NATIONAL DEFENSE UNIVERSITY
STRATEGIC FORUM
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Number 132, November 1997

Information Dominance

by Martin C. Libicki

Conclusions

- Information dominance may be defined as superiority in the generation, manipulation, and use of information sufficient to afford its possessors *military* dominance.

- It has three sources:

  - Command and control that permits everyone to know *where* they (and their cohorts) are in the battlespace, and enables them to execute operations *when* and as quickly as necessary.

  - Intelligence that ranges from knowing the enemy's dispositions to knowing the location of enemy assets in real-time with sufficient precision for a one-shot kill.

  - Information warfare that confounds enemy information systems at various points (sensors, communications, processing, and command), while protecting one's own.

Technical means, nevertheless, are no substitute for information dominance at the strategic level: knowing oneself and one's enemy; and, at best, inducing them to see things as one does.

The Role of Information

It is now widely accepted within the U.S. Department of Defense that its military capabilities will be decisive to the extent that the United States can enjoy information dominance over its foes extant and potential. Behind this simple formulation, however, is a set of complex interrelationships between knowledge and action. Information has always been part of conflict, but in times past it has been almost entirely at the human level: who is my enemy, what are his intentions, what can I see and hear of him, and how can I best confound him. Today, human-level analog information is being supplemented by a wealth (perhaps a flood) of machine generated information that can be further processed and distributed through electronic means. Although the United States sees itself as second to none in the quality and training of its manpower, its status as a leader in the production and use of digital information is what undergirds its claim to information dominance.

Information dominance may be defined as superiority in the generation, manipulation, and use of information sufficient to afford its possessors *military* dominance. But information dominance *per se* is not particularly meaningful, for three reasons. First, unlike air combat, where one air force can keep

another one grounded (e.g., Coalition forces in the Gulf War), information power on one side does not prevent its use on the other (with some specialized exceptions such as radio-electronic combat).

Second, every side to a conflict has its own requirement for information depending on its strategy, operations, and tactics. A modern (information age) force needs more information just to function than does a pre-modern force. In Somalia, the United States enjoyed information superiority at the tactical level—its forces could see objects from great distances. But, its insight at the operational level and the political level was inferior to what its adversaries enjoyed.

Third, as Sun Tzu observed 2500 years ago, the most important knowledge one can bring to the battlefield is knowledge of self (what one wants, why, and how badly), and second, a corresponding insight of the other side. Human knowledge forges strategy; machine knowledge produces tactics. Poor strategy can rarely be saved by tactical information superiority.

Information superiority can be analyzed in terms of three elements: command and control, intelligence, and information warfare.

Command and Control

In *Command in War,* (1987, Harvard University Press, Cambridge, MA) Professor Martin Van Creveld identified the primary problem of command and control as knowing where one's forces were (and secondarily, in what shape). John Boyd, a U.S. fighter pilot, posited that conflict was a matter of observing the battlespace, orienting yourself in it, deciding what to do, and doing it (his Observe, Orient, Decide, and Act (OODA) loop); those who could run the cycle better and faster would win. *Where* and *when* are the two key attributes of command and control.

Today, a large share of DOD's investments in information technologies (both computers and communications) is dedicated to improving its knowledge of where and when. The U.S. Army's Force XXI project, for instance, is designed to outfit every fighting vehicle with digital equipment that would report its location, and keep every soldier in electronic contact with his cohorts and commanders. When this concept was taken to the National Training Center in March 1997, observers reported that operations could be planned and carried out in half the time.

The U.S. Navy's emerging network-centric concept holds that the conjunction of communications, sensors, and weapons systems is more important than the individual aircraft, ships, or submarines on which they are deployed. Carrier operations in March 1996 off Taiwan were executed with only three written orders; everything else was communicated in real time. The U.S. Navy's Cooperative Engagement Capability permits many ships (notably their radars and fire control systems) to act as one.

The U.S. Air Force's new expeditionary warfare concept seeks the ability to conduct distributed collaborative planning literally across the world even up to the point that the missions of entire air wings could be reprogrammed even as aircraft are warming up for takeoff. Other initiatives, such as sensor-to-shooter, permit imagery from space and airborne assets to be conveyed to pilots in real time. Scud-hunting techniques under development seek to coordinate multiple aircraft so as to acquire, illuminate, and engage enemy targets literally within minutes. If successful, these efforts could couple the firepower of concentrated forces with the agility of small teams.

Intelligence

Traditionally the role of intelligence in warfare was to inform commanders of the size, location, and intentions of opposing forces—e.g., that a tank battalion was situated on the far side of a mountain ridge. The ability of Coalition forces to organize the "left hook" unnoticed by Iraq was an example of broad intelligence superiority. Technology may soon permit individual platforms to be located in real time within a few meters so that such information can be fed directly to warfighters and, ultimately, to their munitions. The ability of JSTARS (Joint Surveillance, Targeting, and Reconnaissance System aircraft) to identify tank platoons on the road to Khafji (and thereby destroy them piecemeal) was a nascent example of precise intelligence superiority.

The ability to see and strike enemy assets from increasing distances (e.g., from space, and over-the-horizon) is an important aspect of what is called the Revolution in Military Affairs (RMA). This RMA has two phases. The first phase, which started 20 years ago, and is likely to culminate a decade or two hence, has been the development and refinement of precision guided munitions (PGMs) which can strike targets precisely on the basis of manned guidance (e.g., a laser targetter), signature (e.g., a heat-seeking missile), or externally provided coordinates (e.g., JDAM; the joint direct attack munition). True, even visible targets can defend themselves if sufficiently armored, buried, fast, or agile; and, some may fire back. But over time the advantages of PGM are likely to prevail.

Success at the first phase introduces the second. If one can destroy every enemy one can see, then the key to prevailing in conventional conflict is the ability to see things: that is, to detect opposing forces and equipment, identify them, get accurate data on their location and bearing, and strike them—while they are still visible and vulnerable. A man with a gun can do this well (if close enough). The trick is to do this without being a target oneself.

The United States will increasingly rely on sensors to collect information on the battlefield and thereby find targets. Future architectures include a mixture of imagery, radar, infrared, and electronic intelligence sensors in space, on aircraft (e.g., AWACS, JSTARS, Rivet Joint, Cobra Ball), on unmanned aerial vehicles, on ships (e.g., Aegis radars), and in ground facilities (e.g., counter-battery radar) supplemented by a wider array scattered on the terrain (e.g., microphones), in the terrain (e.g., seismic sensors) or in the water (e.g., sonobuoys). Over the next 20 years the various data streams produced by these sensors will be networked, merged, and intelligently fused so as to be able to see more things, faster, and in greater detail. The combination of sensors, networks, and weapons has been referred to as a "System of Systems." When integrated it would reify the RMA as much as any other single innovation. Meanwhile, U.S. forces would keep themselves from becoming casualties by using a combination of stealth and stand-off range. Under the best circumstances, an enemy attempting to move obvious weapons of war over clear boundary lines could be subject to withering attack as U.S. forces, *scan* the battlespace, *sift* for targets, *sort* them into priority order, and *strike* them using long-range fires. In this way, information superiority can, in the right circumstances, be converted into military dominance.

This example also illustrates some limits of seeking information superiority from electronic devices. A tank in combat may be easy to distinguish from anything else; those not specifically identified friendly can be classified as targets. But a pick-up truck with a 25mm machine gun mounted on the back (known as a "technical" in Somalia) is hard to distinguish from a pick-up truck carrying innocent machinery. A peasant tending her fields may or may not be an intelligence agent of a guerrilla force. In such circumstances human intelligence can be helped only modestly by sensor-fed intelligence—and the U.S. military cannot necessarily count on superior human intelligence in every possible scenario it faces.

Information Warfare

The more information is central to military proficiency, the greater the ostensible logic of attacking another side's information systems. Even if these information systems remain intact, simply slowing them down or reducing their fidelity can help. An information system, however, is not a simple mechanism but the combination of sensors, networks, processors, command centers, and operators. Correspondingly, information warfare has five elements:

- *intelligence-based warfare* in which sensors are attacked or otherwise spoofed or confused,
- *electronic warfare* in which communications, radar returns, and signals are either degraded, corrupted, or collected,
- *hacker warfare* in which processors and other automated nodes in the system are degraded, corrupted, or spied on by gaining unauthorized access to computers and then using a system's own features to attack itself,
- *command and control warfare* in which shot and shell are used to disable command centers and their linkages to the field, and
- *psychological operations* in which information is used to discourage, pacify, or confuse opposing forces.

Many argue that information warfare *is* the RMA—that struggles over the information domain may determine the outcomes of conflicts by themselves, or, at least make the results of warfare in other media foregone conclusions (much as air power decided the Gulf War but ground power ended it). This view is probably exaggerated; attacks upon information systems will be useful and necessary adjuncts to other forms of conflict but such attacks, and the defenses against attack, are unlikely to determine the outcome of conflicts themselves. Even a quick perusal of the five categories suggests that many had long antecedents. Picking off opposing commanders, shooting at cavalry pickets, tearing up telegraph lines, deceiving opposing commanders, and manipulating the media were all features of the U.S. Civil War (1861-65). Today's electronic warfare techniques are refinements of what the British and Germans did in World War II. Only hacker warfare is new, for obvious reasons.

Information warfare is an extremely difficult enterprise for several reasons. First, most information systems are complex and opaque: where are the key links, how is information communicated, how are decisions made—and under what influence—are all matters that require considerable intelligence, largely human intelligence, to unearth and comprehend. Second, defense is increasingly favored by technological trends: plunging costs and sophisticated software favor finely distributed information networks that can route around obstruction; cryptology helps people keep secrets and authenticate messages. Third, as a result, success at information warfare tends to be highly opportunistic in that it must take advantage of mistakes, oversights, chance, and circumstance. Fourth, accurate battle damage assessment is elusive because there is little direct physical evidence and indirect evidence can often be masked or faked. Fifth, the uncertainties of information warfare (and its frequent reliance on deception) suggest it is hard to use it as a form of deterrence (information about information warfare is itself information warfare). Sixth, removing the other side's ability to command its forces sometimes makes it difficult for them to come to cease-fire or surrender terms.

Make Them See Things Your Way

As Sun Tzu noted, the acme of military skill is the ability to win without fighting. Information dominance, as such, may obtain, for instance, if one state could convince another that its interests were just and should be acceded to. History shows few cases where zero-sum claims (I want what you have) are happily conceded. But the interests of the United States (or the West, in general) are regarded as universal and positive: an acceptance of the status quo, abjuring the use of force and coercion in

international relations, adhering to the rule of law, the fair and free flow of commerce, the bolstering of human rights, etc. If all other nations were to accept these principles (the Nazis and Communists did not), then the resolution of further disputes would lie in implementation details. Ideological dominance, the "End of History" as it were, is, in many ways the highest form of information dominance.

Such dominance may have a counterpart in cyberspace. In a digitized age, information systems are the lenses through which warfighters look at their world: these lenses magnify the important at the expense of the trivial. Might there be a way to construct an information system for international security that reflects the orientation of its chief architects? Can others be induced to adopt it; if so, will they let their own systems atrophy? That being so, might then a renegade nation be unable to develop an opposing concept of international security without a determined act of will, global scrutiny, decades of work, and considerable national treasure? No one knows the answer to these questions, but if they are "yes" the concept of information dominance may some day assume a far greater importance than mere support to warfighting as known and practiced throughout human history.

Dr. Martin C. Libicki is a senior fellow of INSS. For more information call (202) 685-2259, fax at (202) 685-3866, e-mail at libickim@ndu.edu, or visit his website at http://www.ndu.edu/ndu/inss/libicki.html.

The Strategic Forum provides summaries of work by members and guests of the Institute for National Strategic Studies and the National Defense University faculty. These include reports of original research, synopses of seminars and conferences,the results of unclassified war games, and digests of remarks by distinguished speakers.

Editor in Chief - Hans Binnendijk

Editor - Jonathan W. PierceNOTE

| Return to Top | Return to Strategic Forum Index | Return to Research and Publications |

Return to NDU Homepage
INSS Homepage

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Information Dominance

B. DATE Report Downloaded From the Internet: 09/25/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **National Defense University Press**
Institute for National Strategic Studies
Washington, DC 20001

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/25/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.