data fusion, high-data-rate communications, and inexpensive precision munitions. See James R. FitzSimonds, "The Coming Military Revolution: Opportunities and Risks," *Parameters*, vol. 25, no. 2 (Summer 1995), p. 34.

[4] See John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, vol. 12, no. 2 (April–June 1993), pp. 144–46; and Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown and Company, 1993).

[5] In some ways, the Gulf War represented the first attempt to implement such a strategy. Coalition air campaign planners hoped to strike at Iraq's central nervous system by attacking the leadership, telecommunications, and electric power systems to paralyze the regime in Baghdad. See Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey*, volume I, *Planning and Command and Control* (Washington: Government Printing Office, 1993), pp. 109–11.

[6] A similar strategy was favored by ancient Chinese generals who viewed operations as the interaction of ordinary force (*cheng*) and extraordinary or unconventional force (*ch'i*). The former fixed and made an enemy vulnerable to unconventional force, a flanking maneuver that disrupted enemy strategy and forced capitulation. See the discussion in Sun Tzu, *The Art of War*, translated by Samuel B. Griffith (London: Oxford University Press, 1963), pp. 42–43.

[7] Conversely, lacking reconnaissance, surveillance, and data processing, an enemy may be able to make up for a relatively low level of information by employing its forces *en masse*.

[8] See Edward A. Smith, Jr., "Putting It Through the Right Window," *U.S. Naval Institute Proceedings*, vol. 121, no. 6 (June 1995), pp. 38–40.

[9] See John A. Warden III, "The Enemy as a System," *Airpower Journal*, vol. 9, no. 1 (Spring 1995), pp. 40–55.

[10] Kenneth F. McKenzie, Jr., "Beyond Luddites and Magicians: Examining the MTR," *Parameters*, vol. 25, no. 2 (Summer 1995), pp. 17–19.

[11] Baron de Jomini, *The Art of War*, translated by G.H. Mendell and W.P. Craighill (Philadelphia: J.B. Lippincott & Co., 1862), p. 245.

[12] For a cogent critique, see Richard Szafranski, "Parallel War: Promise and Problems," *U.S. Naval Institute Proceedings*, vol. 121, no. 8 (August 1995), pp. 57–61.

[13] Keaney, *Gulf War Air Power Survey*, volume I, chapter 1.

[14] Gordon R. Sullivan and James M. Dubik, *Land Warfare in the 21st Century* (Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 1993), pp. 12–25.

[15] See, for example, A.J. Bacevich, *The Pentomic Era: The U.S. Army Between Korea and Vietnam* (Washington: National Defense University Press, 1986), chapters 3 and 5.